博 士 論 文

Proposals of Checking Method and Tool for National Cybersecurity Capacity Enhancement

Shigeo MORI
森　滋男

情報セキュリティ大学院大学
情報セキュリティ研究科
情報セキュリティ専攻

2019 年 3 月

Doctoral Thesis

Proposals of Checking Method and Tool for National Cybersecurity Capacity Enhancement

Shigeo MORI

Department of Information Security

Institute of Information Security

March 2019

(Blank Page)

Acknowledgement

Firstly, I would like to express my sincere gratitude to my supervisor Prof. A. Goto for the continuous support of my Ph.D. study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my Ph.D. study.

Besides my advisor, I would like to thank the rest of my thesis committee: Prof. A. Nakanishi of Meiji University, Prof. H. Yuasa, and Prof. T. Okubo, for their insightful comments and encouragement, but also for the hard question which incented me to widen my research from various perspectives.

I would like to thank Dr. Paul Cornish, Ms. Lara Pace, and the Global Cyber Security Capacity Centre for introduction to their Cybersecurity Capability Maturity Model. That was the beginning of everything of my research.

Also, I would like to thank Prof. T. Nakaizumi of Kanto Gakuin University and Prof. K. Hayashi for their valuable advices especially about policy appraisal and evaluation.

I thank my fellow labmates for the stimulating discussions, for the late night talks we had at the camps, and for all the fun we have had in the last four years.

I also thank the faculties and the participants of the Doctoral Consortium at the Pacific Asia Conference on Information Systems 2018 held in Yokohama for their valuable comments to my research and delightful time during the stay.

I thank the professors and staff of the Institute of Information Security for their guidance and immense support directed to me.

I thank the Mitsubishi Electric Corporation, Mitsubishi Electric Information Systems Corporation, and my colleagues for their cooperation and encouragement to my Ph.D. Study.

Last but not the least, I would like to thank my family for supporting me spiritually throughout writing this thesis and my life in general.

Table of Contents

List of Tables/Figures

Chapter 2

Chapter 3

Chapter 4

論文要旨

サイバー脅威が激化しており，サイバー攻撃に起因する大規模な被害，巨額金銭損失，さらには市民の日常生活に影響する被害まで生じる事態となっている．加えて，一部のサイバー攻撃は国家による活動の一部であることが疑われる．このような状況下，個人，企業，組織による努力のみでは，最早サイバー攻撃に十分に対抗することができるとは言い難く，それらの対策に加えて，国レベルでのサイバーセキュリティ能力を向上させることが，国民の安全安心な生活を維持するためには必須となっている．

さらに，情報技術や，サイバー攻撃者の技能，他国家の能力は急速に進展しており，そのため，国レベルのサイバーセキュリティ能力も，同等程度のペースか，むしろより速いペースで向上させていく必要がある．もしも後手に回ってしまった場合には，取り戻すために多大なる労力と多額のコストを要するものとなる．

また，国レベルのサイバーセキュリティ能力は，国レベルに求められる能力領域において包括的に向上されなければならない．例えば，法執行機関のサイバー犯罪対応能力の向上は果たしたが，検察や法廷の能力向上はできなかったということではいけないのである．さらに，能力は必要な水準まで高められなければならない．能力向上はしたものの攻撃者等の能力に追いつかない，というようなことは許されないのである．一部の能力向上が置き去りにされる，あるいは，能力向上はしたものの不十分であるという状態は，上述した，能力向上が後手に回るということなので，こういった状態を避けなければならないことは明らかであろう．

加えて，国レベルのサイバーセキュリティ能力向上は，効率的に行われなければならない．税金を無駄にしてはいけないということもあるが，予算は有限であり，もしも無駄な向上策が採られた場合には，本来実施すべき，より有効な向上策が阻害されるかもしれないのである．

このように，個人，企業，組織によるサイバー攻撃対策に加えて，国レベルでのサイバーセキュリティ能力を向上させなければならないのであるが，その向上は，以下の 4 要件を満たさなければならない．

1) 国レベルのサイバーセキュリティ能力は，技術発展，攻撃者／他国家の能力向上と，同等もしくはそれ以上のペースで向上されなければならない．（以下、「要件 1『速度』」）
2) 国レベルのサイバーセキュリティ能力は，国レベルで必要な能力領域を包括的にカバーしなければならない．（以下、「要件 2『包括性』」）
3) 国レベルのサイバーセキュリティ能力は，攻撃者や非友好的国家の能力に対抗し得る水準まで向上されなければならない．（以下、「要件 3『水準』」）
4) 国レベルのサイバーセキュリティ能力向上は，限られた資源から最大の効果を得られるよう、効率的でなければならない．（以下、「要件 4『効率性』」）

したがって，国レベルのサイバーセキュリティ能力向上が 4 要件を満たすように施策が立案されているかを確認することは極めて重要である．もしいずれかの要件が満たされていない場合には，国のサイバーセキュリティ戦略に照らして適切な対応，例えば施策の追加や変更，を行う必要がある．

一般的に国の施策が，その目的に照らして適切であるかを確認する方法としては，政策評価が実施されている．しかしながら，調査したところ，政策評価は，本来実施されるべき施策が検討対象に挙がっていないというような状態を検出することには適していない．すなわち，政策評価は，要件 2『包括性』を確認することができない．施策が要件 2『包括性』を満たしているかを評価するためには，政策評価とは異なる方法が必要である．その一方，政策評価は，要件 4『効率性』を確認することには適していると考えられる．

政策評価の調査に加え，国レベルのサイバーセキュリティ能力測定モデル，および，組織や企業向けのサイバーセキュリティガイドラインについて調査を行った．しかしながら，国レベルのサイバーセキュリティ能力を向上させる施策が 4 要件を満たすかどうかを評価する手法は存在しないことが分かった．主な理由は，既存モデルが施策を評価するようには設計されていないこと，および／または，要件 2『包括性』や 3『水準』を評価できないためである．

したがって，国レベルのサイバーセキュリティ能力を向上させる施策が 4 要件を満たすかどうかを評価する手法を開発しなければならない．また，その手法で用いられるチェックリストも開発する必要がある．

チェックリストに関しては，国レベルのサイバーセキュリティ能力測定モデルのひとつであり，グローバル・サイバーセキュリティ能力センターにより開発された「国レベルのサイバーセキュリティ能力成熟度モデル改訂版」（以下、『サイバー成熟度モデル』）が，国レベルで必要な能力領域を包括的に有しており，また，能力を段階的に向上させていけるような水準も示していることから，チェックリストのベースとなり得ることが分かった．

さらに，調査によって，チェックリストには自律的強化機構に関する要求事項を含めるべきであることが分かった．「能力成熟度モデル統合」は，もとはカーネギーメロン大学ソフトウエア工学研究所によって開発され，現在ではプロセス改善の遂行，および，評価のプログラムとして幅広く活用されているものであるが，ここでは，能力が自律的，かつ，永久に最適化するような成熟度が求められる．これをサイバーセキュリティ能力に置き換えてみると，能力が，環境の変化に応じて，外部から指摘を受けずとも自律的に向上できる，そのような能力を醸成する必要があるということであり，それによって要件 1『速度』を満たすことができるということである．したがって，要件 1『速度』は，チェックリストに自律的強化機構に関する要求事項を盛り込み，施策がそのような機構の獲得を目指しているかを評価することで確認できる．

よって，関連研究調査によって，国レベルのサイバーセキュリティ能力を向上させる施策が 4 要件を満たすかどうかを評価する手法を開発しなければならないこと，および，その手法で用いられるチェックリストはサイバー成熟度モデルをベースとすることができることが分かった．4 要件は，以下のように評価する．

1) 要件 1『速度』は，チェックリストに自律的強化機構に関する要求事項を盛り込むことにより評価する．
2) 要件 2『包括性』は，国レベルで必要な能力領域を包括的に有しているサイバー成熟度モデルをベースにチェックリストを策定することにより評価する．
3) 要件 3『水準』は，能力を段階的に向上させていけるような水準を示しているサイバー成熟度モデルをベースにチェックリストを策定することにより評価する．
4) 要件 4『効率性』は，政策評価と本手法を連携させる，すなわち，手法が非効率である可能性のある施策を指摘し，そこに政策評価を集中的に行う，といった形で効果的に評価する．

よって，本論文において，国レベルのサイバーセキュリティ能力の向上を図る施策を評価するための手法を提案する．手法においてチェックリストとして使用するツールも提案する．手法は「ANC3M」（Approaches for National Cybersecurity Capacity enhancement Checking Method：国レベルサイバーセキュリティ能力向上施策評価手法）と呼称する．ツールは「ANC3T」（Approaches for National Cybersecurity Capacity enhancement Checking Tool： 国レベルサイバーセキュリティ能力向上施策評価ツール）と呼称する．

手法である ANC3M は，能力向上施策が適切に立案されていない疑いのある，換言すれば，4 要件のいずれかを満たしていないサイバーセキュリティ能力領域を検出するように設計されている．ANC3M は以下のプロセスによって実行される．

1) 収集：　ある国における国レベルのサイバーセキュリティ能力の向上を図るための施策を全て収集する．
2) 細分化：　それらの施策を個々の行動計画に細分化する．
3) マッピング：行動計画をツール（ANC3T）上にマップする．マップするとは，各行動計画が満たす，もしくは，満たすことに貢献することのできるツール上の要求事項を特定することである．
4) 評価：　マッピング結果を評価する．

評価プロセスにおいて，4 要件は以下のとおり評価される．

1) 要件 1『速度』は，自律的強化機構に関する要求事項に関連付けられた行動計画の数を精査することで評価する．ツール（ANC3T）にはそのような要求事項が 58 項目ある．
2) 要件 2『包括性』は，関連付けられた行動計画が極めて少ない能力領域を検出することで評価する．
3) 要件 3『水準』は，関連付けられた行動計画が低水準に集中している能力領域を検出することで評価する．

4) 要件 3『水準』は，また，関連付けられた行動計画が高水準に集中している能力領域を検出することでも評価する．このケースは，要件 2『包括性』を満たさない可能性も指摘する．
5) 要件 4『効率性』は，関連付けられた行動計画が非常に多い能力領域を検出することで評価する．

ANC3Mは，日本，および，英国の施策に同手法を適用することにより，検証を行った．本検証において，ツールについては，サイバー成熟度モデルをベースとしたものを暫定 ANC3T として使用した．検証の結果，日本，および，英国，双方において，施策が要件を満たしていない可能性のある能力領域が相当数検出された．よって，ANC3M が有効であるものと判断した．

一方，検証によって，暫定 ANC3T が改善を要することが判明した．施策のいくつかが，暫定 ANC3T に定義されている要求事項の，いずれとも対応しなかったのである．したがって，それらの施策に対応する新たな要求事項を ANC3T に追加することとした．

このように，国は，ANC3Mによって施策が要求事項を満たしていない可能性があると指摘された能力領域を詳しく精査することによって，サイバーセキュリティ能力向上が 4 要件を満たすよう，適切に施策が立案されているかを確認することができる．しかしながら，もし何らかの要件が満たされていない場合，国は，そのサイバーセキュリティ戦略に照らして対応を検討しなければならない．すなわち，施策を追加するか，削除するか，変更するかである．そのような意思決定を支援するため，施策のデータベースを提案する．このデータベースは，当該能力領域，または，類似の能力領域において，他の国が計画し実行している施策の事例に関する情報を提供するものであり，「ANC3DB」（Approaches for National Cybersecurity Capacity enhancement Checked DataBase：国レベルサイバーセキュリティ能力向上施策評価済みデータベース）と呼称する．

ANC3DB は，ANC3M によって関連付けられた行動計画と要求事項の組み合わせのデータベースである．AC3DB は以下の機能を提供する．

1) ある能力領域の強化を検討している国に，他国で導入されている施策事例を提供する．
2) 他国の取り組みを模範としたい国に，模範国の施策事例を提供する．
3) 統計分析機能も提供する．例えば，
   a) 世界的に見て，積極的に向上に取り組まれている能力領域は何か？
   b) 世界的に見て，多くの国が目指している能力水準は，どの水準か？
   c) 積極的に取り組まれている領域は，時間の経過とともに変化しているか？
   d) 目指す能力水準は，上昇しているか？
   など．

本研究は，国レベルのサイバーセキュリティ能力の向上を図る施策の適切性を評価する手法とツールを提案することで，国が施策適切性を確認することに貢献するものと考える．ANC3M，ANC3T，および，ANC3DB は，施策を改善することの一助となる．したがって，これらは，国レベルのサイバーセキュリティ能力の向上に貢献するものと考える．究極的には，本研究は，サイバー攻撃の減少と，サイバー攻撃による被害の縮小に貢献できることを目指すものである．

本研究が施策改善に貢献するためには，政府が ANC3M，および，ANC3T を使用して施策評価を行い，ANC3DB を参照して施策改善を検討することが望ましい．しかしながら，これらを使用するのは必ずしも政府である必要はなく，第三者が利用することも可能である．政府以外の誰か，あるいは，他の国の誰かが施策の評価を行い，その結果が施策に関する意思決定に影響することができれば，本研究が，その国の施策の改善に貢献することができる．多くの人が ANC3M を使用して様々な国の施策を評価すれば，本研究の貢献もより大きなものとなる．

本手法は，使用する人による非再現性があまり大きくならないように設計されている．評価者による多少の評価結果の相違は生じるであろうが，非常に大きな相違となる可能性は低い．多少の相違は，評価プロセスにおいて，閾値を調整することで吸収可能である．さらに，ANC3M を使用しての施策評価は，評価者に高度なスキルを求めない．サイバーセキュリティに関する基本的知識があれば十分である．したがって，複数の評価者でマッピング・プロセスを並行して実施し，結果を持ち寄ることで再現性の高い評価結果を目指すことも可能である．

ANC3DB については，現在，データベースには約 1,000 件の組み合わせが含まれている．多様な国の，より多くのデータが収集されれば，データベースの機能性は向上する．したがって，データ収集の努力は今後も継続していく所存である．

Abstract

Cyber threat became so intense that cyber-attacks now can cause huge impacts and monetary damages and even affect daily life of citizens. Additionally, some cyber-attacks are suspected to be parts of national campaigns. Under such circumstances, efforts by the individuals, enterprises and organisations cannot sufficiently counteract against cyber-attacks, and the public sector must enhance the national cybersecurity capacity on top of the countermeasures by the private sector in order to maintain safe and secure lives of citizens.

Moreover, rapid development of information technology, skills of cyber-attackers and capacities of other nations forces a nation to enhance the national capacities at the same velocity or even faster. If a nation falls behind, it will require very hard work and high cost to catch up.

Then, a nation must enhance its cybersecurity capacities in the areas that a nation has to have comprehensively. For example, a nation may not enhance anti-cybercrime capacity of its law enforcement, while the cybersecurity capacities of prosecution and courts are not enhanced. Furthermore, a nation must enhance the national cybersecurity capacities up to the necessary levels. It will not be acceptable that a nation enhances some particular capacities but the enhanced capacities do not match the opponents. The failure of enhancement of some particular capacities and/or insufficient enhancement of capacities will cause a nation to fall behind the development race. It is apparent that a nation must prevent such situations.

Additionally, the national cybersecurity capacity enhancement must be carried out efficiently. Inefficient enhancement will waste tax payers' money, and more importantly, incompetent enhancement may crowd out the essential and more effective enhancement approaches under the limited budget.

Thus, a nation must enhance the national cybersecurity capacity on top of the countermeasures by the private sector, and, furthermore, a nation must satisfy the following four conditions when it enhances its capacities.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (hereafter 'condition 1 *"velocity"*')
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (hereafter 'condition 2 *"coverage"*')
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (hereafter 'condition 3 *"levels"*')
4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (hereafter 'condition 4 *"efficiency"*')

It is essential for a nation to assure that its cybersecurity capacity enhancement is planned so that the four conditions are satisfied. If any conditions are not satisfied, it should consider appropriate actions, for example, addition and/or alteration of the approaches, in light of its cybersecurity strategy.

In order to ensure that the national approaches are appropriate to accomplish the objectives in general, the policy appraisal and evaluation are carried out. However, the survey about the policy appraisal and evaluation revealed that they are not suitable for finding out the situation where the necessary approaches have not even come up for discussion. This means that the policy appraisal and evaluation cannot check the above-mentioned conditions 2 *"coverage"*. In order to make sure that the approaches satisfy the condition 2, a different checking procedure is needed. On the other hand, the policy appraisal and evaluation are supposed to be good at checking the condition 4 *"efficiency"*.

In addition to the above-mentioned policy appraisal and evaluation, the benchmarking models of the national cybersecurity capacities and the cybersecurity guidelines for organisations and enterprises were surveyed. However, the survey revealed that there does not exist the method to check if the national cybersecurity enhancement approaches satisfy the four conditions, mainly because the existing methods are not designed for checking the approaches and/or cannot check the condition 2 *"coverage"* and/or 3 *"levels"*.

Therefore, the method to check if the national approaches satisfy the four conditions must be created. The checklist that will be used in the method should also be created.

With regard to the checklist, the survey about the benchmarking models of the national cybersecurity capacities indicated that one of the models, namely, the "Cybersecurity Capacity Maturity Model for Nations Revised Edition" (hereafter "CSCMMN") developed by the Global Cyber Security Capacity Centre can become the basis of the checklist, as it has the comprehensive coverage of the capacities that a nation has to have and indicates the levels so that a nation can plan to enhance the capacities in step by step manner, in other words, can check the condition 2 *"coverage"* and 3 *"levels"*.

Another implication obtained from the survey is that the checklist should include the requirements for autonomous enhancement mechanism. The "Capability Maturity Model Integration", which was originally developed by Software Engineering Institute of Carnegie Mellon University and is now widely utilised as a process improvement training and appraisal program, requires the maturity where the capabilities optimise autonomously and everlastingly. When it is put into the case of cybersecurity capacity, a nation has to cultivate the ability to improve its capacities autonomously in response to the changes of environments without being instructed to do so by the outside organs, in order to satisfy the condition 1 *"velocity"*. Therefore, the condition 1 *"velocity"* can be checked by incorporating the requirements for

autonomous enhancement mechanism into the checklist and checking if the approaches are intended to obtain such mechanisms.

Thus, the survey of the related researches indicated that the method must be created to check if the approaches for the national cybersecurity capacity enhancement satisfy the four conditions, and that the checklist that will be used in the method can be based on the CSCMMN. The four conditions will be checked as follows;

1) The condition 1 *"velocity"* will be checked by incorporating the requirements of autonomous enhancement mechanism to the checklist.
2) The condition 2 *"coverage"* will be checked by creating the checklist based on the CSCMMN which has the comprehensive coverage of the capacities that a nation has to have.
3) The condition 3 *"levels"* will be checked by creating the checklist based on the CSCMMN which indicates the levels so that a nation can plan to enhance the capacities in step by step manner.
4) The condition 4 *"efficiency"* will be effectively checked by combining the policy appraisal and evaluation and the method, where the method indicates the possible inefficient approaches which will be intensely applied the policy appraisal and evaluation.

Therefore, in this thesis, the method for checking the approaches for the national cybersecurity capacity enhancement and the tool that is used as the checklist in the method are proposed. The method is called "ANC3M" (Approaches for National Cybersecurity Capacity enhancement Checking Method). The tool is called "ANC3T" (Approaches for National Cybersecurity Capacity enhancement Checking Tool).

The method, ANC3M, is designed to find out the cybersecurity capacity areas for which the enhancement approaches are suspected to be inappropriately planned, in other words, not satisfying any of the four conditions. The ANC3M consists of the following processes.

1) Collection: All approaches of a nation for national cybersecurity capacity enhancement are collected.
2) Itemisation: The approaches are itemised into pieces of action items.
3) Mapping: The action items are mapped onto the tool (ANC3T). "Map" in this case means to identify the requirements of the tool that each action item will fulfil or contribute toward fulfilling.
4) Evaluation: The mapping result is evaluated.

The four conditions are checked in the evaluation process as follows;

1) The condition 1 *"velocity"* will be checked by examining the number of the action items (itemised approaches) related to the requirements for autonomous enhancement mechanism. There exist 58 such requirements in the tool (ANC3T).

2) The condition 2 *"coverage"* will be checked by finding out the capacity areas that few action items are related to.
3) The condition 3 *"levels"* will be checked by finding out the capacity areas where the action items are related only to the lower levels.
4) The condition 3 *"levels"* will also be checked by finding out the capacity areas where the action items are related only to the higher levels. This case may also indicate the unsatisfaction of the condition 2 *"coverage"*.
5) The condition 4 *"efficiency"* will be checked by finding out the capacity areas that a lot of action items are related to.

The ANC3M was verified by applying the method to the approaches of Japan and the United Kingdom. For this verification, the tool based on the CSCMMN was used as the tentative ANC3T. The verification discovered a number of capacity areas where the enhancement approaches may not be satisfying the conditions in both Japan and the U.K. Therefore, it is thought that the ANC3M is effective.

On the other hand, the verification also revealed that the tentative ANC3T needs to be enhanced, because some approaches did not match any of the requirements described in the tentative ANC3T. Therefore, new requirements that correspond the unmatched approaches are added to the ANC3T.

Thus, by further examination of the capacity areas where the ANC3M indicates the possible dissatisfactory approaches, a nation can assure that its cybersecurity capacity enhancement is planned appropriately so that the capacity enhancement satisfies the four conditions. However, if any conditions are not satisfied, a nation must consider corresponding actions in light of its cybersecurity strategy, i.e., addition, reduction and/or alteration of the approaches. In order to support such decisions by providing with the information about the approaches that are implemented by the other nations, the database of the approaches is also proposed. The database is called "ANC3DB" (Approaches for National Cybersecurity Capacity enhancement Checked DataBase).

The ANC3DB is the database of the pairs of the action items and the requirements that are related each other by the ANC3M processes. The ANC3DB is supposed to function as follows;

1) When a nation plans to enhance some particular capacities, the ANC3DB can provide with the examples of the approaches that are implemented by other nations.
2) When a nation considers another nation as a role model, the ANC3DB can provide with the examples that are implemented by the model nation.
3) The ANC3DB can provide with the functionality for statistical analysis, for example;
   a) What capacity areas are emphasised on a global basis?
   b) What levels are intensely aimed at on a global basis?
   c) Are the emphasised areas shifting according to the lapse of time?

d) Are the aimed levels rising?

and so on.

By proposing the method and the tool to check the appropriateness of the approaches for the national cybersecurity capacity enhancement, this research should contribute toward ensuring the appropriateness of the approaches. And the ANC3M, ANC3T and ANC3DB will help improving the approaches. Then, they should contribute toward improvement of the national cybersecurity capacities. Ultimately, this research is aiming at contribution to the decrease of cyber-attacks world-wide and reduction of the possible damages caused by cyber-attacks.

In order for the research to contribute toward improvement of the approaches, it is desirable that the policymakers carry out the check of the approaches using the ANC3M and ANC3T, and refer to the ANC3DB for consideration of improvement of the approaches. However, it is not necessarily the policymakers who use them, but anyone else can do. If anyone other than the policymakers of the nation, or even anyone outside of the nation carry out the check of the approaches and the result informs to the decision of the approaches, this research can contribute towards improvement of the approaches of that nation. If a lot of people join and check the approaches of various nations using the ANC3M, the contribution of this research will be greater.

The method is designed so that the checking result will not be much inconsistent subject to the person who use it. There may be some inconsistency of the checking results subject to the checker, but the inconsistency is hardly supposed to become significant. And small inconsistency can be absorbed by adjusting the thresholds when evaluating the mapped results. Additionally, checking the approaches using the ANC3M does not require the checkers to have very high skills. People with a basic knowledge about cybersecurity can do. Therefore, it is possible for two or more checkers to perform the mapping process in parallel and then to consolidate the outputs for a stable result.

With regard to the ANC3DB, the database currently contains approximately 1,000 pairs. The database will function better if it contains more data of the various nations. Therefore, it is planned to continue collecting the data.

Chapter 1. Introduction

1.1 Background

Cyber incidents are reported almost daily. Although there exist various targets, attack methods, damages, presumed attackers and presumed objectives, their impact seems to be getting larger, broader and more serious. In October 2017, Yahoo! announced that three billion (roughly 40%! of the global population) of its customer data had been exfiltrated by cyber-attackers [1]. In February 2016, the Bangladesh Bank, which is the central bank of Bangladesh, was attacked and had US$ 951 million stolen via the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network [2]. In December 2015 and in December 2016, Ukraine experienced wide area power downs as a result of cyber-attacks [3, 4]. Nowadays, cyber-attacks can cause huge impact and monetary damages and even affect the daily life of citizens. Moreover, some incidents are arguably suspected to be parts of national campaigns [5].

1.2 Rise of Public Sector's Responsibilities in Cybersecurity

Under such circumstances which are described in section 1.1, efforts by the private sector, including individuals, cannot sufficiently counteract against cyber-attacks. Therefore, the public sector must endeavour to enhance the national cybersecurity capacity such that a nation can retain safe and secure life of its citizens.

Tagawa and Hayashi believe that it is necessary to enhance the national cybersecurity in every aspect with the combined efforts of the entire country. They also think that this should be done by building the proactive national cybersecurity capacities, based on sustained and private-sector-initiated reactive cybersecurity countermeasures [6] (original in Japanese).

1.3 Necessity of Enhancement of National Cybersecurity Capacities

A nation must have sufficient cybersecurity capacities in order to counteract against cyber-attackers and to retain safe and secure life of its citizens. If the capacities are not sufficient, the public sector must enhance the capacities to the sufficient level.

Furthermore, information technology, skills of cyber-attackers and capacities of other nations develop rapidly. Such a rapid development forces a nation to enhance its capacities at the same velocity or even faster. If a nation falls behind, the nation will be required very hard work and high cost to catch up. The nations with the insufficient capacities must work even harder to surpass the development speed of the others.

Additionally, a nation has to have comprehensive cybersecurity capacities that are necessary for nations. For example, a nation must have the capacities to prosecute and judge cybercrimes as well as anti-cybercrime capacity of its law enforcement. And, of

course, those capacity areas must be enhanced as technology and capacities of the others develop.

Moreover, a nation must enhance the national cybersecurity capacities up to the necessary levels. It will not be acceptable that a nation enhances some particular capacity areas but the enhanced capacities do not match the opponents.

If a nation fails enhancement of some particular capacity areas, or enhances its capacities but the enhanced capacities do not match the opponents, the nation will fall behind and will be forced to pay a lot of work and money to catch up, or otherwise the cyber-attackers may bring serious damages to the nation.

Thus, a nation must have sufficient cybersecurity capacities and must enhance its capacities. Moreover, the enhancement must have the following characteristics.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those.
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations.
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations.

1.4 Importance of National Approaches for Cybersecurity Capacity Enhancement

The public sector has the responsibilities to ensure that the national cybersecurity capacities are sufficient and to enhance the capacities satisfying the following three conditions (as stated in section 1.3)

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (hereafter ‘condition 1 *“velocity”*’)
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (hereafter ‘condition 2 *“coverage”*’)
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (hereafter ‘condition 3 *“levels”*’)

If the condition 1 *“velocity”* is not satisfied, the capacities will not effectively mitigate the risk. For example, even if a security device capable to detect unknown malwares is

developed and used, if cyber-attackers have already developed the techniques to evade such a device, the defender may not effectively prevent the malwares to intrude.

If the condition 2 *"coverage"* is not satisfied, the capacities will not effectively mitigate the risk. For example, even if the countermeasures against cyber-attacks are robust, if the legal framework against cybercrimes are unestablished, cyber-attackers will be encouraged to act vigorously and even foreign attackers may be attracted to recognise the nation as an attacking base.

If the condition 3 *"levels"* is not satisfied, the capacities will not effectively mitigate the risk. For example, even if the approaches are executed successfully to promote the anti-malware softwares used in the PCs that have internet connectivity and such PCs become secure, if cyber-attackers shift their attacking accesses to the PCs that are not connected to internet and/or to the IoTs (Internet of Things), the above-mentioned approaches alone cannot sufficiently contribute to the security of the network and need to be considered for expansion to promote security on the wider coverage of the devices.

Additionally, a nation must carry out the enhancement of its cybersecurity capacities efficiently. This is the fourth condition.

4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (hereafter 'condition 4 *"efficiency"*')

If the condition 4 *"efficiency"* is not satisfied, i.e., if the enhancement of the capacities is done inefficiently, it will be a waste of taxpayers' money, and moreover, may be preventing other more important approaches from being implemented. For example, two or more government agencies plan and execute the different approaches that are aimed at the same result, they may possibly be integrated into fewer and more efficient approaches. Or, if the approaches that are aimed at the very basic cybersecurity, for example, the promotion of anti-malware softwares, are continued even after such attitudes have been widespread, it should be considered to cancel the approaches and reallocate the resources to others such as awareness raising of IoT security, etc.

Thus, the public sector must assure that the enhancement of the national cybersecurity capacities satisfies the four conditions. Can they check it by assessing the enhanced capacities? No. It's already dissatisfactory in the condition 1 *"velocity"*. They must check it before enhancing. Therefore, the public sector must ensure that the approaches for enhancement of the national cybersecurity capacities are planned so that the four conditions will be satisfied.

1.5 Purposes of this Research

In the previous sections (1.1 - 1.4), it was pointed out that the cyber-attacks became more serious and the sufficient national cybersecurity capacity became essential in order to retain safe and secure life of citizens. Moreover, rapid development of information technology, skills of cyber-attackers and capacities of other nations forces a nation to enhance the national capacities at the same velocity or even faster. If a nation falls behind, it will require very hard work and high cost to catch up. In order to avoid falling behind, a nation must assure that the enhancement covers the necessary capacity areas comprehensively and aims at the levels to match the opponents, as well as being efficient.

Thus, the public sector must ensure that the approaches for enhancement of the national cybersecurity capacities are satisfying the following four conditions.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (condition 1 *"velocity"*)
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (condition 2 *"coverage"*)
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (condition 3 *"levels"*)
4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (condition 4 *"efficiency"*)

Then, how can they make sure that the approaches are satisfying the four conditions?

The purpose of this research is to help ensuring it by providing with the method to check the approaches for the national cybersecurity capacity enhancement. The tool that is used in the method is also proposed.

The method (and the tool) can be used in the following occasions.

1) When policymakers ensure that the existing approaches are satisfying the conditions.
2) When policymakers check that the planned approaches are satisfying the conditions.
3) When policymakers plan the new approaches to enhance particular capacities.
4) When the third parties review the approaches if they are satisfying the conditions.
5) When anyone learn the aims and the targeted levels of the approaches of other nation(s).

In order to check the appropriateness of the national approaches (or regulations), the policy appraisal and evaluation (or regulatory impact analysis) are widely executed [7]. The proposed method is complementary to the appraisal and evaluation. The difference between the proposed method and the appraisal and evaluation is discussed in section 2.2, where it is also indicated that the former complements the latter.

Additionally, the national approaches for cybersecurity capacity enhancement must be considered for improvement if the approaches appear to be dissatisfying any of the four conditions. In order to support such consideration and decision making for alteration, addition and/or reduction of the approaches, the database of the approaches is also proposed in this research.

1.6 Contribution of this Research

By proposing the method and the tool to check the appropriateness of the approaches for the national cybersecurity capacity enhancement, this research will contribute toward ensuring the appropriateness of the approaches. And the method, the tool and the database will help improving the approaches. Then, they should contribute toward improvement of the national cybersecurity capacities. Ultimately, this research is aiming at contribution to the decrease of cyber-attacks world-wide and reduction of the possible damages caused by cyber-attacks.

In order for the research to contribute toward improvement of the approaches, it is desirable that the policymakers carry out the check of the approaches using the method and the tool, and refer to the database for consideration of improvement of the approaches. However, it is not necessarily the policymakers but anyone else who use the method, tool and database. If anyone other than the policymakers of the nation, or even anyone outside of the nation carry out the check of the approaches and the result informs to the decision of the approaches, this research can contribute towards improvement of the approaches of that nation.

In the verification process, the author checked the approaches of Japan and the United Kingdom. Even if the author continues checking the approaches of other nations, the number of the nations whose approaches are check by the method will be limited. However, if other people join and check the approaches of various nations using the method, the approaches of an increased number of nations will be checked and the contribution of this research will be greater.

The method is designed so that the checking result will not be much inconsistent subject to the person who use it. The discussion about the reproducibility is in section 4.5.2.

Furthermore, the database that is proposed in this research can be used with or without the checking method. In other words, while the database can be used after checking the approaches using the method, it can also be used on its own for consideration of improvement of the approaches.

Therefore, this research is supposed to contribute widely toward improvement of the approaches, the national cybersecurity capacities and ultimately cyber threat environment.

1.7 Definition

1.7.1 Definition of Capacity

In this research, national ability to do something with regard to cybersecurity is called “capacity”. “Capacity” also includes the state where something is at a certain status that enables something to be done with regard to cybersecurity. For example, the followings all describe that the nation has capacities.

1) Law enforcement can utilise sophisticated digital forensic tools.
2) Analytical capacity exists to support the coordination of resource allocation for national cyber defence;
3) The majority of users trust in the secure use of e-commerce services and make use of them.
4) Cybersecurity standards and good practices in guiding procurement processes are being adhered to widely within public and private sectors.

On the other hand, “capability” is not used in this research except for the cases referring to the Capability Maturity Model Integration, because it is not essential in this research that an ability is capacity or capability. Please note that another exception using “capability” is the name of the Cybersecurity *Capability* Maturity Model v1.2 in December 2014, which then was renamed as the Cybersecurity *Capacity* Maturity Model for Nations Revised Edition in February 2017. The publisher of the models is the Global Cyber Security *Capacity* Centre.

Additionally, “capacity area” means the domain where some capacities assemble to enable something more significant with regard to cybersecurity, for example;

1) Identification of incidents.
2) Risk management and response in critical infrastructure protection.
3) Executive awareness raising.
4) Legislative framework for ICT security.
5) Adherence to ICT security standards.
6) Responsible disclosure.

and so on.

1.7.2 Definition of Approach

In this research, the “approaches” mean practical actions that are performed by the public sector. The actions carried out by the central government of a nation are usually classified to the following three tiers; [7]

1) Policy: a basic course to counteract against a concern
2) Program: a practical means to achieve the objective of the policy

3) Project: an individual project/service under the program

The actions that are the subjects of this research range from the programs to the projects. Therefore, the “approach” represents the programs and the projects that are the subjects of the research.

The approaches that are planned and executed in order to enhance the national cybersecurity capacities are the subjects of the research. The approaches carried out by organisations and enterprises in order to enhance their capacities or to counteract against cyber-attacks are not the subjects of this research. However, the cybersecurity capacities of the organisations and enterprises are the parts of the national cybersecurity capacity. Therefore, a national approach that urges the organisations and enterprises to bring about the approaches for enhancing their capacities is included in the subjects of the research.

(Blank Page)

Chapter 2. Related Researches

2.1 Introduction

The purpose of this research is to provide with the method and the tool to check if the national approaches for cybersecurity capacity enhancement are satisfying the following four conditions.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (condition 1 *"velocity"*)
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (condition 2 *"coverage"*)
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (condition 3 *"levels"*)
4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (condition 4 *"efficiency"*)

As mentioned in section 1.5, the policy appraisal and evaluation are widely executed. The survey about the policy appraisal and evaluation revealed that the existing appraisal and evaluation do not satisfy the purpose of this research. Therefore, the proposed method is necessary in order to complement the appraisal and evaluation. The survey about the appraisal and evaluation is introduced in section 2.2.

Thus, the method is necessary to check if the national approaches are satisfying the four conditions. The survey revealed that there does not exist any such method at present, but there do exist the benchmarkings of the national cybersecurity capacities. Benchmarking the national capacities is different from checking the national approaches for capacity enhancement. Nevertheless, the benchmarkings of the national cybersecurity capacities were surveyed to see if the tools can be used for checking the approaches.

The survey about the benchmarkings revealed the tools for benchmarking cannot be used for checking the approaches. However, it was also revealed that one of those tools can become the basis of the tool that will be used in the method for checking the approaches. The survey about the benchmarkings is introduced in section 2.3.

Also, there exist the tools to guide the organisations and enterprises for enhancement of their cybersecurity. One of the most notable guidelines of the kind is the "Framework for Improving Critical Infrastructure Cybersecurity" (hereafter "NIST framework") established by the National Institute of Standards and Technology (NIST) of the United States [8]. However, the NIST framework is targeted at enterprises and organisations, and does not cover some of the capacity areas that nations have to have, for example, the

anti-cybercrime legal framework. Therefore, the NIST framework cannot check the condition 2 *"coverage"* at least, and is apparently not suitable for checking the national approaches. Other tools and guidelines for cybersecurity for organisations and enterprises are surveyed but no such tools or guidelines that are suitable for checking the national approaches were found. The survey about the tools and guidelines for organisations and enterprises is introduced in section 2.4.

The survey about the policy appraisal and evaluation, the benchmarkings of the national cybersecurity capacities, and the tools and guidelines for cybersecurity for organisations and enterprises revealed that the existing tools are not suitable for checking the approaches, and the method and the tool for checking the approaches for national cybersecurity capacity enhancement should be created. The survey also revealed that one of the benchmarking tools can be used as the basis for the checking tool.

Then, the Capability Maturity Model Integration" (hereafter "CMMI") was surveyed because the CMMI is a process improvement program and was supposed to give good implication for the development of the method and the tool that are aimed at improving the approaches. The survey about the CMMI is introduced in section 2.5.

2.2 Policy Appraisal and Evaluation

2.2.1 What are Policy Appraisal and Evaluation

It is pointed out that the role of the public sector must be based on the market principle and divided clearly from the roles of the private sector. The public sector itself must function more efficiently. Moreover, the public sector must refresh its recognition that it owes to account for its activities both in ex ante and ex post manners. One of the mechanisms to do that is the "policy appraisal and evaluation" which is sometimes referred to as a "quality management of policy" [7] (original in Japanese).

The Green Book: Central Government Guidance on Appraisal and Evaluation [9] published by the Treasury of the United Kingdom says that the policy appraisal is the process of assessing the costs, benefits and risks of alternative ways to meet government objectives. It helps decision makers to understand the potential effects, trade-offs and overall impact of options by providing an objective evidence base for decision making. Economic appraisal is based on the principles of welfare economics – that is, how the government can improve social welfare or wellbeing, referred to in the Green Book as social value. According to the definition in the green book, the policy appraisal is done before policy implementation while the policy evaluation is the systematic assessment of an intervention's design, implementation and outcomes and done after implementation.

The policy appraisal and evaluation vary by nations and by fields of activities of the public sector [7].

Regulations: In the U.K., the U.S.A., Canada, Australia and so on, when the public sector implements a new regulation or alters the existing regulation, the appraisal of the regulation must be carried out. This appraisal is usually called "Regulatory Impact Assessment (RIA)" or "Regulatory Impact Analysis (RIA)". RIA consists of explanation of the necessity of the regulation, the estimated costs and benefits arising from the implementation of the regulation, explanation that the benefits exceed the costs and comparison among the alternatives. In some nations, publication of the result of the RIA and collection of the public comments are mandatory.

Public Works Projects: The appraisal for the public works projects has been executed for very long time. Appraisal is usually done by cost-benefit analyses.

Science and Technology Researches: The evaluation of resource allocation is mainly used for the appraisal of science and technology researches policy rather than cost-benefit analysis.

Official Development Assistance: The appraisal for official development assistance (ODA) has been institutionalised for long time. Appraisal and evaluation are done both before and after the project.

General Public Sector Services/Activities: Various appraisal methods are institutionalised for the appraisal of general public sector services and activities. The Green Book [9] of the U.K. is the general guideline for the policy appraisal in the U.K.

2.2.2 Effectiveness and Limitations of Policy Appraisal and Evaluation

As mentioned in section 2.2.1, the policy appraisal and evaluation are widely carried out for the various policy fields under the various institutionalised systems using the various methods. The policy appraisal and evaluation are the processes of assessing the costs, benefits and risks, and mainly focus on 3E (economy, efficiency and effectiveness).

Kodama says in "Verification of the Policy Appraisal and Evaluation of the United Kingdom and Suggestion to Japan" [10] that the policy appraisal and evaluation of the U.K. originated from the Comprehensive Spending Review (CSR) in 1998 (Original in Japanese). The CSR is a governmental process in the U.K. to set the expenditure limits and define the improvements. In 1997, Tony Blair, leader of the Labour Party, became the Prime Minster of the U.K. after 18 years of governance of the Conservative Party. Mr. Blair coped with administrative and financial reforms under his pledge "Modernising Government" and published Economic and Fiscal Strategy Report (EFSR). The CSR was based on the EFSR. Thus, the CSR from which the policy appraisal and evaluation evolved is aimed at streamlining the expenditure of the public sector.

Therefore, the policy appraisal and evaluation alone cannot assure that the approaches effectively enhance the national cybersecurity capacities.

For example, even if the approaches are effectively implemented to enhance the capability of the law enforcement for tackling cyber-crimes and arresting the criminals, if there do not exist any plan to enhance the capabilities of the prosecutors to handle the digital evidence and to pursue the cyber cases, the nation may become a good haven for cyber-attackers. The policy appraisal and evaluation can probably improve the approaches for enhancing the law enforcement, but may fail to point out the lack of the approaches for enhancing the prosecution.

Thus, the policy appraisal and evaluation are good at evaluating the effectiveness and efficiency of the approaches (and their alternatives) that have come up for discussion, but are not suitable for discovery of the approaches that have not. In other words, the policy appraisal and evaluation cannot check if the

approaches satisfy the condition 2 *"coverage"*, while they are supposed to be suitable for checking the condition 4 *"efficiency"*.

2.2.3 Policy Appraisal and Evaluation and Proposed Method Coexist

As mentioned in the previous section (section 2.2.2), the policy appraisal and evaluation are not suitable for discovering the approaches that have not come up for discussion. The proposed method is most useful in finding out such approaches. It can discover the cybersecurity capacity areas that the approaches are not planned to enhance sufficiently by some reasons. The reasons may include that the areas are considered to have been enhanced enough, that the areas are considered necessary to be enhanced but not prioritised, or that the areas are not recognised to be important. After discovery, the reasons should be examined and the additional approaches should be planned if necessary. Then the new approaches will be appraised accordingly.

The proposed method can also discover the capacity areas for which the approaches are planned possibly inefficiently. It can be used as an indicator for the policy appraisal and evaluation to be focused on. The policy appraisal and evaluation are the processes that require a lot of hard and nervous work. By pointing out the possibly inefficient capacity areas, the proposed method may improve the effectiveness of the policy appraisal and evaluation.

Thus, the policy appraisal and evaluation and the proposed method can coexist. The proposed method will complement the policy appraisal and evaluation. The combination is considered to contribute to the effectiveness of the cybersecurity policy.

2.3 Benchmarking of National Cybersecurity Capacities

2.3.1 ITU Global Cybersecurity Index

In July 2017, the Cybersecurity Team of the International Telecommunication Union (ITU) investigated and announced the Global Cybersecurity Index (hereafter "GCI") 2017 as a measure of the commitment of countries to cybersecurity [11]. This is their second iteration following the GCI presented in 2014.

The GCI is a composite index that combines 25 indicators categorised into five pillars: Legal, Technical, Organizational, Capacity Building and Cooperation. Nations receive and answer the questionnaires that include 157 questions. The questionnaires are collected and scored.

The GCI 2017 top 13 nations are shown in the Table 2.3-1.

Table 2.3-1 Top 13 Nations in GCI 2017

Rank	Nation	Score
1	Singapore	0.925
2	United States of America	0.919
3	Malaysia	0.893
4	Oman	0.871
5	Estonia	0.846
6	Mauritius	0.830
7	Australia	0.824
8	Georgia	0.819
	France	0.819
10	Canada	0.818
11	Russia	0.788
12	Japan	0.786
	Norway	0.786

The GCI covers 193 ITU member states.

The questions included in the questionnaires are simple and understandable, for example:

- Is there any substantive cybercriminal law?
- Are there any articles on the unauthorized access of computers, systems and data?
- Is there any cybersecurity training for law enforcement officers, judicial and other legal actors?
- Is the training recurring?

and so on.

The questions are not considered to be comprehensive as a measurement of the national cybersecurity capacities. Also, the questions are not prioritised. Therefore, the GCI does not have the levels of cybersecurity capacities.

The GCI cannot check the national approaches. In addition, it cannot become the basis of the checking tool, because it would not check the condition 2 *"coverage"* or the condition 3 *"levels"* of the approaches.

2.3.2 Cybersecurity Capacity Maturity Model

The Global Cyber Security Capacity Centre founded around Oxford University released the Cybersecurity Capability Maturity Model v1.2 in December 2014 as the first public edition, and the Cybersecurity Capacity Maturity Model for Nations Revised Edition (hereafter "CSCMMN") in February 2017 [12, 13].

The Cybersecurity Capability/Capacity Maturity Models are aimed at assisting nations in improving their cybersecurity capacities in systematic and substantive ways.

The Global Cyber Security Capacity Centre considers cybersecurity capacity to comprise the following five 'dimensions'.

1) Devising cybersecurity policy and strategy
2) Encouraging responsible cybersecurity culture within society
3) Developing cybersecurity knowledge
4) Creating effective legal and regulatory frameworks
5) Controlling risks through standards, organisations and technologies

Each dimension is categorised into several 'factors', which are then divided into multiple 'aspects' (in the Revised Edition. It was called as 'category' in the v1.2). The Revised Edition has five dimensions, 24 factors and 53 aspects (the v1.2 had five dimensions, 20 factors and 47 categories).

The Centre also defined the five 'stages' ('levels' in the v1.2) as the degree of the progress of the nation in relation to a certain aspect of cybersecurity capacity. The five stages are 'start-up', 'formative', 'established', 'strategic' and 'dynamic', with the 'start-up' being the very first stage and the 'dynamic' being the most developed.

Each stage has 'indicators' which describe the steps, actions, or building blocks that are indicative of a specific stage of maturity within a distinct aspect. A nation must fulfil all indicators within a particular stage to advance to the next stage.

The relationship of 'dimension', 'factor', 'aspect', 'stage' and 'indicator' is shown in the Figure 2.3-1.

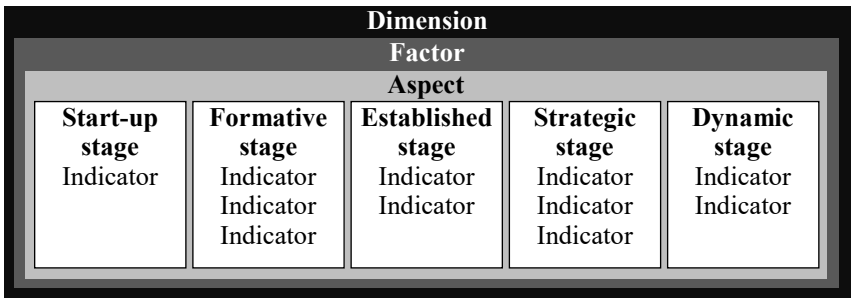


Figure 2.3-1 Relationship of Elements in CSCMMN
(Produced based on the Cybersecurity Capacity Maturity Model for Nations Revised Edition)

Uganda, Senegal, Bhutan and Kosovo had pilot assessments using the v1.2 and the official assessment of the United Kingdom was carried out with the same version [14, 15, 16, 17, 18]. Latin American and Caribbean states had assessments under the initiatives of the Organization of American States and the Inter-American Development Bank with a slightly different version from either the v1.2 or the Revised Edition [19].

Also, the nations namely, Albania, Armenia, Bangladesh, Bosnia and Herzegovina, Cyprus, Fiji, Gambia, Georgia, Ghana, Iceland, Indonesia, Kyrgyzstan, Lithuania, Macedonia, Madagascar, Montenegro, Myanmar, Samoa, Sierra Leone, Thailand, Tonga and Zambia had carried out the assessment using either the v1.2 or the Revised Edition. As of December 2018, the CSCMMs have been deployed almost 100 times according to the Global Cyber Security Capacity Centre web site [20].

The CSCMMN has more than 500 indicators in as many as 53 aspects. A lot of researchers and business people from all over the world have been involved in formulating the model. It is believed to include the cybersecurity capacities that a nation has to have comprehensively. Therefore, the CSCMMN appears to be suitable for checking the condition 2 *"coverage"* of the approaches, while it has the level (called as the 'stages' in the CSCMMN) structures and is suitable for checking the condition 3 *"levels"*.

The CSCMMN is designed for benchmarking the national cybersecurity capacities, not for checking the approaches. Therefore, it cannot be used as the method for checking the approaches, but can become the basis for the checking tool because of its characteristics that are suitable for checking the condition 2 *"coverage"* and the condition 3 *"levels"*.

2.3.3 Other Benchmarking Models

Other models for benchmarking the national cybersecurity capacities, for example, “Cyber Maturity” [21] of the Australian Strategic Policy Institute and “Cybersecurity Dashboard” [22] of the Software Alliance (BSA), are also surveyed.

There do not exist any benchmarking models that can be used for checking the approaches, nor can become the better basis for the checking tool than the CSCMMN, because the other models are simple and seem to be focusing on geographical coverage as the comparison of the national cybersecurity capacities.

2.4 Guidelines for Enterprises and Organisations

2.4.1 NIST Framework

In February 2013, President Barack Obama of the United States of America issued Executive Order (EO) 13636 “Improving Critical Infrastructure Cybersecurity”, recognising the national and economic security of the United States depends on the reliable function of critical infrastructure. The National Institute of Standards and Technology (NIST) worked with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure, based on existing standards, guidelines, and practices.

The NIST released the “Framework for Improving Critical Infrastructure Cybersecurity Version 1.0” in February 2014, which was then updated and released as Version 1.1 in April 2018 [8].

The NIST framework is composed of three parts, namely “Framework Core”, “Framework Implementation Tiers” and “Framework Profiles”.

The framework core is a set of cybersecurity activities, desired outcomes and applicable references that are common across critical infrastructure sectors, and presents industry standards, guidelines and practices. The core consists of five concurrent and continuous functions, Identify, Protect, Detect, Respond, Recover, then identifies underlying key categories and subcategories for each function.

The framework implementation tiers provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk. The tiers describe the degree to which an organisation’s cybersecurity risk management practices exhibit the characteristics defined in the framework. The tiers characterise an organisation’s practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).

A framework profile represents the outcomes based on business needs that an organisation has selected from the framework categories and subcategories. The profile can be characterised as the alignment of standards, guidelines, and practices to the framework core in a particular implementation scenario. The profiles can be used to identify opportunities for improving cybersecurity posture by comparing a “Current” profile with a “Target” profile.

The functions, categories and subcategories of the framework core are shown in the Table 2.4-1.

As shown in the Table 2.4-1, the NIST framework is a comprehensive guideline for cybersecurity capacities for enterprises and organisations, but does not cover some of the capacity areas that nations have to have, for example, the anti-cybercrime legal framework.

Table 2.4-1 Functions, Categories and Subcategories of the NIST Framework Core

Function	Category	Subcategory (98 subcategories)	
ID: Identify	ID.AM: Asset Management	ID.AM-1	Physical devices and systems within the organization are inventoried
		ID.AM-2	Software platforms and applications within the organization are inventoried
		ID.AM-3	Organizational communication and data flows are mapped
		ID.AM-4	External information systems are catalogued
		ID.AM-5	Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
	ID.BE: Business Environment	ID.BE-1	The organization's role in the supply chain is identified and communicated
		ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated
		ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated
		ID.BE-4	Dependencies and critical functions for delivery of critical services are established
		ID.BE-5	Resilience requirements to support delivery of critical services are established
	ID.GV: Governance	ID.GV-1	Organizational information security policy is established
		ID.GV-2	Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
		ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
		ID.GV-4	Governance and risk management processes address cybersecurity risks
	ID.RA: Risk Assessment	ID.RA-1	Asset vulnerabilities are identified and documented
		ID.RA-2	Threat and vulnerability information is received from information sharing forums and sources
		ID.RA-3	Threats, both internal and external, are identified and documented
		ID.RA-4	Potential business impacts and likelihoods are identified
		ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
		ID.RA-6	Risk responses are identified and prioritized
	ID.RM: Risk Management Strategy	ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders
		ID.RM-2	Organizational risk tolerance is determined and clearly expressed
		ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
PR: Protect	PR.AC: Access Control	PR.AC-1	Identities and credentials are managed for authorized devices and users
		PR.AC-2	Physical access to assets is managed and protected
		PR.AC-3	Remote access is managed
		PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate

(continue…)

Function	Category	Subcategory (98 subcategories)	
	PR.AT: Awareness and Training	PR.AT-1	All users are informed and trained
		PR.AT-2	Privileged users understand roles & responsibilities
		PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities
		PR.AT-4	Senior executives understand roles & responsibilities
		PR.AT-5	Physical and information security personnel understand roles & responsibilities
	PR.DS: Data Security	PR.DS-1	Data-at-rest is protected
		PR.DS-2	Data-in-transit is protected
		PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4	Adequate capacity to ensure availability is maintained
		PR.DS-5	Protections against data leaks are implemented
		PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
		PR.DS-7	The development and testing environment(s) are separate from the production environment
	PR.IP: Information Protection Processes and Procedures	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained
		PR.IP-2	A System Development Life Cycle to manage systems is implemented
		PR.IP-3	Configuration change control processes are in place
		PR.IP-4	Backups of information are conducted, maintained, and tested periodically
		PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met
		PR.IP-6	Data is destroyed according to policy
		PR.IP-7	Protection processes are continuously improved
		PR.IP-8	Effectiveness of protection technologies is shared with appropriate parties
		PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
		PR.IP-10	Response and recovery plans are tested
		PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
		PR.IP-12	A vulnerability management plan is developed and implemented
	PR.MA: Maintenance	PR.MA-1	Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
		PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
	PR.PT: Protective Technology	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
		PR.PT-2	Removable media is protected and its use restricted according to policy
		PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality
		PR.PT-4	Communications and control networks are protected
DE: Detect	DE.AE: Anomalies and Events	DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed
		DE.AE-2	Detected events are analyzed to understand attack targets and methods
		DE.AE-3	Event data are aggregated and correlated from multiple sources and sensors
		DE.AE-4	Impact of events is determined
		DE.AE-5	Incident alert thresholds are established

(continue…)

Function	Category	Subcategory (98 subcategories)	
	DE.CM: Security Continuous Monitoring	DE.CM-1	The network is monitored to detect potential cybersecurity events
		DE.CM-2	The physical environment is monitored to detect potential cybersecurity events
		DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events
		DE.CM-4	Malicious code is detected
		DE.CM-5	Unauthorized mobile code is detected
		DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events
		DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed
		DE.CM-8	Vulnerability scans are performed
	DE.DP: Detection Processes	DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability
		DE.DP-2	Detection activities comply with all applicable requirements
		DE.DP-3	Detection processes are tested
		DE.DP-4	Event detection information is communicated to appropriate parties
		DE.DP-5	Detection processes are continuously improved
RS: Respond	RS.RP: Response Planning	RS.RP-1	Response plan is executed during or after an event
	RS.CO: Communications	RS.CO-1	Personnel know their roles and order of operations when a response is needed
		RS.CO-2	Events are reported consistent with established criteria
		RS.CO-3	Information is shared consistent with response plans
		RS.CO-4	Coordination with stakeholders occurs consistent with response plans
		RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
	RS.AN: Analysis	RS.AN-1	Notifications from detection systems are investigated
		RS.AN-2	The impact of the incident is understood
		RS.AN-3	Forensics are performed
		RS.AN-4	Incidents are categorized consistent with response plans
	RS.MI: Mitigation	RS.MI-1	Incidents are contained
		RS.MI-2	Incidents are mitigated
		RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks
	RS.IM: Improvements	RS.IM-1	Response plans incorporate lessons learned
		RS.IM-2	Response strategies are updated
RC: Recover	RC.RP: Recovery Planning	RC.RP-1	Recovery plan is executed during or after an event
	RC.IM: Improvements	RC.IM-1	Recovery plans incorporate lessons learned
		RC.IM-2	Recovery strategies are updated
	RC.CO: Communications	RC.CO-1	Public relations are managed
		RC.CO-2	Reputation after an event is repaired
		RC.CO-3	Recovery activities are communicated to internal stakeholders and executive and management teams

2.4.2 FFIEC CAT

The Federal Financial Institutions Examination Council (FFIEC) was established in March 1979, and is a formal interagency body empowered by the five banking regulators of the United States of America to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. The five banking regulators are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB).

In light of the increasing volume and sophistication of cyber threats, the FFIEC developed the "Cybersecurity Assessment Tool" (hereafter "CAT") to help institutions identify their risks and determine their cybersecurity preparedness [23]. The CAT provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.

The CAT consists of two parts: Inherent Risk Profile and Cybersecurity Maturity.

Cybersecurity inherent risk is the level of risk posed to the institution, and incorporates the type, volume, and complexity of the institution's operations and the threats directed at the institution. Inherent risk does not include mitigating controls.

The inherent risk profile (image is shown in the Table 2.4-2) includes descriptions of activities across risk categories with definitions for the least to most levels of inherent risk, and thus helps management determine institution's exposure to risk.

The cybersecurity maturity (image is shown in the Table 2.4-3) is designed to help management measure the institution's level of risk and corresponding controls. The levels range from baseline to innovative. The cybersecurity maturity includes statements to determine whether an institution's behaviours, practices, and processes can support cybersecurity preparedness.

Once the two parts of the CAT are completed, management can evaluate whether the institution's inherent risk and preparedness are aligned. The risk/maturity relationship (shown in the Table 2.4-4) depicts the relationship between an institution's inherent risk profile and its domain maturity levels. In general, as inherent risk rises, an institution's maturity levels should increase. But there is no single expected level for an institution. An institution's inherent risk profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change. Thus, management should consider

reevaluating the institution's inherent risk profile and cybersecurity maturity periodically and when planned changes can affect its inherent risk profile.

Designed for financial institutions, the FFIEC CAT includes the components that are not applicable to the non-financial corporates or organisations, for example, automated teller machines (ATM) (category: delivery channel), issue debit or credit cards (category: online/mobile products and technology services), originating wholesale payments (e.g., CHIPS) (category: online/mobile products and technology services), and so on.

On the other hand, the CAT requires the maturity assessment after assigning the risk profile. In other words, the institutions who have higher risks need to endeavour to achieve the higher maturities. Those who have lower risks do not have to seek for the higher maturities but need to care about the basic maturities. This structure is comprehensible and efficient as a guideline.

The FFIEC CAT is not applicable to nations, because it does not cover some of the capacity areas that nations have to have, for example, the anti-cybercrime legal framework.

Table 2.4-2 Image of Inherent Risk Profile

	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Category: Technologies and Connection Types					
Wholesale customers with dedicated connections					
Internally hosted and developed or modified vendor applications supporting critical activities					
Internally hosted, vendor-developed applications supporting critical activities					
User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools)					
End-of-life (EOL) systems					
Open Source Software (OSS)					
Network devices (e.g., servers, routers, and firewalls; include physical and virtual)					
Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)					
Cloud computing services hosted externally to support critical activities					
Category: Delivery Channels					
Online presence (customer)					
Mobile presence					
Automated Teller Machines (ATM) (Operation)					
Category: Online/Mobile Products and Technology Services					
Issue debit or credit cards					
Prepaid cards					
Emerging payments technologies (e.g., digital wallets, mobile wallets)					
Person-to-person payments (P2P)					
Originating ACH payments					
Originating wholesale payments (e.g., CHIPS)					
Wire transfers					
Merchant remote deposit capture (RDC)					
Global remittances					
Treasury services and clients					
Trust services					
Act as a correspondent bank (Interbank transfers)					
Merchant acquirer (sponsor merchants or card processor activity into the payment system)					
Host IT services for other organizations (either through joint systems or administrative support)					

Descriptions

(continue…)

	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Category: Organizational Characteristics					
Mergers and acquisitions (including divestitures and joint ventures)					
Direct employees (including information technology and cybersecurity contractors)					
Changes in IT and information security staffing					
Privileged access (Administrators–network, database, applications, systems, etc.)					
Changes in IT environment (e.g., network, infrastructure, critical applications, technologies supporting new products or services)					
Locations of branches/business presence					
Locations of operations/data centers					
Category: External Threats					
Attempted cyber attacks					
Number of statements selected in each risk level					
Based on individual risk levels selected, assign an inherent risk profile	Least	Minimal	Moderate	Significant	Most

Table 2.4-3 Image of Cybersecurity Maturity

Domain		Assessment Factor	Component	Maturity Level				
				Baseline	Evolving	Intermediate	Advanced	Innovative
1	Cyber Risk Management and Oversight	Governance	Oversight					
			Strategy/Policies					
			IT Asset Management					
		Risk Management	Risk Management Program					
			Risk Assessment					
			Audit					
		Resources	Staffing					
			Training					
			Culture					
2	Threat Intelligence and Collaboration	Threat Intelligence	Threat Intelligence and Information					
		Monitoring and Analyzing	Monitoring and Analyzing					
		Information Sharing	Information Sharing					
3	Cybersecurity Controls	Preventative Controls	Infrastructure Management					
			Access and Data Management					
			Device/Endpoint Security					
			Secure Coding					
		Detective Controls	Threat and Vulnerability Detection					
			Anomalous Activity Detection					
			Event Detection					
		Corrective Controls	Patch Management					
			Remediation					
4	External Dependency Management	Connections	Connections					
		Relationship Management	Due Diligence					
			Contracts					
			Ongoing Monitoring					
5	Cyber Incident Management and Resilience	Incident Resilience Planning and Strategy	Planning					
			Testing					
		Detection, Response, and Mitigation	Detection					
			Response and Mitigation					
		Escalation and Reporting	Escalation and Reporting					

Descriptions

Table 2.4-4 Risk/Maturity Relationship

		Inherent Risk Levels →				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Domain ↑	Innovative					
	Advanced					
	Intermediate					
	Evolving					
	Baseline					

2.4.3 Other Guidelines for Enterprises and Organisations

There exist a lot of cybersecurity guidelines designed for enterprises and organisations, for example, “ISO/IEC 27032:2012” [24], “Cybersecurity Management Guidelines” [25] co-developed by the Ministry of Economy, Trade and Industry of Japan and the Independent Administrative Agency Information-technology Promotion Agency, and so on. However, they are designed for enterprises and organisations as well as for individuals, and are not suitable for nations.

2.5 Guidelines for Software Development Process

2.5.1 CMMI for Development

The “Capability Maturity Model Integration” (hereafter “CMMI”) is a process improvement training and appraisal program [26]. It was originally developed by Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) and is now developed by the CMMI project, which consists of members of industry, public sector and SEI. The CMMI is required by many United States Government contracts especially in software development.

Mary Beth Chrissis, Mike Konrad and Sandy Shrum, who are the authors of “CMMI for Development: Guidelines for Process Integration and Product Improvement” [27], have stated in their book that we live in a world where technology is changing at an incredible speed. To deal with such a world and to maximize the productivity, we need to focus on process. Many organizations in manufacturing and service industries now recognize the importance of quality processes in addition to the process effectiveness and efficiency. Process helps an organization’s workforce to work smarter, not harder, and with improved consistency. Effective processes also provide a vehicle for introducing and using new technology in a way that best meets the business objectives of the organization.

The CMMI defines 22 process areas and five maturity levels. The process areas are classified into four categories. Each process area is determined what maturity level it is required. For the highest maturity level, all process areas must be satisfied.

The maturity levels are characterised as follows, which draw the property of the CMMI well.

1) Level 1 Initial: Processes unpredictable, poorly controlled and reactive.
2) Level 2 Managed: Processes characterized for projects and is often reactive.
3) Level 3 Defined: Processes characterized for the organization and is proactive.
4) Level 4 Quantitatively Managed: Processes measured and controlled.
5) Level 5 Optimizing: Focus on process improvement

The process areas and the maturity levels that each area must be satisfied are shown in the Table 2.5-1.

Table 2.5-1 The Process Areas of the CMMI

#	Process Area	Category	Maturity Level					
				Initial	Managed	Defined	Quantitatively Managed	Optimizing
1	Casual Analysis and Resolution (CAR)	Support	5					x
2	Configuration Management (CM)	Support	2		x	x	x	x
3	Decision Analysis and Resolution (DAR)	Support	3			x	x	x
4	Integrated Project Management (IPM)	Project Management	3			x	x	x
5	Measurement and Analysis (MA)	Support	2		x	x	x	x
6	Organizational Process Definition (OPD)	Process Management	3			x	x	x
7	Organizational Process Focus (OPF)	Process Management	3			x	x	x
8	Organizational Performance Management (OPM)	Process Management	5					x
9	Organizational Process Performance (OPP)	Process Management	4				x	x
10	Organizational Training (OT)	Process Management	3			x	x	x
11	Product Integration (PI)	Engineering	3			x	x	x
12	Project Monitoring and Control (PMC)	Project Management	2		x	x	x	x
13	Project Planning (PP)	Project Management	2		x	x	x	x
14	Process and Product Quality Assurance (PPQA)	Support	2		x	x	x	x
15	Quantitative Project Management (QPM)	Project Management	4				x	x
16	Requirements Development (RD)	Engineering	3			x	x	x
17	Requirements Management (REQM)	Project Management	2		x	x	x	x
18	Risk Management (RSKM)	Project Management	3			x	x	x
19	Supplier Agreement Management (SAM)	Project Management	2		x	x	x	x
20	Technical Solution (TS)	Engineering	3			x	x	x
21	Validation (VAL)	Engineering	3			x	x	x
22	Verification (VER)	Engineering	3			x	x	x

Note: “x” denotes that the process area is required in the maturity level.

2.5.2 Capability Levels and Maturity Levels in CMMI

The CMMI for development defines two representations; the continuous representation and the staged representation [27].

The continuous representation is used by an organisation to improve processes corresponding to an individual process area (or group of process areas), while the staged representation is used to improve a set of related processes. The continuous representation enables the organisation to achieve “capability levels”. The staged representation enables to achieve “maturity levels”. In other words, the capability levels apply to achievement of an organisation’s process improvement in individual process areas, and the maturity levels apply to achievement of an organisation’s process improvement across multiple process areas.

The definition of the capability levels is different from that of the maturity levels mentioned in the 2.5.1. The comparison of the two definitions is shown in the Table 2.5-2.

Table 2.5-2 Comparison of Definitions of Levels

Level	Capability Levels (Continuous Representation)	Maturity Levels (Staged Representation)
Level 0	Incomplete	-
Level 1	Performed	Initial
Level 2	Managed	Managed
Level 3	Defined	Defined
Level 4	-	Quantitatively Managed
Level 5	-	Optimizing

It is notable that there do not exist the level 4 or 5 in the capability levels. This means that there is no point in improving the capability in an individual process area higher than the level 3. Instead, an organisation that wants to improve its processes higher than the level 3 needs to aim at achieving the maturity levels. In other words, an organisation can pay efforts on improving its capability until it reaches a certain level of capability, but after that it must focus on improving its maturity.

Another notable characteristic of the maturity levels is that the definition of the level 5 is not “optimized” but “optimizing”. It insists that there is no perfection of the processes and the processes must be improved everlastingly. In other words, improvement of the capability transforms into improvement of the maturity, and the maturity means the capability to improve its capabilities as a whole. In the most matured stage, the capabilities optimise autonomously and everlastingly.

When it is put into the case of cybersecurity capacity, a nation enhances its cybersecurity capacity but it also has to consider cultivating the ability to improve

its capacities autonomously. It is very important because the very fast development of information technology and cyber-attackers' skills do not allow a nation to evaluate the effectiveness of the capacities one year and implement other approaches to enhance the inferior capacities the following year. A nation must enhance the capacities immediately after they notice that the current capacities are left behind the latest technology and skills. This means an autonomous evaluation-enhancement process must be built-in into the capacities. Therefore, when the national cybersecurity capacities are evaluated, the existence of an autonomous enhancement mechanism must be checked.

The fact that a nation must enhance the capacities immediately after they notice corresponds to the condition 1 *"velocity"*. Therefore, the checklist will have functionality to check the condition 1 *"velocity"* by incorporating the items to check the autonomous enhancement mechanism.

2.6 Conclusion of Survey of Related Researches

Firstly, it has been ascertained that the policy appraisal and evaluation do not find out the approaches that have not come up for discussion. Therefore, the policy appraisal and evaluation are not suitable for checking if the approaches satisfy the condition 2 *"coverage"*. Therefore, a complementary checking method is needed. Besides, the policy appraisal and evaluation are supposed to be good at checking the condition 4 *"efficiency"*, and, therefore, the proposed method will be able to check the condition 4 *"efficiency"* more effectively when it is combined with the policy appraisal and evaluation.

Secondly, the attempts to benchmark the national cybersecurity capacities are not suitable for checking the approaches, as they are designed to measure the capacities. However, it was revealed that the CSCMMN developed by the Global Cyber Security Capacity Centre has a comprehensive coverage of the cybersecurity capacity areas that a nation has to have, and shows the levels that help nations to develop the capacities in step by step manner. It means that the CSCMMN has the characteristics to check the conditions 2 *"coverage"* and 3 *"levels"*, and can become the basis for the checking tool when the method and the tool have to be created.

Thirdly, the guidelines that are intended for the use by enterprises and organisations to enhance their cybersecurity capacities were surveyed. It was discovered that they are not suitable for nations because they do not include some capacity areas that are necessary for nations, for example, the capacities of law enforcement or legal framework. In other words, such guidelines are not suitable for checking the condition 2 *"coverage"*.

Finally, the survey of the CMMI for development revealed that the cybersecurity capacities must include the abilities to autonomously enhance its capacities according to

the recognition of the environment. The checklist will be able to check the condition 1 *"velocity"* by incorporating the items to check the existence of the autonomous enhancement mechanism

Thus, the survey of the related researches indicated that the method and the tool to check the approaches for the national cybersecurity capacity enhancement have to be created and can be designed to check all four conditions by the following courses.

Condition 1 *"velocity"*: the checklist should have the items to check the existence of the autonomous enhancement mechanism.

Condition 2 *"coverage"*: the checklist should be based on the CSCMMN which has the comprehensive coverage of the capacity areas that are necessary for nations.

Condition 3 *"levels"*: the checklist should define the capacity levels based on the 'stages' defined in the CSCMMN.

Condition 4 *"efficiency"*: the result of the check using the method should be informed to the policy appraisal and evaluation for more effective appraisal/evaluation.

The proposal that realises the above-mentioned is introduced in **Chapter 3. Proposal**.

Chapter 3. Proposal

3.1 Introduction

As stated in **Chapter 1. Introduction**, the approaches for national cybersecurity capacity enhancement must be checked if they are satisfying the four conditions. However, as mentioned in **Chapter 2. Related Researches**, there is no existing method or tool for that purpose at present.

Therefore, in this research, a method and a tool to check the approaches for the national cybersecurity capacity enhancement are proposed.

The method is called "ANC3M" (Approaches for National Cybersecurity Capacity enhancement Checking Method).

The tool is called "ANC3T" (Approaches for National Cybersecurity Capacity enhancement Checking Tool).

In addition, creation of a database of the approaches that are categorised and classified by the method/tool is proposed.

The database is called "ANC3DB" (Approaches for National Cybersecurity Capacity enhancement Checked DataBase).

The ANC3DB is supposed to provide with the functionality of transnational analyses of cybersecurity approaches.

3.2 Method

3.2.1 Outline of the Method (ANC3M)

The basic flow of the method is shown below.

1) Collection: All approaches of a nation for national cybersecurity capacity enhancement are collected.
2) Itemisation: The approaches are itemised into pieces of action items.
3) Mapping: The action items are mapped onto the tool (ANC3T).
4) Evaluation: The mapping result is evaluated.

Each process is described in the following sections.

3.2.2 Collection

It is desirable that all approaches that are related to enhancement of the national cybersecurity capacity are collected. If not, the checking result will be compromised. For example, even if the result reveals that the approaches are not satisfying the condition 2 *"coverage"*, i.e., enough approaches are not planned in

some capacity areas, if there exist some uncollected approaches, it will be unable to judge.

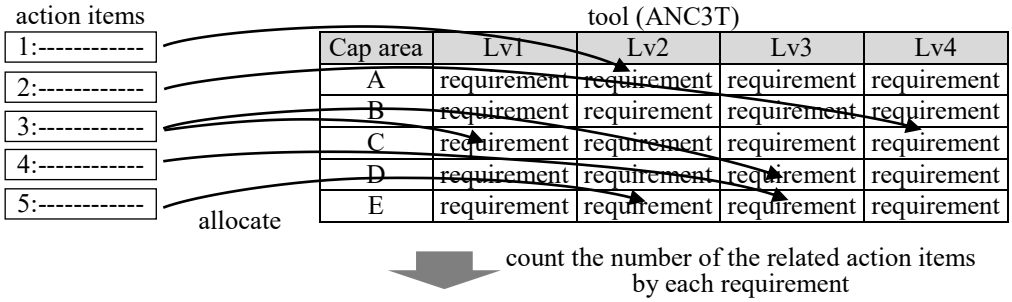
3.2.3 Itemisation

If a collected approach includes two or more actions, it must be split into several actions as the preparation for the following step. These separated actions are called “action items” in this research. Each action item must have one single action. An approach that has one single action will be called “action item” as it is.

3.2.4 Mapping

“Mapping” in this research means allocating the action items onto the tool (ANC3T). The tool, the details of which will be described in section 3.3, is basically the list of the requirements which are categorised by the cybersecurity capacity areas and classified by the capacity levels. In order to allocate an action item onto the tool, it is necessary to identify the requirement(s) that the action item will fulfil or contribute toward fulfilling. When an action item will fulfil or contribute toward fulfilling a requirement, the action item is said to be “related” to the requirement in this research. An action item is not necessarily related to a single requirement, but to two or more requirements.

Once all action items are allocated onto the tool, the number of the related action items are counted by each requirement to obtain the mapped result.
The process of mapping is drawn in the Figure 3.2-1.



Cap area	Lv1	Lv2	Lv3	Lv4
A	0 related action items	2 related action items	1 related action items	3 related action items
B	1 related action items	0 related action items	2 related action items	0 related action items
C	0 related action items	1 related action items	0 related action items	2 related action items
D	2 related action items	3 related action items	5 related action items	1 related action items
E	1 related action items	2 related action items	1 related action items	0 related action items

Note: Cap area = capacity area, Lv = level.

Figure 3.2-1 Process of Mapping

3.2.5 Evaluation

The purpose of evaluation of the mapping result is to see whether the approaches are satisfying the four conditions.

Among the four conditions, the condition 1 *"velocity"* is checked by examining the number of the action items related to the requirements for the autonomous enhancement mechanism, while the other conditions are checked by finding out the capacity areas that may not satisfy the conditions.

3.2.5.1 Evaluation for Condition 1

As mentioned in section 2.6, the condition 1 *"velocity"* is checked by the requirements for the autonomous enhancement mechanism.

Among the requirements described in the ANC3T, some requirements refer to the capacities with the built-in autonomous enhancement mechanism. Such capacities enable a nation to enhance its capacities according to the changes in cybersecurity environments and the threat landscape without being instructed to do so by the outside organs. Without such capacities, a nation cannot enhance its capacities at the same velocity as information technology and the opponents develop, i.e. fails satisfying the condition 1 *"velocity"*.

There are 58 requirements that include the autonomous enhancement mechanism in the ANC3T. The details of the requirements are introduced in section 3.3.4.

To help checking if the nation satisfies the condition 1 *"velocity"*, the method counts the number of the action items related to the requirements for the autonomous enhancement mechanism. It indicates whether the nation is planning to obtain such capacity in a particular capacity area. However, it is not learned from this analysis whether the nation has such capacities. Likewise, if no action item is related to a particular requirement for the autonomous enhancement mechanism, it does not mean that the nation is not concerned about obtaining the capacity, as the nation may already has the capacity.

Furthermore, if the nation has only a primitive capacity in a particular capacity area, the nation should concentrate to enhance the capacity to the higher level, rather than try to obtain the autonomous enhancement mechanism.

Thus, the evaluation for the condition 1 *"velocity"* only tells that the nation plans to obtain the autonomous enhancement mechanism, and cannot give definitive verdicts. However, it is supposed to help checking

the condition 1, because the nation can ensure that it satisfies the condition 1 by examining if the result is along with its cybersecurity strategy.

3.2.5.2 Evaluation for Condition 2, 3, 4

The condition 2 *"coverage"*, 3 *"levels"* and 4 *"efficiency"* are checked by finding out the capacity areas that have the following characteristics.

1) The areas that few action items are related to.
2) The areas where the action items are related only to the lower levels.
3) The areas where the action items are related only to the higher levels.
4) The areas that a lot of action items are related to.

The areas that few action items are related to are the capacity areas that are not planned to be enhanced. It means that the nation has already high level of capacities in those areas, or otherwise the areas are to be left unenhanced by some reasons. There may be necessary to have further examination in those areas. This helps checking if the nation satisfies the condition 2 *"coverage"*.

The areas where the action items are related only to the lower levels are the capacity areas that are planned to be maintained at the lower levels or to be enhanced from the very low levels. It means that the nation only has low level of capacities but does not intend to enhance to the higher levels in those areas. It is alright if the nation does not have to obtain the high level of capacities in those areas by some reasons, for examples, the nation relies on other nations in those capacities. There may be necessary to have further examination in those areas. This helps checking if the nation satisfies the condition 3 *"levels"*.

The areas where the action items are related only to the higher levels are the capacity areas that are planned to be aimed at the very high levels. It is alright if the nation already has the high level of capacities in those areas and intends to have the higher levels of capacities. However, if the nation does not have enough capacities in the more fundamental levels, the capacities may not effectively mitigate the cyber threats. There may be necessary to have further examination in those areas. This helps checking if the nation satisfies the condition 3 *"levels"* and possibly the condition 2 *"coverage"* as well.

The areas that a lot of action items are related to are the capacity areas that are planned to be enhanced by executing a lot of approaches. It means that the nation is emphasising to obtain the capacities in those areas. It is alright if that is consistent with its cybersecurity strategy. However, it is possible that the nation has a lot of legacy activities that are not easily canceled by some reasons. There may be necessary to have further examination in those areas. Or, the areas may have to be applied the policy appraisal and evaluation intensely for more effective and efficient appraisal/evaluation. Thus, this helps checking if the nation satisfies the condition 4 *"efficiency"*.

Each characteristic is abbreviated in this research as follows;

1) The case 2 *"few"*
2) The case 3 *"low"*
3) The case 4 *"high"*
4) The case 5 *"a lot"*

Please note that the case 1 denotes the evaluation for the condition 1.

The examples are shown in the Figure 3.2-2.

Mapping Result (number of related action items)

Capacity area	Level 1	Level 2	Level 3	Level 4	
A	0	1	0	0	← *"Few"*
B	1	4	5	2	
C	10	8	0	0	← *"Low"*
D	0	3	4	3	
E	0	0	1	8	← *"High"*
F	2	5	6	3	
G	10	15	8	6	← *"A lot"*

Figure 3.2-2 Examples of Evaluation

It is difficult to define the thresholds for judging *"few"* or *"a lot"*. For example, in the case of *"few"* in the Figure 3.2-2, is one related action item few? If that is zero, it is definitely few. How about two or three? The thresholds differ according to the number of the total action items. Similarly, how many action items can be said a lot?

It's been decided not to define the distinct thresholds. As mentioned earlier, the findings do not immediately mean dissatisfactory of the conditions, and will require the further examination of the approaches. Therefore, the thresholds can be decided by the checker depending on how many capacity areas he/she wants to indicate for the further examinations.

3.3 Tool

3.3.1 Prerequisites of the Tool (ANC3T)

The tool (ANC3T) is basically the list of the requirements which are categorised by the cybersecurity capacity areas and classified by the capacity levels.

Moreover, the tool must have the following characteristics.

1) The tool must have the comprehensive coverage of the cybersecurity capacity areas that a nation has to have. (hereafter 'prerequisite 1 *"coverage"*')
2) The tool must indicate several levels in each capacity area that a nation can plan to achieve in a step by step manner. (hereafter 'prerequisite 2 *"levels"*')
3) The tool must be updated regularly according to the development of information technology and cyber-attacking technology. (hereafter 'prerequisite 3 *"updates"*')
4) The tool must include the items that require nation's maturity to sustain high level of capacities by the autonomous enhancement mechanism. (hereafter 'prerequisite 4 *"autonomy"*')

The prerequisite 1 *"coverage"* corresponds to the condition 2 *"coverage"*. The prerequisite 2 *"levels"* corresponds to the condition 3 *"levels"*. The prerequisite 4 *"autonomy"* corresponds to the condition 1 *"velocity"*.

It is obvious that the prerequisite 3 *"updates"* of the tool itself is required considering rapid development of information technology, skills of attackers and the capacities of other nations.

3.3.2 Outline of the Tool (ANC3T)

The outline of the tool is shown in the Table 3.3-1.

Table 3.3-1 Outline of the Tool (ANC3T)

#	Category	Sub-category	Capacity area	Level 1		Level 2		Level 3		Level 4	
111	a	z	A	111L1-1	req't	111L2-1	req't	111L3-1	req't	111L4-1	req't
				-	-	111L2-2	req't	111L3-2	req't	111L4-2	req't
112			B	112L1-1	req't	112L2-1	req't	112L3-1	req't	112L4-1	req't
				112L1-2	req't	-	-	112L3-2	req't	-	-
121		y	C	121L1-1	req't	121L2-1	req't	121L3-1	req't	121L4-1	req't
				-	-	121L2-2	req't	121L3-2	req't	121L4-2	req't
				-	-	121L2-3	req't	-	-	121L4-3	req't
211	b	x	D	211L1-1	req't	211L2-1	req't	211L3-1	req't	211L4-1	req't
				211L1-2	req't	211L2-2	req't	211L3-2	req't	-	-
				-	-	211L2-3	req't	211L3-3	req't	-	-

Note: req't = requirement

The “capacity areas” are supposed to cover the necessary cybersecurity capacity areas that a nation has to have comprehensively. The capacity areas are categorised and subcategorised for easier reference. Then each area is numbered such as “111”, “112”, “113”, ….

The number of levels is four, mainly because the CSCMMN which the tool is based on has five levels. Please note that the tool is assuming that there exists the level 0 and the requirements of the level 1 mean stepping up from the level 0 to the level 1.

The requirement for a level in an area is not necessarily one. There may be two or more requirements. Then the requirements are numbered such as “111L1-1”, “111L1-2”, “111L2-1”, …. which stand for “capacity area number, level number - order within the level/area”.

3.3.3 Deriving from CSCMMN

As mentioned in section 2.6, the tool (ANC3T) is created based on the CSCMMN [13].

The CSCMMN (Cybersecurity Capacity Maturity Model for Nations Revised Edition) has the following characteristics.

1) CSCMMN was developed by a lot of researchers and business people from all over the world and aiming at covering the comprehensive cybersecurity capacity areas that a nation has to have. (satisfying the prerequisite 1 *“coverage”*)
2) CSCMMN indicates the levels that a nation can plan to advance toward. (satisfying the prerequisite 2 *“levels”*)
3) CSCMMN has already been updated once and is expected to be updated regularly in accordance with changes in the field of cybersecurity. (satisfying the prerequisite 3 *“updates”*)
4) CSCMMN requires a nation such maturities that it advances its capacities autonomously and continuously in the higher stages. For example, the indicators in the ‘strategic’ (2nd highest) stage for the ‘strategy development’ aspect of the ‘national cybersecurity strategy’ factor of the 1st dimension require that the reviewing process of the strategy is defined. There exist 58 indicators that require the autonomous enhancement mechanism in the CSCMMN. (satisfying the prerequisite 4 *“autonomy”*)

The CSCMMN is able to satisfy all four prerequisites described in section 3.3.1. Therefore, the CSCMMN is used as a base of the ANC3T and the names of the elements are replaced as in the Figure 3.3-1.

CSCMMN
Dimension
Factor
Aspect
Stage
Start-up
Formative
Established
Strategic
Dynamic
Indicator

AC3T
Category
Subcategory
Capacity area
Level
n/a (supposed as Level 0)
Level 1
Level 2
Level 3
Level 4
Requirement

CSCMMN

Dimension	Factor	Aspect	Stage				
			Start-up	Formative	Established	Strategic	Dynamic
			Indicator(s)	Indicator(s)	Indicator(s)	Indicator(s)	Indicator(s)

ANC3T

Category	Subcategory	Capacity area	Level			
			Level 1	Level 2	Level 3	Level 4
			Requirement(s)	Requirement(s)	Requirement(s)	Requirement(s)

Figure 3.3-1 Replacement of Names of Elements

The indicators of the CSCMMN are described literarily. An indicator usually denotes a single condition, but some indicators include two or more conditions. A requirement must denote one single condition. Therefore, such indicators have been split into two or more requirements in the process of transforming the CSCMMN into the ANC3T.

3.3.4 Requirements for Autonomous Enhancement Mechanism

As mentioned in section 3.3.3, the CSCMMN has 58 indicators that require the autonomous enhancement mechanism, which then become the requirements for autonomous enhancement mechanism in the ANC3T.

The list of the requirements for autonomous enhancement mechanism is shown in the Table 3.3-2.

Table 3.3-2 List of Requirements for Autonomous Enhancement Mechanism

ID	Keywords	Details
111L4-1	Continual revision of strategy	Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments.
112L3-1	PDCA processes of cybersecurity programme	Evidence exists of iterative application of metrics and resulting refinements to operations and strategy across government, including resource allocation considerations.
112L4-1	Reassignment & reallocation of resources for cybersecurity programme	A singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically according to changing risk assessments.
113L4-1	Continual revision of strategy	New content is periodically incorporated in the strategy in response to evolving threat landscapes.
121L3-1	Regular revision of incident registry	Regular, systematic updates to the national-level incident registry are made.
124L3-3	Regular review of incident response processes	Key processes (detection, resolution, prevention, etc.) are being monitored and reviewed in regular basis, and tested with different case scenarios.
124L4-2	Evaluating effectiveness of CSIRT members training	The benefits of training and accreditation are being evaluated and inform the future training planning.
131L4-1	Regular review of CI risk priorities	Priority listing of CI assets is regularly re-appraised to capture changes in the threat environment.
132L4-1	Ability to adjust of CI protection	Owners of critical infrastructure and assets are able to rapidly respond to the changing threat landscape.
133L3-4	Regular review of resource allocation for CI protection	Resources are allocated in proportion to the assessed impact of an incident to ensure rapid and effective incident response.
133L4-1	Regular audit of CI	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of CI risk portfolio, technologies, policies and processes.
141L3-4	Evaluation of national incident exercise informing investment	(Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance key indicators (PKI) inform decisions in crisis management,) and evaluation results inform future investment in national cybersecurity capacity.
161L3-3	Evaluation of national incident exercise informing investment	The results of these scenarios then inform strategic investment in future emergency response assets.
221L4-1	Users can evaluate risk & adjust behaviour	Individuals assess the risk in using online services, including changes in the technical and cybersecurity environment and continuously adjust their behaviour based on this assessment.
222L4-1	Promotion of e-gov revised	E-government services and promotion thereof are continuously improved and expanded to enhance transparent/open and secure systems and user trust.
223L4-1	Continuous improvement of e-commerce	E-commerce services are continuously improved in order to promote transparent, trustworthy and secure systems.
231L4-1	Users can adapt to changing environments	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment.
231L4-3	Security & privacy balanced in changing environment	Policies are in place in private and public sectors to ensure that privacy and security are not competing in a changing environment and are informed by user feedback and public debate.
231L4-4	Regular assessment of privacy protection	Assessments of personal information protection in eservices are regularly conducted and feed back into policy revision.
241L4-1	Regular enhancement of incident reporting	All relevant stakeholders actively collaborate and share good practice to enhance existing reporting mechanisms and there is a clear distribution of roles and responsibilities, including regarding the response to reported incidents.
251L4-1	Discussion changing policy & society	The broad discussion of personal experiences and personal attitudes of individuals across mainstream and social media inform policy making and facilitate societal change.
311L4-1	Awareness raising programmes adapted according to effectiveness	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments.

(continue…)

ID	Keywords	Details
311L4-2	Revision of national awareness raising programme	Metrics contribute toward national cybersecurity strategy revision processes.
312L3-2	Executives' ability to reallocate resources	Executives are able to alter strategic decision making, and allocate specific funding and people to the various elements of cyber risk, contingent on their company's prevailing situation.
321L4-3	Cybersecurity education adapting to changing needs	Prevailing cybersecurity requirements are considered in the redevelopment of all general curricula.
322L4-3	Cybersecurity education aligned with practical problems	Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges, and provides a mechanism for enhancing curriculum based on the evolving landscape.
331L3-4	Metrics of effectiveness of cybersecurity training	Metrics of effectiveness assess the modes and procedures of training.
332L3-1	Review of cybersecurity training programmes	The uptake of cybersecurity training is used to inform future training programmes.
411L3-1	Regular review of cybersecurity legal framework	The country reviews existing legal and regulatory mechanisms for ICT security, identifies where gaps and overlaps exist, and amends laws accordingly or enacts new laws.
411L4-1	Balance between cybersecurity legal framework & best practices	Mechanisms are in place for continuously harmonising ICT legal frameworks with national cybersecurity related ICT policies, international law, standards and good practices.
412L4-1	Amendment procedures for cybersecurity legal framework	In order to meet dynamic changes in the application of technology to human rights, procedures are in place to amend and update legal frameworks as needed.
413L4-1	Amendment procedures for data protection legislation	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
414L4-1	Amendment procedures for online child protection legislation	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
415L4-1	Amendment procedures for consumer protection legislation	In order to meet dynamic changes in the application of technology to consumer protection, procedures are in place to amend and update legal frameworks as needed.
416L4-1	Balance between intellectual property & open access policy	Decisions to update legislation are based on the balance between intellectual property and open access policies, through multi-stakeholder discussion.
417L4-2	Regular review of substantive cybercrime legislation	Laws, where needed, are amended to reflect changes in the international ICT environment.
418L4-2	Regular review of procedural cybercrime legislation	Procedural law, where needed, is amended to adapt to the changing cybercrime landscape and emerging investigative challenges.
421L4-3	Regular review of investigative capabilities for cybercrimes	The institutional capacity of law enforcement is frequently reviewed and revised based on an assessment of effectiveness.
422L3-3	Exchange of best practices between prosecutors & judges	A mechanism exists that enables the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.
422L4-3	Specialised and continuous training for prosecutors	All prosecutors receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
423L4-1	Specialised and continuous training for judges	Judges receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
423L4-2	Regular review of court system capabilities to judge cybercrimes	The institutional capacity of the court system is frequently reviewed and revised based on an assessment of effectiveness.
431L4-1	Regular review of international cooperation	Formal international cooperation mechanisms are regularly reviewed to determine effectiveness, and are revised accordingly to reflect the changing cybercrime landscape.
431L4-3	Regularly adjusted information exchange between public & private sectors	Formal mechanisms that enable the exchange of information between domestic public and private sectors are adapted in accordance with identified needs and changing threat environment.

(continue…)

ID	Keywords	Details
432L4-1	Adapted cooperation & exchange of information	Government and criminal justice actors exchange information timely and efficiently, and cooperation is adapted to the changing cybercrime environment and associated requirements.
432L4-2	Adapted international cooperation	A routinized relationship between law enforcement and ISPs, domestically and across borders, has been established and is adaptable to emerging forms of cybercrime.
511L4-1	Regular review of adoption of standards & best practices	The choice of adopted standards and good practices and their implementation is continuously improved.
511L4-2	Decision making of non-compliance to standards & best practices	Adoption of standards and non-compliance decisions are made in response to changing threat environments and resource drivers across sectors and CI through collaborative risk management.
511L4-3	Risk-based decision making of compliance	Evidence exists of debate within all sectors on compliance to standards and good practices, based on continuous needs assessments.
512L3-2	Regular review of procurement	Critical aspects of procurement and supply, such as prices and costs, quality, timescales and other value adding activities are continuously improved,
521L4-1	Controlled acquisition of infrastructures	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics.
521L4-2	Optimised cost for internet infrastructures	Costs for infrastructure technologies are continually assessed and optimised.
531L4-3	Regular review of quality requirement	Requirements of software quality are being systematically reviewed, updated, and adapted to the changing cybersecurity environment.
541L4-1	Continuous assess of technical security controls	All sectors have the capacity to continuously assess the security controls deployed for their effectiveness and suitability according to their changing needs.
551L4-1	Regular review of relevance of cryptographic controls	The relevance of cryptographic controls deployed for securing data at rest and data in transit is continuously assessed through risk assessments.
551L4-2	Revision of cryptographic control policies	The public and private sector adapt encryption and cryptographic control policies based on the evolution of technological advancement and changing threat environment.
571L4-1	Regular review of vulnerability disclosure policies	Responsible disclosure policies are continuously reviewed and updated based on the needs of all affected stakeholders.
571L4-4	Reviewing process of deadlines	Processes are in place to review and reduce deadlines.

3.3.5 Enhancement over CSCMMN

Although the CSCMMN is supposed to cover the necessary cybersecurity capacity areas that a nation has to have comprehensively, it was found that some capacities are not included in the CSCMMN but are supposed to be important for a nation to have, through the verification of the method/tool.

Those capacities are the counter-intelligence capacity and the capacity to support the neighbouring nations for establishing legislative frameworks. In fact, Japan actually works on those capacities. Therefore, it was decided that the capacities are to be included into the ANC3T, the details of which are introduced in section 4.3.3.6.

3.4 Database

3.4.1 Outline of the Database (ANC3DB)

When the approaches are checked by the ANC3M, the approaches (more precisely, action items) are categorised and classified. In other words, each action item is tagged with category, subcategory, capacity area and level. In addition, some action items are tagged with two or more categories/subcategories/capacity areas/levels. Through the verification, more than 250 action items of Japan and 140 action items of the United Kingdom were tagged. The total number of the relationship is more than 850.

This is a fairly large data set of the approaches that are aimed at enhancing the national cybersecurity capacities. If the further examples of the approaches of other nations are collected and input into the data set, the data set will be supposed to provide with a platform for the cross-border analyses of the cybersecurity approaches.

3.4.2 Purposes

This database (ANC3DB) is supposed to be useful in the following occasions.

4) When a nation plans to enhance some particular capacities, the ANC3DB can provide with the examples of the approaches that are implemented by other nations.
5) When a nation considers another nation as a role model, the ANC3DB can provide with the examples that are implemented by the model nation.
6) The ANC3DB can provide with the functionality for statistical analysis, for example;
    e) What capacity areas are emphasised on a global basis?
    f) What levels are intensely aimed at on a global basis?
    g) Are the emphasised areas shifting according to the lapse of time?
    h) Are the aimed levels rising?

    and so on.

3.4.2 Details

The database (ANC3DB) consists of the aggregate of the approaches (action items) for the national cybersecurity capacity enhancement that are related to the requirements of the ANC3T. A datum consists of a relationship, in other words, a combination of an action item and a requirement.

The images of the ANC3DB tables are shown in the Figure 3.4-1.

Relationship		
Ref. #	Action item #	Requirement ID

Action items (Approaches)					
Action item #	Nation	National #	Source	Year	Details

ANC3T					
Requirement ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)

Figure 3.4-1 Image of the ANC3DB Tables

3.4.4 Data Collection

The examples of the approaches of other nations are not necessarily to be collected as a complete set of the national approaches, as mentioned in the collection process of the method. Instead, they can be collected one by one. For example, if nation A announces to increase its budget for research and development of cybersecurity technology, it can be input into the database. When nation B decides to have the application of an international standard for cybersecurity mandatory to the listed companies, it can be input into the database. Thus, the database will gradually grow and will be more useful.

It is almost obvious that the more examples are added to the database, the more the database will be useful. Therefore, it was decided to add fairly good amount of data as a short-term solution by using the recommendations for cybersecurity enhancement published by the Commission on Enhancing National Cybersecurity of the United States.

The former President Barack Obama of the United States issued the Executive Order 13718 in February 2016, ordering to form the Commission on Enhancing National Cybersecurity and to develop a plan for protecting cyberspace and America's economic reliance on it [28]. The Commission was formed by the eminent experts in April and reported the recommendations in December 2016.

The report made 16 major recommendations with 53 specific action items broadly grouped under the following six areas [29].

1) Protect, defend, and secure today’s information infrastructure and digital networks.

2) Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3) Prepare consumers to thrive in a digital age.
4) Build cybersecurity workforce capabilities.
5) Better equip Government to function effectively and securely in the digital age.
6) Ensure an open, fair, competitive, and secure global digital economy.

The method (ANC3M) was applied to the 53 action items that are described in the Commission's report and 142 relationships were obtained. Thus, 142 data were added to the database (ANC3DB).

Please note that this does not mean that the approaches of the U.S. are checked by the ANC3M because of the following reasons.

1) The Commission's report does not describe all the approaches of the U.S. to enhance its national cybersecurity capacity.
2) The Commission's report made the recommendations which are not necessarily adopted by the administration of the President Trump.

Nevertheless, the 53 action items are the cutting-edge approaches which are supposed to be essential to enhance the national cybersecurity capacity under the latest cyber threat landscapes and should give the very useful implication to the analysers who use the database. However, they may be better excluded from the statistical analyses because they are not the actually implemented approaches.

A part of the database, as a sample, is shown in the Table 3.4-1.

The full set of the data is in the Appendix J. Please note that both Table 3.4-1 and Appendix J show the views that join all three tables, relationships, action items and ANC3T.

Table 3.4-1 Sample of the ANC3DB

Ref.	Approaches					Categorization / Classification					
	Nation	#	Source	Year	Action Item	ID	Category	Subcategory	Capacity area	Lv	Requirement (keyword)
0001	Japan	7-111a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.	511 L2-4	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best practices
0002	Japan	7-111a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.	512 L1-2	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best practices for procurement
0003	Japan	7-111a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.	513 L3-1	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	3	Security consideration in all stages
0004	Japan	7-112a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.	511 L2-4	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best practices
0005	Japan	7-112a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.	512 L1-2	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best practices for procurement
0006	Japan	7-112a	Cyber security 2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.	513 L3-1	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	3	Security consideration in all stages
0007	Japan	7-112a2	Cyber security 2017	2017	Promoting secure IoT systems based on "General Framework for Secure IoT Systems".	511 L2-4	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best practices
0008	Japan	7-112b	Cyber security 2017	2017	Considering measures to exterminate 'bot-net'.	221 L2-2	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	2	Promotion of online trust established
0009	Japan	7-112b	Cyber security 2017	2017	Considering measures to exterminate 'bot-net'.	521 L2-1	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	2	Reliable internet infrastructures
0010	Japan	7-112b	Cyber security 2017	2017	Considering measures to exterminate	541 L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security	2	Latest technical controls & patch managements

(Blank Page)

Chapter 4. Verification

4.1 Introduction

Verification was done to see if the method (ANC3M) works well by applying the method to the approaches for cybersecurity capacity enhancement of Japan and the United Kingdom.

The purpose of the ANC3M is to check whether the national approaches are satisfying the four conditions. Therefore, if the checking process recognises the discrepancies against the conditions, the ANC3M can be considered workable.

As a result of the verification, the discrepancies were discovered and the ANC3M was proved to be workable.

On the other hand, with regard to the tool, the CSCMMN was tentatively used as the tool during the verification. It has been proved that the CSCMMN can be used as the tool, but needs enhancement. The enhancement was applied to the tentative tool to create the ANC3T.

As mentioned in section 3.2.2, in order to judge if the approaches of a nation are satisfying the conditions, all related approaches should be collected. Japan and the U.K. published their cybersecurity strategies where all of their cybersecurity related approaches are described. Therefore, the collection process of the approaches of the ANC3M is omissible as far as the approaches of Japan and the U.K. are used for verification.

4.2 Procedures and Criteria of Verification

The procedures of the verification are to apply ANC3M to the approaches of Japan and the U.K. As stated in section 4.1, the collection process were omitted and the cybersecurity strategy documents that are published by the governments were used instead.

The CSCMMN was used as the tentative ANC3T for the verification.

Basically, if the ANC3M discovers the capacity areas where the approaches are not satisfying the conditions, the verification is successful. However, it is difficult to set the definitive threshold, for example, “more than five discrepancies in the condition 2 and more than three in the condition 3”. That is because of the following reasons.

1) The approaches of Japan and the U.K. may be absolutely satisfying the conditions, i.e., there may be no discrepancies that the ANC3M should discover.
2) As mentioned in section 3.2.5, the thresholds for judging “few” or “a lot” are decided by the checker. Therefore, the number of the capacity areas that are discovered by the ANC3M is subject to the checker.

Therefore, it has been decided not to set the definitive criteria for the verification, but if the ANC3M discovers the reasonable number of the discrepancies, it should be recognised that the ANC3M should be workable.

4.3 Verification (Japan)

4.3.1 Cybersecurity Strategy of Japan

The Government of Japan established its cybersecurity strategy in 2013 and published “Cybersecurity Strategy - Toward a world-leading, resilient and vigorous cyberspace -” [30]. Japan had established its “Information Security Strategy for Protecting the Nation” in 2010 [31]. However, the extremely quick changes in the information security environment since then and the emergence of cyber-attacks against the public sector and the critical infrastructures urged Japan to revise the strategy within three years to emphasise the wide promotion of cyberspace measures.

However, the changes in cyberspace continued and malicious activities became more widespread. Threats against national safety and security increased. And the public sector and the business operators, which provided mission-critical infrastructure necessary to the people’s daily lives and economic activities, were left exposed to cyber-attacks. Under these circumstances, the Basic Act on Cybersecurity was enacted in November 2014. This Act prescribes the concept of cybersecurity and defines the roles and responsibilities of the Government, local governments and other relevant stakeholders. Additionally, it designates the Cybersecurity Strategic Headquarters as the command and control body of national cybersecurity, and gives strong authorities, such as making recommendations to national administrative organs, to the Cybersecurity Strategic Headquarters. Pursuant to the Basic Act that prescribes the responsibility of the public sector to establish a cybersecurity strategy, the “Cybersecurity Strategy” was formulated in 2015 [32]. The strategy “outlines the basic directions of Japan’s cybersecurity policies for the coming three years approximately” and is “looking towards the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games” [33].

Based on the cybersecurity strategies of 2013 and 2015, the Government of Japan decides and announces updates, results and achievements every fiscal year (hereafter abbreviated to “FY”) since FY2013. The results of FY2016 was published in July 2017 and the updated strategy for FY2017 was published in the following month [33, 34]. The strategy for FY2017, “Cybersecurity 2017”, includes awareness raising, cybersecurity countermeasures, education, training, critical infrastructure protection, cyber defence, anti-cybercrime, research and development, human resource management, international cooperation and promotion of cybersecurity-related business [34]. “Cybersecurity 2017”, wherein 220 approaches are described in five categories and 12 sub-categories, appears to be a prudent and comprehensive cybersecurity capacity building plan [34].

4.3.2 Mapping Result (Japan)

The mapping result (accumulated by the capacity areas) is shown in the Table 4.3-1.

The interim outputs, i.e., the collected cybersecurity approaches (produced from the Japanese Cybersecurity Strategy), the action items allocated to the tentative ANC3T and the mapping result (accumulated by the requirements) are shown in the Appendices C, E and F.

Table 4.3-1 Mapping Result of the Approaches of Japan

#	Category	Subcategory	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	0	0	0	1	1
112			Organisation	0	0	0	0	0
113			Content	0	0	0	1	1
121		Incident Response	Identification of Incidents	0	0	1	1	2
122			Organisation	0	0	1	4	5
123			Coordination	0	6	24	8	38
124			Mode of Operation	0	4	21	11	36
131		Critical Infrastructure (CI) Protection	Identification	0	0	2	2	4
132			Organisation	0	20	4	1	25
133			Risk Management and Response	0	3	19	2	24
141		Crisis Management	Crisis Management	0	5	12	0	17
151		Cyber Defence	Strategy	0	0	1	2	3
152			Organisation	0	0	1	6	7
153			Coordination	0	4	4	8	16
161		Communications Redundancy	Communications Redundancy	0	0	6	1	7
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	0	1	4	0	5
212			Private Sector	0	0	4	1	5
213			Users	0	6	9	2	17
221		Trust and Confidence on the Internet	User Trust and Confidence on the Internet	0	18	9	0	27
222			User Trust in E-government Services	0	0	3	0	3
223			User Trust in E-commerce Services	0	2	0	0	2
231		User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	0	3	0	0	3
241		Reporting Mechanisms	Reporting Mechanisms	0	1	0	0	1
251		Media and Social Media	Media and Social Media	0	0	3	0	3
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	0	1	7	2	10
312			Executive Awareness Raising	0	0	8	0	8
321		Framework for Education	Provision	0	11	6	6	23
322			Administration	0	2	4	11	17
331		Framework for Professional Training	Provision	1	7	13	6	27
332			Uptake	0	2	4	2	8
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	0	0	1	1	2
412			Privacy, Freedom of Speech & Other Human Rights Online	0	0	1	1	2
413			Data Protection Legislation	0	0	0	0	0
414			Child Protection Online	0	0	0	0	0
415			Consumer Protection Legislation	0	0	0	0	0
416			Intellectual Property Legislation	0	0	0	0	0
417			Substantive Cybercrime Legislation	0	1	1	3	5
418			Procedural Cybercrime Legislation	0	1	1	3	5
421		Criminal Justice System	Law Enforcement	0	0	8	3	11
422			Prosecution	0	0	0	1	1
423			Courts	0	0	0	0	0
431		Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	3	9	12	1	25
432			Informal Cooperation	3	2	1	0	6
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	0	33	9	2	44
512			Standards in Procurement	6	0	8	0	14
513			Standards in Software Development	4	4	9	1	18
521		Internet Infrastructure Resilience	Internet Infrastructure Resilience	0	2	0	3	5
531		Software Quality	Software Quality	0	0	0	0	0
541		Technical Security Controls	Technical Security Controls	1	21	15	2	39
551		Cryptographic Controls	Cryptographic Controls	0	3	1	6	10
561		Cybersecurity Marketplace	Cybersecurity Technologies	0	2	1	0	3
562			Cyber Insurance	0	1	0	0	1
571		Responsible Disclosure	Responsible Disclosure	0	3	2	1	6
Total				18	178	240	106	542

4.3.3 Evaluation Results (Japan)

4.3.3.1 Case 1: Autonomous Enhancement Mechanism

The list of the number of relationships with the requirements for autonomous enhancement mechanism is shown in the Table 4.3-2.

Table 4.3-2 Number of Relationships with Requirements for Autonomous Enhancement Mechanism (Japan)

ID	Keywords	Nb of relationships
111L4-1	Continual revision of strategy	1
112L3-1	PDCA processes of cybersecurity programme	0
112L4-1	Reassignment & reallocation of resources for cybersecurity programme	0
113L4-1	Continual revision of strategy	1
121L3-1	Regular revision of incident registry	0
124L3-3	Regular review of incident response processes	3
124L4-2	Evaluating effectiveness of CSIRT members training	1
131L4-1	Regular review of CI risk priorities	2
132L4-1	Ability to adjust of CI protection	1
133L3-4	Regular review of resource allocation for CI protection	0
133L4-1	Regular audit of CI	2
141L3-4	Evaluation of national incident exercise informing investment	0
161L3-3	Evaluation of national incident exercise informing investment	0
221L4-1	Users can evaluate risk & adjust behaviour	0
222L4-1	Promotion of e-gov revised	0
223L4-1	Continuous improvement of e-commerce	0
231L4-1	Users can adapt to changing environments	0
231L4-3	Security & privacy balanced in changing environment	0
231L4-4	Regular assessment of privacy protection	0
241L4-1	Regular enhancement of incident reporting	0
251L4-1	Discussion changing policy & society	0
311L4-1	Awareness raising programmes adapted according to effectiveness	0
311L4-2	Revision of national awareness raising programme	0
312L3-2	Executives' ability to reallocate resources	0
321L4-3	Cybersecurity education adapting to changing needs	2
322L4-3	Cybersecurity education aligned with practical problems	5
331L3-4	Metrics of effectiveness of cybersecurity training	1
332L3-1	Review of cybersecurity training programmes	2
411L3-1	Regular review of cybersecurity legal framework	1
411L4-1	Balance between cybersecurity legal framework & best practices	0
412L4-1	Amendment procedures for cybersecurity legal framework	0
413L4-1	Amendment procedures for data protection legislation	0
414L4-1	Amendment procedures for online child protection legislation	0
415L4-1	Amendment procedures for consumer protection legislation	0
416L4-1	Balance between intellectual property & open access policy	0
417L4-2	Regular review of substantive cybercrime legislation	0
418L4-2	Regular review of procedural cybercrime legislation	0
421L4-3	Regular review of investigative capabilities for cybercrimes	0
422L3-3	Exchange of best practices between prosecutors & judges	0
422L4-3	Specialised and continuous training for prosecutors	1
423L4-1	Specialised and continuous training for judges	0
423L4-2	Regular review of court system capabilities to judge cybercrimes	0
431L4-1	Regular review of international cooperation	1

(continue…)

ID	Keywords	Nb of relationships
431L4-3	Regularly adjusted information exchange between public & private sectors	0
432L4-1	Adapted cooperation & exchange of information	0
432L4-2	Adapted international cooperation	0
511L4-1	Regular review of adoption of standards & best practices	2
511L4-2	Decision making of non-compliance to standards & best practices	0
511L4-3	Risk-based decision making of compliance	0
512L3-2	Regular review of procurement	4
521L4-1	Controlled acquisition of infrastructures	0
521L4-2	Optimised cost for internet infrastructures	1
531L4-3	Regular review of quality requirement	0
541L4-1	Continuous assess of technical security controls	2
551L4-1	Regular review of relevance of cryptographic controls	4
551L4-2	Revision of cryptographic control policies	2
571L4-1	Regular review of vulnerability disclosure policies	0
571L4-4	Reviewing process of deadlines	0
Total number of relationships		39
Requirements with action items >0		20
Requirements with action items =0		38

Among 58 requirements for autonomous enhancement mechanism, 20 requirements are related with one or more action items. 38 requirements are related with none. This result alone cannot give any judgement about the condition 1 *"velocity"*. Further examination is needed to see if the result is along with the national strategy.

4.3.3.2 Case 2: *"Few"*

The capacity areas that few action items are related to are shown in the Table 4.3-3.

Table 4.3-3 Capacity Areas of Case 2 *"Few"* (Japan)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
111	Strategy Development	0	0	0	1	1
112	Organisation	0	0	0	0	0
113	Content	0	0	0	1	1
413	Data Protection Legislation	0	0	0	0	0
414	Child Protection Online	0	0	0	0	0
415	Consumer Protection Legislation	0	0	0	0	0
416	Intellectual Property Legislation	0	0	0	0	0
422	Prosecution	0	0	0	1	1
423	Courts	0	0	0	0	0
561	Cybersecurity Technologies	0	2	1	0	3
562	Cyber Insurance	0	1	0	0	1

This may be the case because Japan is already at a high level (level 3 or level 4) and, therefore, does not need many approaches to enhance these capacity areas.

However, for example, while the "prosecution" area (#422) has only one related action item and the "courts" area (#423) has none, the "law enforcement" area (#421) in the same subcategory has 11 related action items (please refer to the Table 4.3-1). This indicates that Japan still needs to work on maturing its capacities of law enforcement. Therefore, this implies that Japan emphasises the enhancement of cybersecurity capacity of law enforcement while focusing less on prosecution and justice.

Another example, the areas, namely, "cybersecurity technologies" (#561) and "cyber insurance" (#562) have three and one related action items, respectively. These areas do not refer to outright strength with regard to fighting against cyber-attackers and cyber-criminals but rather relate to the vigorousness of the cybersecurity industries. By considering that the first category of the "Cybersecurity 2017" [34] is "improvement of socio-economic vitality and sustainable development", which includes 48 action items, and shows the strong intention of Japan to promote cybersecurity industries, it would be more encouraging if more action items were related to these areas.

4.3.3.3 Case 3: *"Low"*

The capacity areas that the action items are related only to the lower levels are shown in the Table 4.3-4.

Table 4.3-4 Capacity Areas of Case 3 *"Low"* (Japan)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
223	User Trust in E-commerce Services	0	2	0	0	2
231	User Understanding of Personal Information Protection Online	0	3	0	0	3

If Japan is at a low level (level 0 or level 1) in the capacity areas, namely, "user trust in e-commerce services" (#223) and "user understanding of personal information protection online" (#231), and working on enhancement for advancing to the level 2, it is understandable that all action items are related to the level 2. However, Japan is apparently one of the most advanced nations with regard to e-commerce. A variety of online services are offered and a considerable proportion of people are using them on a daily basis. In such

circumstances, there exist a lot of threats and risks to cheat the users so that the personal information is exfiltrated and money is stolen. Moreover, such threat actors are motivated to sophisticate their cheating skills and use more advanced cheating technology. Therefore, Japan should enhance its national capacity in these areas to the world leading level (level 3 or level 4). For that reason, the approaches for these capacity areas are considered to be possibly dissatisfactory to the condition 3 *"levels"* and need further examination.

4.3.3.4 Case 4: *"High"*

The capacity areas that the action items are related only to the higher levels are shown in the Table 4.3-5.

Table 4.3-5 Capacity Areas of Case 4 *"High"* (Japan)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
151	Strategy	0	0	1	2	3
152	Organisation	0	0	1	6	7
153	Coordination	0	4	4	8	16

In the capacity areas, namely, "Strategy" (#151), "Organisation" (#152) and "Coordination" (#153), most of the action items are related to the level 4, with a few action items to the level 2 and 3. It looks as if Japan were at the level 3 now and working for the highest level. However, these capacity areas belong to the "cyber defence" subcategory, where Japan is hardly considered to be at the world leading level. A highly advanced capacity that is required in the level 4 does not always substitute for a fundamental capacity that is required in the level 1 or 2. Therefore, even if Japan successfully obtains the level 4 capacities, if it lacks the level 2 capacities, it will not be able to sufficiently defend against cyber threat. The approaches for these capacity areas need further examination.

4.3.3.5 Case 5: *"A lot"*

The capacity areas that a lot of action items are related to are shown in the Table 4.3-6.

Table 4.3-6 Capacity Areas of Case 5 *"A lot"* (Japan)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
123	Coordination	0	6	24	8	38
124	Mode of Operation	0	4	21	11	36
511	ICT Security Standards	0	33	9	2	44
541	Technical Security Controls	1	21	15	2	39

The capacity area with the most related action items is the "ICT security standards" area (#511). Here, the number of related action items is 44. Following with 39 items is the "technical security controls" area (#541). The areas, namely, "coordination" (#123) and "mode of operation" (#124) are in the third and fourth place with 38 and 36, respectively. Cumulatively, these top four areas have 157 related action items which is approximately 29% of the total 542 relationships. Note that the average number of related action items per area is 10.2.

Every capacity area in the "top four" is important and emphasising on these areas is an appropriate approach. However, it may be necessary to carry out a detailed investigation to determine that all related action items are not duplicates nor replaceable with fewer and more effective approaches.

We must bear in mind that the "ICT security standards" area (#511), which refers to the establishment of standards and best practices, the promotion and the compliance to these standards and best practices and the contribution to international standards, etc., is the most basic of all security activities. Therefore, it requires tremendous effort to develop it and focusing on this capacity area may mean to demand a large number of approaches.

4.3.3.6 Case 6: Not Allocated

It was found during the verification that some action items were not allocated to any requirement. Such action items are shown in the Table 4.3-7.

Table 4.3-7 Not Allocated Action Items (Japan)

#	Category	Subcategory	Strategy	Agency	Action Item
7-311a	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	Cabinet Secretariat	Enhancing counter-intelligence capabilities.
7-331b	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Asia Pacific	NPA, MOJ, MOFA	Supporting countries in Asian Pacific region to establish cybercrime jurisdiction.

There is no requirement that corresponds to these action items in the tentative ANC3T. However, Japan is actually coping with enhancement of the capacities and such capacities are considered essential to combat against cyber threats. Therefore, the ANC3T should be enhanced to include such requirements corresponding to those action items. The details of enhancement of the ANC3T are discussed in section 3.3.4.

The action item #7-311a refers to the enhancement of counter-intelligence capacities of Japan. Japan is working on it based on the "Basic Strategy for Enhancing Counter-Intelligence Capabilities" [35].

Counter-intelligence in cyberspace essentially consists of countermeasures against cyber-attacks aiming to exfiltrate information. Therefore, it may be classified into the "technical security controls" area (#541), "cryptographic controls" area (#551) or "ICT security standards" area (#511). However, unlike information leakage prevention at the organisational level, national level counter-intelligence is a part of national incident response or cyber defence.

Therefore, it was decided not to relate this action item to the capacity areas that were mentioned above, but to add new requirements corresponding to counter-intelligence capability. Thus, 152L3-2 and 152L4-2 were added in the "organisation" area (#152) of the ANC3T.

The action item #7-331b refers to the support provided to nations in the Asian Pacific region for the establishment of a cybercrime jurisdiction.

There exist the requirements for international or regional cooperation and coordination in incident response (in the 'incident response' subcategory), the requirements for contribution to international cooperation agreements and international treaties with regard to anti-

cybercrime activities (in the ‘legal framework’ subcategory) and the requirements for cooperation in cross-border investigation (in the ‘formal and informal cooperation frameworks to combat cybercrime’ subcategory). However, there is no requirement referring to the provision of support to other nations with regard to the establishment of legal capacities with objective of tackling cybercrime in these nations.

Therefore, it was decided to add new requirements corresponding to international/regional cooperation in supporting establishment of legislative framework. Thus, 411L4-4 and 432L4-4 were added in the “legislative framework for ICT security” area (#411) and the “informal cooperation” area (#432), respectively.

The details of the added requirements are shown in the Table 4.3-8.

Table 4.3-8 Requirements Added for Enhancement

#	Category	Subcategory	Capacity area	Level	ID	Keyword	Requirement
152	Cybersecurity Policy and Strategy	Cyber Defence	Organisation	3	152L3-2	Counter-cyber intelligence activities	There exist activities for detecting and/or defending against intelligence assessment through cyber-space from other nations.
-do-	-do-	-do-	-do	4	152L4-2	Established counter-cyber intelligence capability	Counter-cyber intelligence activities are centrarised and have capability to defend effectively.
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	4	411L4-4	International and/or regional cooperation of establishing legislative framework	The nation cooperates internationally and/or regionally in supporting other nations in establishing legislative framework for ICT security.
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Informal Cooperation	4	432L4-4	International and/or regional cooperation of establishing cybercrime legislation	The nation cooperates internationally and/or regionally in supporting other nations in establishing cybercrime legislation.

4.3.4 Provisional Assessment of Japanese Cybersecurity Capacity

Although it is not directly informing the verification, the national cybersecurity capacity of Japan was provisionally assessed using the CSCMMN [13]. The full result of the assessment is shown in the Appendix I, and the summary is shown in the Table 4.3-9 and 4.3-10.

The result shows that Japan has achieved approximately half (51.0%) of the indicators. Moreover, there exist six unachieved indicators (two partly achieved and four not achieved) in the "formative" stage which corresponds to the level 1 in the ANC3T.

As stated in section 4.3.3.2, 11 capacity areas are supposed to be the case 2 *"few"*. Among the 11 areas, six areas (#413, #414, #415, #416, #422 and #423) belong to the "legal and regulatory frameworks" category, which corresponds to the "dimension 4" of the CSCMMN. In the "dimension 4", Japan has achieved 54.3% of the indicators, which is almost the same as the average. It suggests that it is not the case that Japan does not emphasise on these capacity areas because it is already at a high level.

Note that the provisional assessment in this research is different from the official assessment designated in the CSCMMN in the following points.

1) The indicators that include two or more conditions have been split so that an indicator denotes one single condition (basically the same process as the ANC3T).
2) The indicators that do not denote conditions but explanations have been excluded.
3) State of achievement were judged into three grades; "achieved", "partly achieved" or "not achieved".
4) The indicators that are not applied to Japan were assigned "achieved". For example, "an outline/draft national cybersecurity strategy has been articulated" does not seem to exist in Japan but was assigned "achieved" because Japan does not need a draft strategy anymore.
5) Stages are judged by aspects rather than factors as prescript in the CSCMMN.

These alterations are applied because the purpose of the provisional assessment is not the measurement of the outright strength of Japan with regard to cybersecurity but the discovery of the status of the capacity of Japan, i.e., what indicators are achieved and what are not achieved.

This provisional assessment is based on the knowledge about the current status of Japan with regard to cybersecurity obtained from the documents published by the Japanese Government, i.e., "Cybersecurity 2015", "Cybersecurity 2016", "Cybersecurity 2017" and "Cybersecurity 2018" [36, 37, 34, 38].

Table 4.3-9 Summary Result of Provisional Assessment of Capacity of Japan

	Formative					Established					Strategic				
	y	p	n	Total	y%	y	p	n	Total	y%	y	p	n	Total	y%
Dimension 1	22	0	2	24	91.7	30	4	6	40	75.0	13	16	17	46	28.3
Dimension 2	19	0	0	19	100.0	19	3	1	23	82.6	9	9	6	24	37.5
Dimension 3	13	1	1	15	86.7	16	1	4	21	76.2	5	7	11	23	21.7
Dimension 4	24	1	1	26	92.3	21	0	9	30	70.0	12	0	19	31	38.7
Dimension 5	27	0	0	27	100.0	24	4	7	35	68.6	8	15	6	29	27.6
Total	105	2	4	111	94.6	110	12	27	149	73.8	47	47	59	153	30.7

	Dynamic					Total				
	y	p	n	Total	y%	y	p	n	Total	y%
Dimension 1	2	3	27	32	6.3	67	23	52	142	47.2
Dimension 2	2	4	11	17	11.8	49	16	18	83	59.0
Dimension 3	0	7	9	16	0.0	34	16	25	75	45.3
Dimension 4	6	3	20	29	20.7	63	4	49	116	54.3
Dimension 5	2	10	18	30	6.7	61	29	31	121	50.4
Total	12	27	85	124	9.7	274	88	175	537	51.0

Note y: achieved, p: partly achieved, n: not achieved, y%: ratio of "y"

Table 4.3-10 Stage Judgement of Japan by Aspect

Dimension	Factor	Aspect	S-u	F	E	S	D
Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development					■
		Organisation					■
		Content					■
	Incident Response	Identification of Incidents				■	■
		Organisation				■	■
		Coordination			■	■	■
		Mode of Operation				■	■
	Critical Infrastructure (CI) Protection	Identification				■	■
		Organisation				■	■
		Risk Management and Response			■	■	■
	Crisis Management	Crisis Management				■	■
	Cyber Defence	Strategy		■	■	■	■
		Organisation				■	■
		Coordination		■	■	■	■
	Communications Redundancy	Communications Redundancy			■	■	■
Cyber Culture and Society	Cybersecurity Mind-set	Government				■	■
		Private Sector				■	■
		Users				■	■
	Trust and Confidence on the Internet	User Trust and Confidence on the Internet				■	■
		User Trust in E-government Services			■	■	■
		User Trust in E-commerce Services			■	■	■
	User Understanding of Personal….	User Understanding of Personal Information Protection Online			■	■	■
	Reporting Mechanisms	Reporting Mechanisms			■	■	■
	Media and Social Media	Media and Social Media				■	■
Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes		■	■	■	■
		Executive Awareness Raising				■	■
	Framework for Education	Provision				■	■
		Administration				■	■
	Framework for Professional Training	Provision				■	■
		Uptake		■	■	■	■
Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security					■
		Privacy, Freedom of Speech & Other Human Rights Online					■
		Data Protection Legislation				■	■
		Child Protection Online			■	■	■
		Consumer Protection Legislation					■
		Intellectual Property Legislation					■
		Substantive Cybercrime Legislation				■	■
		Procedural Cybercrime Legislation				■	■
	Criminal Justice System	Law Enforcement			■	■	■
		Prosecution			■	■	■
		Courts			■	■	■
	Formal and Informal….	Formal Cooperation		■	■	■	■
		Informal Cooperation		■	■	■	■
Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards			■	■	■
		Standards in Procurement			■	■	■
		Standards in Software Development			■	■	■
	Internet Infrastructure Resilience	Internet Infrastructure Resilience					■
	Software Quality	Software Quality			■	■	■
	Technical Security Controls	Technical Security Controls				■	■
	Cryptographic Controls	Cryptographic Controls				■	■
	Cybersecurity Marketplace	Cybersecurity Technologies			■	■	■
		Cyber Insurance			■	■	■
	Responsible Disclosure	Responsible Disclosure			■	■	■

Note S-u: Start-up, F: Formative, E: Established, S: Strategic, D: Dynamic

□: Achieved ■: Not Achieved

4.4 Verification (U.K.)

4.4.1 Cybersecurity Strategy of the U.K.

The United Kingdom released the "National Cyber Security Strategy 2016-2021" [39] in November 2016 and stated in its "Foreword" that "Much of our prosperity now depends on our ability to secure our technology, data and networks from the many threats we face. Yet cyber-attacks are growing more frequent, sophisticated and damaging when they succeed. So, we are taking decisive action to protect both our economy and the privacy of U.K. citizens".

The U.K. had formerly announced the "U.K. Cyber Security Strategy 2011-2016" [40] with £860 million underpinned for the National Cyber Security Programme. Under the new strategy, the U.K. "will invest £1.9 billion in defending our systems and infrastructure, deterring our adversaries, and developing a whole-society capability - from the biggest companies to the individual citizen" [39].

In the new strategy, the cybersecurity policies are described in the categories - Defend, Deter, Develop and International Action.

The report of assessment using the CSCMM, "Cybersecurity Capacity Review of the United Kingdom" [18], states in its "Introduction" that the evaluation "will contribute to the development of the UK National Cybersecurity Strategy 2016–2020."

4.4.2 Mapping Result (U.K.)

The mapping result (accumulated by the capacity areas) is shown in the Table 4.4-1.

The interim outputs, i.e., the collected cybersecurity approaches (produced from the U.K. Cybersecurity Strategy), the action items allocated to the tentative ANC3T and the mapping result (accumulated by the requirements) are shown in the Appendices D, G and H.

Table 4.4-1 Mapping Result of the Approaches of U.K.

#	Category	Subcategory	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	0	0	1	4	5
112			Organisation	0	0	0	1	1
113			Content	0	0	0	1	1
121		Incident Response	Identification of Incidents	0	2	0	0	2
122			Organisation	0	0	0	1	1
123			Coordination	0	0	7	3	10
124			Mode of Operation	0	1	3	2	6
131		Critical Infrastructure (CI) Protection	Identification	0	0	2	2	4
132			Organisation	0	1	1	3	5
133			Risk Management and Response	0	0	4	0	4
141		Crisis Management	Crisis Management	0	2	4	5	11
151		Cyber Defence	Strategy	0	0	4	0	4
152			Organisation	0	0	7	4	11
153			Coordination	0	1	3	12	16
161		Communications Redundancy	Communications Redundancy	0	0	4	3	7
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	0	0	0	1	1
212			Private Sector	0	0	1	2	3
213			Users	0	0	1	1	2
221		Trust and Confidence on the Internet	User Trust and Confidence on the Internet	0	0	0	0	0
222			User Trust in E-government Services	0	4	1	5	10
223			User Trust in E-commerce Services	0	0	1	0	1
231		User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	0	0	0	0	0
241		Reporting Mechanisms	Reporting Mechanisms	0	2	0	0	2
251		Media and Social Media	Media and Social Media	0	0	0	0	0
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	0	1	5	5	11
312			Executive Awareness Raising	0	0	2	1	3
321		Framework for Education	Provision	0	5	8	12	25
322			Administration	0	4	8	19	31
331		Framework for Professional Training	Provision	0	1	7	6	14
332			Uptake	0	1	4	0	5
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	0	0	1	4	5
412			Privacy, Freedom of Speech & Other Human Rights Online	0	0	0	2	2
413			Data Protection Legislation	0	0	0	0	0
414			Child Protection Online	0	0	0	0	0
415			Consumer Protection Legislation	0	0	0	1	1
416			Intellectual Property Legislation	0	0	0	1	1
417			Substantive Cybercrime Legislation	0	0	0	3	3
418			Procedural Cybercrime Legislation	0	0	0	3	3
421		Criminal Justice System	Law Enforcement	0	0	10	3	13
422			Prosecution	0	0	0	3	3
423			Courts	0	0	0	1	1
431		Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	0	1	1	2	4
432			Informal Cooperation	0	0	4	3	7
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	0	8	4	0	12
512			Standards in Procurement	0	1	2	0	3
513			Standards in Software Development	0	1	3	0	4
521		Internet Infrastructure Resilience	Internet Infrastructure Resilience	0	1	4	0	5
531		Software Quality	Software Quality	0	2	1	0	3
541		Technical Security Controls	Technical Security Controls	0	5	3	13	21
551		Cryptographic Controls	Cryptographic Controls	0	0	0	4	4
561		Cybersecurity Marketplace	Cybersecurity Technologies	0	0	5	9	14
562			Cyber Insurance	0	0	0	2	2
571		Responsible Disclosure	Responsible Disclosure	0	0	0	0	0
Total				0	44	116	147	307

4.4.3 Evaluation Results (U.K.)

4.4.3.1 Case 1: Autonomous Enhancement Mechanism

The list of the number of relationships with the requirements for autonomous enhancement mechanism is shown in the Table 4.4-2.

Table 4.4-2 Number of Relationships with Requirements for Autonomous Enhancement Mechanism (U.K.)

ID	Keywords	Nb of relationships
111L4-1	Continual revision of strategy	1
112L3-1	PDCA processes of cybersecurity programme	0
112L4-1	Reassignment & reallocation of resources for cybersecurity programme	1
113L4-1	Continual revision of strategy	1
121L3-1	Regular revision of incident registry	0
124L3-3	Regular review of incident response processes	0
124L4-2	Evaluating effectiveness of CSIRT members training	0
131L4-1	Regular review of CI risk priorities	2
132L4-1	Ability to adjust of CI protection	2
133L3-4	Regular review of resource allocation for CI protection	1
133L4-1	Regular audit of CI	0
141L3-4	Evaluation of national incident exercise informing investment	2
161L3-3	Evaluation of national incident exercise informing investment	2
221L4-1	Users can evaluate risk & adjust behaviour	0
222L4-1	Promotion of e-gov revised	0
223L4-1	Continuous improvement of e-commerce	0
231L4-1	Users can adapt to changing environments	0
231L4-3	Security & privacy balanced in changing environment	0
231L4-4	Regular assessment of privacy protection	0
241L4-1	Regular enhancement of incident reporting	0
251L4-1	Discussion changing policy & society	0
311L4-1	Awareness raising programmes adapted according to effectiveness	0
311L4-2	Revision of national awareness raising programme	0
312L3-2	Executives' ability to reallocate resources	1
321L4-3	Cybersecurity education adapting to changing needs	5
322L4-3	Cybersecurity education aligned with practical problems	4
331L3-4	Metrics of effectiveness of cybersecurity training	2
332L3-1	Review of cybersecurity training programmes	1
411L3-1	Regular review of cybersecurity legal framework	1
411L4-1	Balance between cybersecurity legal framework & best practices	3
412L4-1	Amendment procedures for cybersecurity legal framework	0
413L4-1	Amendment procedures for data protection legislation	0
414L4-1	Amendment procedures for online child protection legislation	0
415L4-1	Amendment procedures for consumer protection legislation	1
416L4-1	Balance between intellectual property & open access policy	1
417L4-2	Regular review of substantive cybercrime legislation	1
418L4-2	Regular review of procedural cybercrime legislation	1
421L4-3	Regular review of investigative capabilities for cybercrimes	3
422L3-3	Exchange of best practices between prosecutors & judges	0
422L4-3	Specialised and continuous training for prosecutors	0
423L4-1	Specialised and continuous training for judges	0
423L4-2	Regular review of court system capabilities to judge cybercrimes	1
431L4-1	Regular review of international cooperation	2

(continue…)

ID	Keywords	Nb of relationships
431L4-3	Regularly adjusted information exchange between public & private sectors	0
432L4-1	Adapted cooperation & exchange of information	0
432L4-2	Adapted international cooperation	3
511L4-1	Regular review of adoption of standards & best practices	0
511L4-2	Decision making of non-compliance to standards & best practices	0
511L4-3	Risk-based decision making of compliance	0
512L3-2	Regular review of procurement	0
521L4-1	Controlled acquisition of infrastructures	0
521L4-2	Optimised cost for internet infrastructures	0
531L4-3	Regular review of quality requirement	0
541L4-1	Continuous assess of technical security controls	12
551L4-1	Regular review of relevance of cryptographic controls	2
551L4-2	Revision of cryptographic control policies	2
571L4-1	Regular review of vulnerability disclosure policies	0
571L4-4	Reviewing process of deadlines	0
Total number of relationships		58
Requirements with action items >0		26
Requirements with action items =0		32

Among 58 requirements for autonomous enhancement mechanism, 26 requirements are related with one or more action items. 32 requirements are related with none. This result alone cannot give any judgement about the condition 1 *"velocity"*. Further examination is needed to see if the result is along with the national strategy.

4.4.3.2 Case 2: "Few"

The capacity areas that few action items are related to are shown in the Table 4.4-3.

Table 4.4-3 Capacity Areas of Case 2 *"Few"* (U.K.)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
112	Organisation	0	0	0	1	1
113	Content	0	0	0	1	1
121	Identification of Incidents	0	2	0	0	2
122	Organisation	0	0	0	1	1
211	Government	0	0	0	1	1
221	User Trust and Confidence on the Internet	0	0	0	0	0
223	User Trust in E-commerce Services	0	0	1	0	1
231	User Understanding of Personal Information Protection Online	0	0	0	0	0
241	Reporting Mechanisms	0	2	0	0	2
251	Media and Social Media	0	0	0	0	0
412	Privacy, Freedom of Speech & Other Human Rights Online	0	0	0	2	2
413	Data Protection Legislation	0	0	0	0	0
414	Child Protection Online	0	0	0	0	0
415	Consumer Protection Legislation	0	0	0	1	1
416	Intellectual Property Legislation	0	0	0	1	1
423	Courts	0	0	0	1	1
562	Cyber Insurance	0	0	0	2	2
571	Responsible Disclosure	0	0	0	0	0

In 18 capacity areas, the approaches of the U.K. are considered possibly dissatisfactory to the condition 2 *"coverage"*. The areas vary evenly over four categories. Therefore, it is not the case that the approaches related to some particular categories are excluded from the strategy.

As mentioned in 4.4.1, the U.K. had carried out an official assessment of its cybersecurity capacity using the CSCMM (version 1.2, not the CSCMMN Revised Edition that the tentative AC3T is based on) and the result of the assessment was informed to the strategy. Therefore, the public sector of the U.K. understood all of the necessary capacity areas (or "category" in the terms of the CSCMM) when they developed the strategy. Nevertheless, they planned a few (or no) approaches for 18 capacity areas. It is needed to examine further.

4.4.3.3 Case 3: *"Low"*

There is no capacity area that the action items are related only to the lower levels.

4.4.3.4 Case 4: *"High"*

There is no capacity area that the action items are related only to the higher levels.

4.4.3.5 Case 5: *"A lot"*

The capacity areas that a lot of action items are related to are shown in the Table 4.4-4.

Table 4.4-4 Capacity Areas of Case 5 *"A lot"* (U.K.)

#	Capacity area	Lv 1	Lv 2	Lv 3	Lv 4	Total
321	Provision	0	5	8	12	25
322	Administration	0	4	8	19	31
541	Technical Security Controls	0	5	3	13	21

The "administration" area (#322) is the area that the most action items are related to with 31 items. Following with 25 items is the "Provision" area (#321). These two areas are of the same subcategory "framework for education" and the total number of related items is 56, or 18% of the total 307 relationships. It suggests that the cybersecurity education is emphasised very much.

The third place with 21 items is the "technical security control" area (#541), which is the second place with 39 items in the case of Japanese approaches.

4.4.3.6 Case 6: Not Allocated

There is no action item that was not allocated to any requirement.

4.5 Discussion

4.5.1 Four Conditions

As mentioned in 1.4, when a nation enhances its cybersecurity capacities, it should satisfy the following four conditions.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (condition 1 *"velocity"*)
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (condition 2 *"coverage"*)
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (condition 3 *"levels"*)
4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (condition 4 *"efficiency"*)

There may be questions if the four conditions are really necessary, or if the four conditions are enough for the appropriate enhancement of the national cybersecurity capacity.

Firstly, all of the four conditions are supposed to be really necessary. Through the verification, the following findings were detected;

1) The number of action items related to each requirement for the autonomous enhancement mechanism is indicated. It does not give a definitive verdict but provides with information for further examination if the nation satisfies the condition 1 *"velocity"*.
2) In some capacity areas, few action items were allocated, which indicates that the nation may not satisfy the condition 2 *"coverage"* in those capacity areas.
3) In some capacity areas, the action items were allocated only to the higher levels or only to the lower levels, which indicates that the capacity areas may not satisfy the condition 3 *"levels"* or the condition 2 *"coverage"* in those capacity areas.
4) Some capacity areas were found to be allocated a lot of action items, which indicates that the capacity areas may not satisfy the condition 4 *"efficiency"*.

If any of the four conditions were dismissed, some of the possible inappropriateness of the approaches would be left undiscovered. Therefore, all of the four conditions are necessary for appropriate enhancement of the national cybersecurity capacity.

Secondly, the four conditions are supposed to be enough for the appropriate enhancement of the national cybersecurity capacity. As mentioned above, the method successfully indicated the possible discrepancies that may appear to be dissatisfactory to the conditions after further examination.

There do not exist any other type of findings through the verification. This does not immediately mean that there may not be any other conditions to be satisfied for appropriate enhancement of the national cybersecurity capacity. However, there do not exist any apparent missing conditions. Therefore, it is thought to be adequate for the time being to focus on the four conditions to check the approaches for the national cybersecurity capacity enhancement. The possibility that there may be found other conditions during the check of the approaches of the other nations using the ANC3M/ANC3T should not be ruled out.

4.5.2 Reproducibility of Checking

The method (ANC3M) is designed so that the checking result will not be much inconsistent subject to the person who use it. This is important because the checking result is intended to inform to consideration of possible alteration of the national approaches.

The Table 4.5-1 shows a part of the tool (ANC3T). The user of the method (ANC3M) is required to examine if an action item will fulfil or contribute toward fulfilling any of the requirements shown in the ANC3T. For example, assume the following action item is given;

“Ministry A requests all the listed companies to be equipped with the cybersecurity countermeasures according to the Standard X.”

What requirements will the action item fulfil or contribute toward fulfilling? Probably it will contribute toward fulfilling the L2-2 “Standards & best practices widely used” and the L2-4 “Promotion of use of standards & best practices.” Anything else? Possibly the L1-3 “International standards & best practices implemented.” But the action item is not supposed to fulfil nor contribute toward fulfilling the L2-5 “Metrics of compliance of standards & best practices”, the L3-3 “Contributing to international standards”, the L4-3 “Risk-based decision making of compliance” nor any other requirements.

Thus, inconsistency subject to the users of the method is supposed to be limited to the small range. In this example, some users may find two relationships between the action item and the capacity area while other users may find three. But few users would say they found four or more relationships, nor say found none.

Therefore, there may be some inconsistency of the checking results subject to the checker, but the inconsistency is hardly supposed to become significant. And

small inconsistency can be absorbed by adjusting the thresholds when evaluating the mapped results.

Table 4.5-1 Part of ANC3T

#	Capacity area	Level 1		Level 2		Level 3		Level 4	
		ID	Keywords	ID	Keywords	ID	Keywords	ID	Keywords
511	ICT Security Standards	L1-1	Standards for information risk management	L2-1	Established standards & best practices	L3-1	Risk-based adoption of standards & best practices	L4-1	Regular review of adoption of standards & best practices
		L1-2	Standards for information risk management partly used	L2-2	Standards & best practices widely used	L3-2	Resource allocation based on standards	L4-2	Decision making of non-compliance to standards & best practices
		L1-3	International standards & best practices implemented	L2-3	Metrics of adoption of standards & best practices	L3-3	Contributing to international standards	L4-3	Risk-based decision making of compliance
				L2-4	Promotion of use of standards & best practices				
				L2-5	Metrics of compliance of standards & best practices				
				L2-6	Standards & best practices used by CI supply chains				

Additionally, checking the approaches using this method (ANC3M) does not require the checkers to have very high skills. People with a basic knowledge about cybersecurity can do. Therefore, it is possible for two or more checkers to perform the mapping process in parallel and then to consolidate the outputs for a stable result.

4.6 Conclusion of Verification

In the verification using Japanese cybersecurity approaches, the proposed method (ANC3M) indicated that 20 capacity areas are any of the case 2 to 5. Please note that the case 1 or the case 6 is not the findings in the approaches.

That is 38% of the total 53 capacity areas. The breakdown of the number by cases is shown in the Table 4.6-1.

The verification using the approaches of the U.K. indicated 21, or 40%.

The total number of indications, 41, or 39%, is a considerable achievement for verification.

Table 4.6-1 Number of Findings

Verification	Case 2 *"few"*	Case 3 *"low"*	Case 4 *"high"*	Case 5 *"a lot"*	Total	Ratio
Verification (Japan)	11	2	3	4	20	38% (20/53)
Verification (UK.)	18	0	0	3	21	40% (21/53)
Total	29	2	3	7	41	39% (41/106)

On the other hand, the verification also indicated the approaches that are not allocated to any of the requirements of the tentative ANC3T but are thought to be meaningful for the vigorousness of the national cybersecurity capacities. In response to the indications, the ANC3T has been enhanced by adding the requirements related to those approaches.

It is thought that the result proves the followings.

1) It is worth checking the national approaches for cybersecurity capacity enhancement. Even a public sector who understands all of the necessary capacity areas may possibly fail to develop a strategy that covers the areas comprehensively.
2) The proposed method (ANC3M) is workable for checking the approaches.
3) The tentative tool must be enhanced to be used as the ANC3T.

(Blank Page)

Chapter 5. Conclusion and Remaining Issues

5.1 Conclusion

This thesis proposes the method and the tool that are aimed at checking if the approaches for the national cybersecurity capacity enhancement are appropriate. In other words, they can check if the approaches satisfy the following four conditions.

1) National cybersecurity capacities must be enhanced at the same velocity as technology, skills of attackers and capacities of other nations develop, or even faster than those. (condition 1 *"velocity"*)
2) National cybersecurity capacities must be enhanced comprehensively over the various capacity areas that are necessary for nations. (condition 2 *"coverage"*)
3) National cybersecurity capacities must be enhanced up to the levels that can match the capacities of the attackers and other hostile nations. (condition 3 *"levels"*)
4) National cybersecurity capacities must be enhanced efficiently so that it can extract the optimised effects from the limited resources. (condition 4 *"efficiency"*)

The method and the tool were verified by applying them to the actual approaches implemented by Japan and the U.K. The verification proved that the method works well while the tool that was tentatively derived from the CSCMMN needs enhancement. The tool has been enhanced by adding four requirements according to the findings obtained through verification.

In order to provide with the analytical functionality, the database is also proposed. The database consists of the set of the approaches for the national cybersecurity capacity enhancement that are categorised and classified according to the proposed method. It is supposed to be used when one wants to know what kind of approaches are adopted for enhancing a particular capacity, what level is aimed at in a particular capacity, what capacity areas are emphasised in a particular period of time, and so on.

The method is called "ANC3M" (Approaches for National Cybersecurity Capacity enhancement Checking Method).
The tool is called "ANC3T" (Approaches for National Cybersecurity Capacity enhancement Checking Tool).
The database is called "ANC3DB" (Approaches for National Cybersecurity Capacity enhancement Checked DataBase).

By proposing the method and the tool to check the appropriateness of the approaches for the national cybersecurity capacity enhancement, this research should contribute toward ensuring the appropriateness of the approaches. And the ANC3M, ANC3T and ANC3DB will help improving the approaches. Then, they should contribute toward

improvement of the national cybersecurity capacities. Ultimately, this research is aiming at contribution to the decrease of cyber-attacks world-wide and reduction of the possible damages caused by cyber-attacks.

In order for the research to contribute toward improvement of the approaches, it is desirable that the policymakers carry out the check of the approaches using the ANC3M and ANC3T, and refer to the ANC3DB for consideration of improvement of the approaches. However, it is not necessarily the policymakers who use them, but anyone else can do. If anyone other than the policymakers of the nation, or even anyone outside of the nation carry out the check of the approaches and the result informs to the decision of the approaches, this research can contribute towards improvement of the approaches of that nation.

In the verification process, the author checked the approaches of Japan and the United Kingdom. Even if the author continues checking the approaches of other nations, the number of the nations whose approaches are check by the method will be limited. However, if other people join and check the approaches of various nations using the ANC3M, the approaches of an increased number of nations will be checked and the contribution of this research will be greater.

The method is designed so that the checking result will not be much inconsistent subject to the person who use it.

Furthermore, the database that is proposed in this research can be used with or without the checking method. In other words, while the ANC3DB can be used after checking the approaches using the ANC3M, it can also be used on its own for consideration of improvement of the approaches.

Therefore, this research is supposed to contribute widely toward improvement of the approaches, the national cybersecurity capacities and ultimately cyber threat environment.

5.2 Remaining Issues

It is desired that the ANC3M/ANC3T are adopted by the public sector to help checking their cybersecurity capacity enhancement approaches. However, applying the ANC3M/ANC3T to the approaches will just provide with the information that the approaches in some capacity areas are possibly inappropriate. The public sector will have to plan and execute additional approaches and/or streamline the approaches to improve the capacity enhancement. If the information about the examples of the approaches that are executed in other nations and/or the statistical data are provided with, the public sector will be more motivated to check their approaches by applying the ANC3M/ANC3T. The ANC3DB is supposed to give such information if the sufficient data are collected.

Therefore, it is supposed to be important to continue collecting the approaches that are aimed at enhancing the national cybersecurity capacity.

Moreover, collecting the data will possibly enhance the ANC3T if the approaches can strengthen the capacities that are not described in the existing requirements in the ANC3T. That will increase the attractiveness of the ANC3M/ANC3T.

Furthermore, if the considerable amount of data is collected, the ANC3DB will not only give information that help determining the alteration of the approaches, but have possibility to lead to a discovery of the statistical findings.

Therefore, it is planned to continue collecting the data besides promoting the ANC3M/ANC3T. If any statistical findings are observed, it will be publicised accordingly.

(Blank Page)

References

[1] Oath Inc. news release on 3 Oct. 2017 “Yahoo provides notice to additional users affected by previously disclosed 2013 data theft” <https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/> (Referred on 12 February 2019)

[2] The New York Times article on 30 Apr. 2016 “Hackers’ $81 Million Sneak Attack on World Banking” <https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html> (Referred on 12 February 2019)

[3] SANS ICS Defense Use Case March 18, 2016 “Analysis of the Cyber Attack on the Ukrainian Power Grid” <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf> (Referred on 12 February 2019)

[4] SANS ICS Defense Use Case No.6 August 2, 2017 “Modular ICS Malware” <https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf> (Referred on 12 February 2019)

[5] Executive Order 13687 of January 2, 2015 “Imposing Additional Sanctions With Respect To North Korea” <https://www.federalregister.gov/documents/2015/01/06/2015-00058/imposing-additional-sanctions-with-respect-to-north-korea> (Referred on 12 February 2019)

[6] Y. Tagawa and K. Hayashi, “Information Sharing and the Core Institution for Cybersecurity”, Bulletin of Institute of Information Security, Vol. 9, PP. 17-44, 2017 (Japanese only)
田川義博，林紘一郎：サイバーセキュリティのための情報共有と中核機関のあり方 －3 つのモデルの相互比較とわが国への教訓－，情報セキュリティ総合科学（情報セキュリティ大学院大学紀要），Vol. 9，pp. 17-44（オンライン），入手先＜http://www.iisec.ac.jp/proc/vol0009/tagawa-hayashi17.pdf＞（2017）

[7] The Policy Appraisal and Evaluation Study Group, The Present Conditions and Concern of the Policy Appraisal and Evaluation. Bokutakusha, 1999 (Japanese only)
政策評価研究会：政策評価の現状と課題－新たな行政システムを目指して，木鐸社（1999）

[8] National Institute of Standards and Technology “Framework for Improving Critical Infrastructure Cybersecurity Version 1.1”

<https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11> (Referred on 12 February 2019)

[9] HM Treasury of the United Kingdom “The Greenbook; Central Government Guidance on Appraisal and Evaluation”
<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/685903/The_Green_Book.pdf> (Referred on 12 February 2019)

[10] H. Kodama, “Verification of the Policy Appraisal and Evaluation of the United Kingdom and Suggestion to Japan”, Hakuoh Review of Law and Politics, Vol. 18 No. 1, PP. 269-349, 2011 (Japanese only)
児玉博昭：英国における政策評価システムの検証とわが国への示唆：政策達成目標明示制度導入の是非，白鴎法学（白鴎大学法学部紀要），Vol. 18，No. 1，pp. 269-349（オンライン），入手先＜
https://hakuoh.repo.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=1940&item_no=1&page_id=13&block_id=21＞（2011）

[11] International Telecommunication Union “Global Cybersecurity Index (GCI) 2017”
<https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf>
(Referred on 12 February 2019)

[12] Global Cyber Security Capacity Centre “Cyber Security Capability Maturity Model (CMM) –V1.2”
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf> (Referred on 12 February 2019)

[13] Global Cyber Security Capacity Centre “Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition”
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf> (Referred on 12 February 2019)

[14] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the Republic of Uganda”
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Uganda%20CMM.pdf>
(Referred on 12 February 2019)

[15] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the Republic of Senegal”
<https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Senegal-Report-v4%20.pdf> (Referred on 12 February 2019)

[16] Global Cyber Security Capacity Centre “Building Cyber-security Capacity in the Kingdom of Bhutan” <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Bhutan_September_2015.pdf> (Referred on 12 February 2019)

[17] Global Cyber Security Capacity Centre “Cybersecurity Capacity Assessment of the Republic of Kosovo” <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM_Review_Report_Kosovo_June_2015.pdf> (Referred on 12 February 2019)

[18] Global Cyber Security Capacity Centre “Cybersecurity Capacity Review of the United Kingdom” <https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity%20Capacity%20Review%20of%20the%20United%20Kingdom.pdf> (Referred on 12 February 2019)

[19] Inter-American Development Bank “Cybersecurity: Are We Ready in Latin America and the Caribbean?” <https://publications.iadb.org/handle/11319/7449> (Referred on 12 February 2019)

[20] Global Cyber Security Capacity Centre “CMM Assessments Around the World” <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments-around-world> (Referred on 12 February 2019)

[21] Australian Strategic Policy Institute “Cyber Maturity in the Asia Pacific Region 2017” < https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017> (Referred on 12 February 2019)

[22] The Software Alliance “EU Cybersecurity Dashboard” <http://cybersecurity.bsa.org/index.html> (Referred on 12 February 2019)

[23] Federal Financial Institutions Examination Council “Cybersecurity Assessment Tool” <https://www.ffiec.gov/cyberassessmenttool.htm> (Referred on 12 February 2019)

[24] International Organization for Standardization “ISO/IEC 27032:2012” <https://www.iso.org/standard/44375.html> (Referred on 12 February 2019)

[25] Ministry of Economy, Trade and Industry, Independent Administrative Agency Information-technology Promotion Agency “Cybersecurity Management Guidelines Ver.1.1” <http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf> (Referred on 12 February 2019)

[26] CMMI Institute “CMMI Development V2.0”
<https://cmmiinstitute.com/products/cmmi/dev> (Referred on 12 February 2019)

[27] Mary Beth Chrissis, Mike Konrad and Sandy Shrum, CMMI for Development: Guidelines for Process Integration and Product Improvement Third Edition. Addison-Wesley Professional, 2011

[28] Executive Order 13718 of February 9, 2016 “Commission on Enhancing National Cybersecurity”
<https://www.federalregister.gov/documents/2016/02/12/2016-03038/commission-on-enhancing-national-cybersecurity> (Referred on 12 February 2019)

[29] The Commission on Enhancing National Cybersecurity “Report on Securing and Growing the Digital Economy”
<https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf> (Referred on 12 February 2019)

[30] Information Security Policy Council “Cybersecurity Strategy - Toward a world-leading, resilient and vigorous cyberspace -”
<https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf> (Referred on 12 February 2019)

[31] Information Security Policy Council “Information Security Strategy for Protecting the Nation”
<https://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf> (Referred on 12 February 2019)

[32] The Government of Japan “Cybersecurity Strategy”
<https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf> (Referred on 12 February 2019)

[33] National center of Incident readiness and Strategy for Cybersecurity “Annual Report of Cybersecurity Policies (Fiscal Year 2016)” (Japanese only)
<https://www.nisc.go.jp/active/kihon/pdf/jseval_2016.pdf> (Referred on 12 February 2019)
内閣サイバーセキュリティセンター：サイバーセキュリティ政策に係る年次報告（2016 年度）（オンライン），入手先＜https://www.nisc.go.jp/active/kihon/pdf/jseval_2016.pdf＞（2017）

[34] National center of Incident readiness and Strategy for Cybersecurity “Cybersecurity 2017” (Japanese only)
<https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf> (Referred on 12 February 2019)
内閣サイバーセキュリティセンター：サイバーセキュリティ 2017（オンライン），入手先＜https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf＞（2017）

[35] Counter-Intelligence Promotion Council “Basic Strategy for Enhancing Counter-Intelligence Capabilities” (Japanese only)
<http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic_decision_summary.pdf > (Referred on 12 February 2019)
カウンターインテリジェンス推進会議：カウンターインテリジェンス機能の強化に関する基本方針（オンライン），入手先＜http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic_decision_summary.pdf＞（2007）

[36] National center of Incident readiness and Strategy for Cybersecurity “Cybersecurity 2015” (Japanese only)
<https://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf> (Referred on 12 February 2019)
内閣サイバーセキュリティセンター：サイバーセキュリティ 2015（オンライン），入手先＜https://www.nisc.go.jp/active/kihon/pdf/cs2015.pdf＞（2015）

[37] National center of Incident readiness and Strategy for Cybersecurity “Cybersecurity 2016” (Japanese only)
<https://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf> (Referred on 12 February 2019)
内閣サイバーセキュリティセンター：サイバーセキュリティ 2016（オンライン），入手先＜https://www.nisc.go.jp/active/kihon/pdf/cs2016.pdf＞（2016）

[38] National center of Incident readiness and Strategy for Cybersecurity “Cybersecurity 2018” (Japanese only)
<https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf> (Referred on 12 February 2019)
内閣サイバーセキュリティセンター：サイバーセキュリティ 2018（オンライン），入手先＜https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf＞（2018）

[39] Government of UK “National Cyber Security Strategy 2016-2021”
<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf> (Referred on 12 February 2019)

[40] Government of UK “The UK Cyber Security Strategy”
<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf> (Referred on 12 February 2019)

Research Achievement

Journals with Peer Review

J-1)

Name of Journal	: Journal of Disaster Research (Vol.13 No.5)
Publisher	: Fuji Technology Press, Ltd.
Published date	: 1 October 2018
Title	: Reviewing National Cybersecurity Strategies
Author(s)	: S. Mori & A. Goto

International Conferences with Peer Review

C-1)

Name of Conference	: Doctoral Consortium, Pacific Asia Conference on Information Systems
Organizer(s)	: Association for Information Systems (AIS), The Japan Society for Management Information (JASMIN)
Conference date	: 26-27 June 2018
Title	: Review of National Cybersecurity Strategy – Case Study: UK –
Author(s)	: S. Mori & A. Goto

Other Achievement

O-1)

Name of Journal	: Administration & Information Systems
Publisher	: Institute of Administrative Information Systems
Published date	: December 2015
Title	: Cybersecurity and Data Leakage Preventive Measures (in Japanese)
Author(s)	: S. Mori & A. Goto

O-2)

Name of Conference	: 72nd Research Workshop for Electronic Intellectual Property
Organizer(s)	: SIG Electronic Intellectual Property, IPSJ, Technical Committee on Social Implications of Technology and Information Ethics, IEICE
Conference date	: 2-3 June 2016
Title	: A Study on Web Access Log Utilization for Understanding of Organizational Climate Changes (in Japanese)
Author(s)	: E. Kamigauchi, S. Mori & A. Goto

O-3)

Name of Conference : Computer Security Symposium 2016
Organizer(s) : SIG Computer Security, IPSJ
Conference date : 11-13 October 2016
Title : Analysis on Cyber Incident of Japan Pension Service based on Cyber Kill Chain (in Japanese)
Author(s) : S. Mori et.al

O-4)

Name of Conference : Computer Security Symposium 2016
Organizer(s) : SIG Computer Security, IPSJ
Conference date : 11-13 October 2016
Title : Financial Cyber Kill Chain for Countermeasures of Financial Fraud (in Japanese)
Author(s) : S. Okada, S. Mori & A. Goto

O-5)

Name of Conference : 75th Research Workshop for Computer Security
Organizer(s) : SIG Computer Security, IPSJ
Conference date : 1-2 December 2016
Title : Cloud Services for Enterprises on Management of OS Updates for Smart Phones/Tablets (in Japanese)
Author(s) : M. Hasegawa, S. Mori & A. Goto

O-6)

Name of Conference : 170th/76th Joint Research Workshop for Distributed Processing System and Computer Security
Organizer(s) : SIG Distributed Processing System, IPSJ, SIG Computer Security, IPSJ
Conference date : 2-3 March 2017
Title : Proposal of automated OSINT Acquisition and Tag Generation System (in Japanese)
Author(s) : J. Amano et.al

O-7)

Name of Conference : 79th National Convention of IPSJ
Organizer(s) : IPSJ
Conference date : 16-18 March 2017
Title : Verification of Financial Cyber Kill Chain for Countermeasures against Financial Fraud (in Japanese)
Author(s) : S. Okada, S. Mori & A. Goto

O-8)

Name of Conference : IEICE General Conference 2018
Organizer(s) : IEICE
Conference date : 20-23 March 2018
Title : Semi-Internal Criminals in the Connected Manufacturing (in Japanese)
Author(s) : K. Nakashima, S. Mori & A. Goto

O-9)

Name of Conference : Computer Security Symposium 2018
Organizer(s) : SIG Computer Security, IPSJ
Conference date : 22-25 October 2018
Title : Assessment of National Capabilities Using the Modified 'Cybersecurity Capacity Maturity Model' (in Japanese)
Author(s) : S. Mori & A. Goto

Note

SIG : Special Interest Group
IPSJ : Information Processing Society of Japan
IEICE : The Institute of Electronics, Information and Communication Engineers

Appendices

Appendix A Cybersecurity Capacity Maturity Model for Nations Revised Edition

#	Dimension	Factor	Aspect	Start-Up	Formative
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	No national cybersecurity strategy exists, although planning processes for strategy development may have begun.	An outline/draft national cybersecurity strategy has been articulated.
				Advice may have been sought from international partners.	Processes for strategy development have been initiated.
					Consultation processes have been agreed for key stakeholder groups, including international partners.
112	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Organisation	No overarching national cybersecurity programme has been developed.	A coordinated cybersecurity programme is being developed through a multistakeholder consultative process.
					However, budgets reside in disparate public departments without a discrete cybersecurity budget line.
113	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Content	Various national policies may exist with a reference to cybersecurity, but if so, the content is generic, not necessarily aligned with national goals, and does not provide actionable directives.	Content includes links established between cybersecurity, national risk priorities and business development, but these are generally ad-hoc and lack detail.
121	Cybersecurity Policy and Strategy	Incident Response	Identification of Incidents	No catalogue of national level incidents exists, or is in development.	Certain cybersecurity incidents have been categorised and recorded as national-level threats.
122	Cybersecurity Policy and Strategy	Incident Response	Organisation	No organisation for national cyber incident response exists.	Private sector organisations key to national cybersecurity have been identified, but no formal coordination and information sharing mechanisms exist between public and private sectors.
					Dispersed public and private sector bodies detect and respond to incidents as they occur but a specific mandate for a national cyber incident response organisation is yet to be agreed.
123	Cybersecurity Policy and Strategy	Incident Response	Coordination	Coordination of incident response is informally managed within or between public and private sectors.	Leads for incident response have been designated at the operational level, but national-level coordination has not yet been established.
124	Cybersecurity Policy and Strategy	Incident Response	Mode of Operation	Key incident response processes (detection, resolution, prevention, etc.) and (digital) tools to support them have not been well defined or documented.	Key incident response processes have been identified, but not officially documented or operationalised.
				There is limited or no sufficient training or understanding of the key concepts of cybersecurity incident response.	Members of CSIRTs receive training in an ad-hoc manner.
					Incident response is reactive and ad-hoc.

(reproduced from original document)

Established	Strategic	Dynamic
A national cybersecurity strategy has been published.	Strategy review and renewal processes are confirmed.	Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments.
Multi-stakeholder consultation processes have been followed and observations fed back to the identified strategy 'owners'.	Regular scenario and realtime cyber exercises that provide a concurrent picture of national cyber resilience are considered a strategic priority.	The country is a leader within the international community and the debate shaping the development of global cybersecurity strategy.
National cybersecurity strategy is promoted and implemented by multiple stakeholders across government and other sectors.	Relevant metrics, measurement, and monitoring processes, data, and historic trends are evaluated and inform decision-making.	
	Cybersecurity strategic plans, aligned with national strategic priorities, drive capacity building and investments in security.	
The single agreed cybersecurity programme has a designated coordinating body with a mandate to consult across public and private sectors, and civil society.	Evidence exists of iterative application of metrics and resulting refinements to operations and strategy across government, including resource allocation considerations.	A singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically according to changing risk assessments.
The programme is defined according to goals and objectives, using metrics to measure progress.	A consolidated cybersecurity budget has been administered in order to allocate resources.	A designated national body disseminates and receives feedback on the strategy from wider society to continuously enhance the national cybersecurity posture.
Discrete budget for cybersecurity exists, but is not yet a part of a consolidated budget.		
The content of the national cybersecurity strategy is linked explicitly and directly to national risks, priorities and objectives, as well as business development.	Metrics and measurements are utilised to update national cybersecurity strategy content to help leaders evaluate the success of the various cybersecurity objectives and guide resource investment.	New content is periodically incorporated in the strategy in response to evolving threat landscapes.
Content at a minimum should seek to raise public awareness, mitigate cybercrime, establish incident response capability and protect critical infrastructure from external and internal threats.	Content now also seeks to protect critical infrastructure internal threats.	Content of the national cybersecurity strategy leads, promotes and encourages national and international cooperation to ensure a secure, resilient and trusted cyberspace.
A central registry of national-level cybersecurity incidents is operational.	Regular, systematic updates to the national-level incident registry are made.	Focus on incident identification and analysis is adapted in response to environmental changes.
	Resources are allocated for analysing incidents in order to prioritise which incidents are most urgent.	
A funded national body for incident response has been established (such as CSIRTs or CERTs), with specified roles and responsibilities.	Distinct and formal security roles and responsibilities are allocated across government, critical infrastructure, enterprise, and individual systems.	National incident response capability is fully financially sustainable, from a single or multiple sources.
	Human and financial resources allocated to incident response are adequate to the cybersecurity threat environment and enhance effectiveness of the organisation.	An early warning capacity is incorporated into the mission of the incident response organisation, which seeks to shape and manage the threat landscape before responding to specific incidents.
Routine and coordinated national incident response is established and published between public and private sectors, with lines of communication prepared for times of crisis.	The national incident response organisation coordinates and collaborates with subnational/ sectorial incidentresponse organisations.	Multi-level and inclusive national and international coordination between all levels and sectors is internalised as vital for continuous and effective incident response.
International cooperation for incident response between organisations exists to resolve incidents as they occur.	Technical capabilities now go beyond coordinating response and include strategically focusing resources in coordinating international incident and threat intelligence analysis/support.	Regional coordination exists to resolve incidents as they occur.
	A platform for the reporting and sharing of incidents across sectors is promoted.	
Key incident response processes and tools are defined, documented and functional.	Incident response teams have established a training policy for their members; members are being trained in specialised subjects and accredited by internationally recognised bodies on a regular basis.	The results of testing key processes through case scenarios are being analysed and are incorporated into the updating of processes.
Members of CSIRTs receive training regularly in order to understand key concepts of cybersecurity incident response.	Team members are able to carry out a sophisticated incident analysis investigation quickly and efficiently.	The benefits of training and accreditation are being evaluated and inform the future training planning.
National-level incident response is limited in scope and still reactive.	Key processes (detection, resolution, prevention, etc.) are being monitored and reviewed in regular basis, and tested with different case scenarios.	Tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities are embedded in incident response organisation(s).
	Forensics services are offered.	Mechanisms for regional cooperation in incident response have been established.
	National incident response teams coordinate with international counterparts.	

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	Some understanding of what comprises CI assets is acknowledged, but no formal categorisation of assets has been produced.	A list of general CI assets has been created.
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	There is little or no interaction between government ministries and owners of CI assets.	There is informal and ad-hoc threat and vulnerability disclosure among CI owners as well as between CI and the government, but the scope of reporting requirements has not been specified.
				No mechanism for collaboration exists.	
133	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Risk Management and Response	Risk management skills and understanding may be incorporated into business practices, but cybersecurity, if recognised, is subsumed into IT and data protection risk and is not recognised as a priority.	Physical and virtual access control is implemented.
				Response planning and threat awareness may have been broadly discussed, but no formal plan exists.	CI has basic capacity to detect, identify, respond to and recover from cyber threats, but such capabilities are uncoordinated and vary in quality.
					Protection of CI assets includes basic level cybersecurity awareness and data security policies, but no protection processes have been agreed.
141	Cybersecurity Policy and Strategy	Crisis Management	Crisis Management	It is understood that general crisis management is necessary for national security, but cybersecurity is not yet considered as a component.	A preliminary cybersecurity needs assessment of measures and techniques that require testing has been undertaken, but no exercise has been conducted at this point.
				Crisis management exercise design and planning authority may have been allocated in principle (either directly or via consultants), but cybersecurity crisis management planning has not been thoroughly outlined.	An exercise planning authority has been designated, and has outlined the steps to be taken in order to conduct the cybersecurity exercise.
					Key stakeholders and other subject matter experts, such as think tanks, academics, civil leaders and consultants are included in the planning process.
					Exercise monitors, if designated, are internal and may lack training.
151	Cybersecurity Policy and Strategy	Cyber Defence	Strategy	National security policy and Defence strategy may be published and may contain a cybersecurity component.	Specific threats to national security in cyberspace have been identified, such as external threat actors (both state and non-state), insider threats, supply chain vulnerabilities, and threats to military operational capacity, but a coherent strategy does not yet exist.
152	Cybersecurity Policy and Strategy	Cyber Defence	Organisation	Informal management of cyber Defence may be distributed among the armed forces and/or government organisations, with occasional reference to signals intelligence.	Cyber operations units are incorporated into the different branches of the armed forces, but no central command and control structure exists.

Established	Strategic	Dynamic
A detailed audit of CI assets as it relates to cybersecurity is performed on a regular basis.	CI risks and assets have been prioritised according to vulnerability and impact, which guides strategic investment.	Priority listing of CI assets is regularly re-appraised to capture changes in the threat environment.
CI asset audit lists are disseminated to relevant stakeholders.	Vulnerability/asset management processes are in place so that incremental security improvements can be made.	
A mechanism is established for regular vulnerability disclosure with defined scope for reporting incidents (either mandatory or voluntary) between CI asset owners and the government.	There is a clear understanding of which threats to CI are managed centrally, and which are managed locally.	Owners of critical infrastructure and assets are able to rapidly respond to the changing threat landscape.
Formal internal and external CI communication strategies have been defined and are consistent across sectors, with clear points of contact.	A public awareness campaign to facilitate the CI communication strategy is established with a point of contact for this information.	Trust has been established between the government and CIs with respect to cybersecurity and exchange of threat information, which is fed into the strategic decision-making process.
Strategic engagement between government and CI is agreed and promoted.	Cybersecurity requirements and vulnerabilities in CI supply chains are clearly identified, mapped and managed.	
Best practices in security measures, guidelines, and standards for CI cybersecurity have been established and adopted.	Cybersecurity is firmly embedded into general risk management practice.	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of CI risk portfolio, technologies, policies and processes.
Cybersecurity risk management processes have been established, supported by adequate technical security solutions, communication links, and harm mitigation measures.	Assessment of the breadth and severity of harm incurred by CI assets is regularly conducted and response planning is tailored to that assessment to ensure business continuity.	The impact of cybersecurity risk on the business operations of CI, including direct and opportunity costs, impact on revenue, and hindrance to innovation, are understood and incorporated into future planning and executive decision making.
CI risk management procedures are used to create a national response plan including the participation of all vital entities.	Resources are allocated in proportion to the assessed impact of an incident to ensure rapid and effective incident response.	
	Insider threat detection is accounted for.	
A cybersecurity exercise, with limited size and geographic scope has been conducted involving all relevant stakeholders in all sectors.	A realistic high-level scenario informs a plan to test information flows, decision-making and resource investment at the national level.	The exercise involves neutral peer stakeholders to observe, and, where appropriate, contribute, and addresses international challenges to produce scalable results for international policy- and decision-making.
Appropriate resources have been allocated to the exercises.	Trust is developed well in advance via the recruitment and pre-exercise briefing process and through guaranteed confidentiality control.	An evaluation of the crisis management exercise is provided for the international community, so that lessons learnt can contribute toward a global understanding of crisis management.
Planning process includes the engagement of participants, an outline of their role in the exercise, and the articulation of benefits and incentives for participation.	Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance key indicators (PKI) inform decisions in crisis management, and evaluation results inform future investment in national cybersecurity capacity.	Crisis management is embedded in risk analysis, review and management.
Trained internal or external monitors facilitate the exercise.	Findings are evaluated against international crisis management good practice.	
The exercise is evaluated and commentary is provided by participants and stakeholders.	Tailored, sector-specific reports are prepared for each stakeholder, while ensuring sensitive information is secured.	
National cyber Defence policy or strategy exists and outlines the country's position in its response to different types and levels of cyber-attacks (for example, cyber-enabled conflict producing a kinetic effect and offensive cyber-attacks aimed to disrupt infrastructure).	Resources dedicated toward Cyber Defence are allocated based on national strategic objectives.	The policy or strategy drives the international discussion on rules of engagement in cyberspace.
	The evolving threat landscape in cybersecurity is captured through repeated review in order to ensure that cyber Defence ways and means continue to meet national security objectives.	Rules of engagement are clearly defined and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the cybersecurity environment.
There is a defined organisation within the Defence apparatus responsible for conflict using cyber means.	Highly specialised expertise with advanced capabilities and full situational awareness are integrated into the national defence posture.	The Defence apparatus contributes to the debate in developing a common international understanding of the point at which a cyber-attack might trigger a cross-domain response.

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
153	Cybersecurity Policy and Strategy	Cyber Defence	Coordination	No, or limited, capacity for coordinated cyber Defence exists between domestic stakeholders (e.g. law enforcement, public, and enterprise, private) or interstate stakeholders (e.g. allied or neutral states).	Cyber Defence capability requirements are agreed between the public and private sector in order to minimise the threat to national and international security.
161	Cybersecurity Policy and Strategy	Communications Redundancy	Communications Redundancy	Digital redundancy measures may be considered, but not in a systematic, comprehensive fashion.	Stakeholders convene to identify gaps and overlaps in emergency response asset communications and authority links.
				Current emergency response assets may have been identified, but lack any level of integration.	Emergency response assets, priorities and standard operating procedures are mapped and identified in the event of a communications disruption along any node in the emergency response network.
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	Government has no or minimal recognition of the need to prioritise a cybersecurity mind-set.	Leading agencies have begun to place priority on cybersecurity, by identifying risks and threats.
				Leading agencies within government may have begun to consider cybersecurity.	
212	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	The private sector has no or minimal recognition of the need to prioritise a cybersecurity mind-set.	Leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices.
					Programmes and materials have been made available to train and improve cybersecurity practices.
213	Cyber Culture and Society	Cybersecurity Mind-set	Users	Users have no or minimal recognition of the need to prioritise a cybersecurity mind-set and take no proactive steps to improve their cybersecurity.	A limited proportion of Internet users have begun to place priority on cybersecurity, by identifying risks and threats.
221	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	Most Internet users have blind trust on websites and regarding what they see or receive online.	A very limited proportion of Internet users critically assess what they see or receive online and believe that they have the ability to use the Internet and protect themselves online.
				Operators of Internet infrastructure may consider measures promoting trust in online services.	A limited proportion of users trust in the secure use of the Internet based on indicators of website legitimacy.
					Operators of Internet infrastructure develop measures to promote trust in online services but have not established them.

Established	Strategic	Dynamic
The entity in charge of cyber Defence coordinates integration regarding cyber events between government, military and critical infrastructure and identifies clear roles and responsibilities.	Analytical capacity exists to support the coordination of resource allocation for national cyber Defence; possibly including a cyberdefence research centre.	The country is leading the international debate on cyber Defence and systematically shares intelligence with allies.
Defence organisations and critical infrastructure providers have established a mechanism to report threat intelligence.	The understanding of strengths and weaknesses within the coordination mechanism then feeds into the re-evaluation of the national security posture of the nation.	
Emergency response assets are hardwired into a national emergency communication network.	Outreach and education of redundant communications protocols is undertaken for key stakeholders and is tailored to their unique roles and responsibilities.	Optimised efficiency is in place to mediate extended outages of systems.
Communication is distributed across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.	Emergency response assets practice interoperability and function effectively under compromised communications scenarios.	National-level assets can act to assist neighbours in the event of an internationallevel crisis or incident.
Appropriate resources are allocated to hardware integration, technology stress testing, personnel training and crisis simulations drills.	The results of these scenarios then inform strategic investment in future emergency response assets.	
	Stakeholders contribute to international efforts on redundancy communication planning.	
Most government officials at all levels are aware of cybersecurity good practices.	Agencies across all levels of government have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit.	The cybersecurity mind-set serves as a foundation for government official's operational practices and is evidenced as global good practice.
	Cybersecurity mind-set informs strategic planning.	Cybersecurity mind-set of government officials is related to a reduction of the overall threat landscape of the government.
Most private sector actors at all levels are aware of cybersecurity good practices.	Most private sector actors, including SMEs, have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit.	The cybersecurity mind-set serves as a foundation for private sector operational practices, informs all IT related initiatives and is evidenced as global good practice.
	Cybersecurity mind-set, informs strategic planning.	Cybersecurity mind-set of the private sector is related to a reduction of the overall threat landscape of the sector.
A growing number of users feel it is a priority for them to employ good cybersecurity practices and make conscious efforts to securely use online systems.	Most users have routinized a cybersecurity mind-set, employing secure practices as a matter of habit.	Cybersecurity mind-set of users is related to a reduction of the overall threat landscape of the country.
A growing proportion of Internet users critically assess what they see or receive online, based on identifying possible risks.	Most Internet users critically assess what they see or receive online, based on identifying possible risks.	Individuals assess the risk in using online services, including changes in the technical and cybersecurity environment and continuously adjust their behaviour based on this assessment.
A growing proportion of users trust in the secure use of the Internet based on indicators of website legitimacy.	Most Internet users feel confident while using the Internet, have the ability to recognise non-legitimate websites (including mimicry attempts), and have a sense of control over providing personal data online.	Internet infrastructure operators assess trust promotion services and integrate findings into programme and policy revision.
Internet infrastructure operators have established programmes to promote trust in online services.	Programmes to promote trust in the use of online services are assessed based on measures of effectiveness which informs resource allocation.	
User-consent policies are in place designed to notify practices on the collection, use or disclosure of sensitive personal information.		

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
222	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-government Services	Government offers no or limited e-services, but has not publicly promoted the necessary secure environment.	Government continues to increase e-service provision, but also recognises the need for the application of security measures to establish trust in these services.
				If e-government services are provided, users are unfamiliar with or lack trust in them.	The need for security in e-government services is recognised by stakeholders and users.
					A limited proportion of users trust in the secure use of e-government services.
					Some e-government services are informing users of the utility of deployed security solutions.
223	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-commerce Services	E-commerce services are not offered or are offered in an unsecure environment.	E-commerce services are being provided to a limited extent.
				If e-commerce services are provided, users are unfamiliar with or lack trust in them.	The private sector recognises the need for the application of security measures to establish trust in e-commerce services.
					A limited proportion of users trust in the secure use of e-commerce services.
					Some e-commerce services are informing users of the utility of deployed security solutions.
231	Cyber Culture and Society	User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	Users and stakeholders within the public and private sectors have no or minimal knowledge about how personal information is handled online, nor do they believe that adequate measures are in place to protect their personal information online.	Users and stakeholders within the public and private sectors may have general knowledge about how personal information is handled online; and may employ good (proactive) cybersecurity practices to protect their personal information online.
				There is no or limited discussion regarding the protection of personal information online.	Discussions have begun regarding the protection of personal information and about the balance between security and privacy, but this has not resulted in concrete actions or policies.
				Discussions may have begun and involve multiple stakeholders, but no privacy standards are in place.	
241	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	There are no reporting mechanisms available, but discussions might have begun.	The public and/or private sectors are providing some channels for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents, but these channels are not coordinated and are used in an ad-hoc manner.
					Promotion of the existing reporting channels has not yet begun or is ad-hoc.

Established	Strategic	Dynamic
E-government services have been fully developed.	Public authorities are routinely publishing certain information about their activities.	E-government services and promotion thereof are continuously improved and expanded to enhance transparent/open and secure systems and user trust.
High-level risks affecting egovernment services are prioritised in order to reduce occurrences.	Privacy-by-default is promoted as a tool for transparency in e-government services.	Impact assessments on data protection in e-government services are consistently taking place and feed back into strategic planning.
The public sector promotes use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users.	The majority of users trust in the secure use of e-government services and make use of them.	
A growing proportion of users trust in the secure use of e-government services.	Processes are employed for gathering user feedback in order to ensure efficient management of online content.	
Possible breaches in egovernment services are being identified, acknowledged, and disclosed in an ad-hoc manner.		
E-commerce services are fully established by multiple stakeholders in a secure environment.	E-commerce service providers recognise the need for building trust in order to ensure business continuity, and resources are allocated accordingly.	E-commerce services are continuously improved in order to promote transparent, trustworthy and secure systems.
Security solutions are updated and reliable payment systems have been made available.	The majority of users trust in the secure use of e-commerce services and make use of them.	Terms and conditions provided by e-commerce services are clear and easily comprehensible to all users.
A growing proportion of users trust in the secure use of e-commerce services.	Stakeholders invest in establishing enhanced service functionality of e-commerce services, protection of personal information and the provision of feedback mechanisms for users.	User feedback mechanisms are integrated into e-commerce services in order to enhance trust between users and providers.
The private sector promotes use of e-commerce services and trust in these services.		
Terms and conditions of use of e-commerce services are easily accessible.		
A growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others.	All stakeholders have the information, confidence and the ability to take measures to protect their personal information online and to maintain control of the distribution of this information.	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment.
There is constant public debate regarding the protection of personal information and about the balance between security and privacy, which informs privacy policies within public and private sectors.	Users and stakeholders within the public and private sectors widely recognise the importance of protection of personal information online, and are sensitised to their privacy rights.	There is a wide recognition of the need to ensure security and protection of personal information.
	Mechanisms are in place in private and public sectors to ensure that privacy and security are not competing.	Policies are in place in private and public sectors to ensure that privacy and security are not competing in a changing environment and are informed by user feedback and public debate.
	Privacy by default as a tool for transparency is promoted.	Assessments of personal information protection in eservices are regularly conducted and feed back into policy revision.
Reporting mechanisms have been established and are regularly used.	Coordinated reporting mechanisms are widely used.	All relevant stakeholders actively collaborate and share good practice to enhance existing reporting mechanisms and there is a clear distribution of roles and responsibilities, including regarding the response to reported incidents.
Programmes to promote the use of these mechanisms have been established by public and private sectors.	Programmes to promote the use of these mechanisms are prioritised by public and private sectors and are considered as an investment in loss prevention and risk control.	Mechanisms have been developed to coordinate response to reported incidents between law enforcement and the national incident response capability.
	Effectiveness metrics of reporting mechanisms are applied and findings inform the revision and promotion of the mechanisms.	

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
251	Cyber Culture and Society	Media and Social Media	Media and Social Media	Media and social media rarely, if ever, cover information about cybersecurity or report on issues such as security breaches or cybercrime.	There is ad-hoc media coverage of cybersecurity, with limited information provided and reporting on specific issues that individuals face online, such as online child protection or cyber-bullying.
					There is limited discussion on social media about cybersecurity.
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	The need for awareness of cybersecurity threats and vulnerabilities across all sectors is not recognised, or is only at initial stages of discussion.	Awareness raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and/or civil society sources, but no coordination or scaling efforts have been conducted.
					Awareness raising programmes may be informed by international initiatives but are not linked to national strategy.
312	Cybersecurity Education, Training and Skills	Awareness Raising	Executive Awareness Raising	Awareness raising on cybersecurity issues for executives is limited or nonexistent.	Executives are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisation.
				Executives are not yet aware of their responsibilities to shareholders, clients, customers, and employees in relation to cybersecurity.	Executives of particular sectors, such as finance and telecommunications, have been made aware of cybersecurity risk in general and how the organisation deals with cybersecurity issues, but not of strategic implications.
321	Cybersecurity Education, Training and Skills	Framework for Education	Provision	Few or no cybersecurity educators are available, and there are no qualification programmes for educators.	Qualification programmes for cybersecurity educators are being explored, with a small cadre of existing professional educators.
				Computer science courses are offered that may have a security component, but no cybersecurity-related courses are offered.	Some educational courses exist in cybersecurityrelated fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered.
				No accreditation in cybersecurity education exists.	A demand for cybersecurity education is evidenced through course enrolment and feedback.

Established	Strategic	Dynamic
Cybersecurity is a common subject across mainstream media, and information and reports on a wide range of issues, including security breaches and cybercrime are widely disseminated.	Media coverage extends beyond threat reporting and can inform the public of proactive and actionable cybersecurity measures, as well economic and social impacts.	The broad discussion of personal experiences and personal attitudes of individuals across mainstream and social media inform policy making and facilitate societal change.
There is broad discussion on social media about cybersecurity.	There is frequent discussion on social media about cybersecurity and individuals regularly exchange experiences online using social media.	
A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) is established, which addresses a wide range of demographics and issues, but no metrics for effectiveness have been applied.	The national awareness raising programme is coordinated and integrated with sector-specific, tailored awareness raising programmes, such as those focusing on government, industry, academia, civil society, and/or children.	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments.
Consultation with stakeholders from various sectors informs the creation and utilisation of programmes and materials.	Metrics for effectiveness are established and evidence of application and lessons learnt are fed into future programmes.	Metrics contribute toward national cybersecurity strategy revision processes.
A single online portal linking to appropriate cybersecurity information exists and is disseminated via that programme.	The evolution of the programme is supported by the adaptation of existing materials and resources, involving clear methods for obtaining a measure of suitability and quality.	Awareness programme planning gives explicit consideration to national demand from the stakeholder communication (in the widest sense), so that campaigns continue to impact the entire society.
	Programmes contribute toward expanding and enhancing international awareness raising good practice and capacitybuilding efforts.	The national awareness raising programme has a measurable impact on reduction of the overall threat landscape.
Awareness raising of executives in the public, private, academic and civil society sectors address cybersecurity risks in general, some of the primary methods of attack, and how the organisation deals with cyber issues (usually abdicated to the CIO).	Executive awareness raising efforts in nearly all sectors include the identification of strategic assets, specific measures in place to protect them, and the mechanism by which they are protected.	Cybersecurity risks are considered as an agenda item at every executive meeting, and funding and attention is reallocated to address those risks.
Select executive members are made aware of how cybersecurity risks affect the strategic decision making of the organisation, particularly those in the financial and telecommunications sectors.	Executives are able to alter strategic decision making, and allocate specific funding and people to the various elements of cyber risk, contingent on their company's prevailing situation.	Executives are regarded regionally and internationally as a source of good practice in responsible and accountable corporate cybersecurity governance.
Awareness raising efforts of cybersecurity crisis management at the executive level is still reactive in focus.	Executives are made aware of what contingency plans are in place to address various cyber-based attacks and their aftermath.	
	Executive awareness courses in cybersecurity are mandatory for nearly all sectors.	
Qualifications for and supply of educators are readily available in cybersecurity.	Cybersecurity educators are not only drawn from the academic environment, but incentives are in place so that industry and/or government experts take these positions as well.	National courses, degrees, and research are at the forefront of cybersecurity education internationally.
Specialised courses in cybersecurity are offered and accredited at the university level.	Accredited cybersecurity courses are embedded in all computer science degrees.	Cybersecurity education programmes maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cybersecurity environment.
Degrees in cybersecurityrelated fields are offered by universities.	Degrees are offered in cybersecurity specifically, which encompasses courses and models in various other cybersecurity-related fields, including technical and nontechnical elements such as policy implications, and multi-disciplinary education.	Prevailing cybersecurity requirements are considered in the redevelopment of all general curricula.
Universities and other bodies hold seminars/lectures on cybersecurity issues aimed at non-specialists.	Cybersecurity educational offerings are weighted and focused based on an understanding of current risks and skills requirements.	
Research and development is a leading consideration in cybersecurity education.	Cybersecurity education is not limited to universities, but ranges from primary to post-graduate levels, including vocational education.	

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
322	Cybersecurity Education, Training and Skills	Framework for Education	Administration	The need for enhancing national cybersecurity education is not yet considered.	The need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders.
				A network of national contact points for governmental, regulatory bodies, critical industries and education institutions is not yet established.	Schools, government, and industry collaborate in an ad-hoc manner to supply the resources necessary for providing cybersecurity education.
				Discussion of how coordinated management of cybersecurity education and research enhances national knowledge development has not, or only just begun.	A national budget focused on cybersecurity education is not yet established.
331	Cybersecurity Education, Training and Skills	Framework for Professional Training	Provision	Few or no training programmes in cybersecurity exist.	The need for training professionals in cybersecurity has been documented at the national level.
					Training for general IT staff is provided on cybersecurity issues so that they can react to incidents as they occur, but no training for dedicated security professionals exists.
					ICT professional certification is offered, with some security modules or components.
					Ad-hoc training courses, seminars and online resources are available for cybersecurity professionals through public or private sources, with limited evidence of take-up.
332	Cybersecurity Education, Training and Skills	Framework for Professional Training	Uptake	Training uptake by IT personnel designated to respond to cybersecurity incidents is limited or nonexistent.	Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings exist, but are limited in scope.
					There is no knowledge transfer from employees trained in cybersecurity to untrained employees.
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	Legislation relating to ICT security does not yet exist.	Experienced stakeholders from all sectors may have been consulted to support the establishment of a legal and regulatory framework.
				Efforts to draw attention to the need to create a legal framework on cybersecurity have been made and may have resulted in a gap analysis.	Key priorities for creating cybersecurity legal frameworks have been identified through multistakeholder consultation, potentially resulting in draft legislation, but legislation has not yet been adopted.
412	Legal and Regulatory Frameworks	Legal Framework	Privacy, Freedom of Speech & Other Human Rights Online	Domestic law does not recognise fundamental human rights in relation to cybercrime.	Domestic legislation partially recognises privacy, freedom of information, freedom of assembly and association, and freedom of expression online.
				Discussions of privacy issues online may have begun and include multiple stakeholders, but no privacy legislation or standards are in place.	Stakeholders from all key sectors have been consulted for the development of legislation addressing human rights online.

Established	Strategic	Dynamic
Broad consultation across government, private sector, academia and civil society stakeholders informs cybersecurity education priorities and is reflected in national cybersecurity strategy.	Metrics are developed to ensure that educational investments meet the needs of the cybersecurity environment across all sectors.	International cybersecurity centres of excellence are established through twinning programmes led by world class institutions.
National budget is dedicated to national cybersecurity research and laboratories at universities.	Government budget and spending on cybersecurity education is managed based on the national demand.	Routinized cooperation between all stakeholders in cybersecurity education can be evidenced.
Competitions and initiatives for students are promoted by government and/or industry in order to increase the attractiveness of cybersecurity careers.	Leading national cybersecurity academic institutions share their lessons learnt with other national and international counterparts.	Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges, and provides a mechanism for enhancing curriculum based on the evolving landscape.
	Government has established academic centres of excellence in cybersecurity.	
Structured cybersecurity training programmes exist to develop skills towards building a cadre of cybersecurity-specific professionals.	A range of cybersecurity training courses is tailored toward meeting national strategic demand and aligns with international good practice.	The public and private sector collaborate to offer training, constantly adapting and seeking to build skillsets drawn from both sectors.
Security professional certification is offered across sectors within the country.	The training programme outlines the priorities in the national cybersecurity strategy.	Training offerings coordinate with education programmes so that the foundation established in schools can enable training programmes to build a highly skilled workforce.
The needs of society are well understood and a list of training requirements is documented.	Training programmes are offered to cybersecurity professionals that focus on the skills necessary to communicate technically complex challenges to nontechnical audiences, such as management and general employees.	Programmes and incentive structures are in place to ensure the retention of trained workforce within the country.
Training programmes for non-cybersecurity professionals are recognised and initially offered.	Metrics of effectiveness assess the modes and procedures of training.	
There is an established cadre of certified employees trained in cybersecurity issues, processes, planning and analytics.	The uptake of cybersecurity training is used to inform future training programmes.	Cybersecurity professionals not only fulfil national requirements, but domestic professionals are consulted internationally to share lessons learnt and good practice.
Knowledge transfer from employees trained in cybersecurity to untrained employees is ad hoc.	Coordination of training across all sectors ensures the national demand for professionals is met.	
Job creation initiatives for cybersecurity within organisations are established and encourage employers to train staff to become cybersecurity professionals.		
Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been adopted.	The country reviews existing legal and regulatory mechanisms for ICT security, identifies where gaps and overlaps exist, and amends laws accordingly or enacts new laws.	Mechanisms are in place for continuously harmonising ICT legal frameworks with national cybersecurityrelated ICT policies, international law, standards and good practices.
Laws address the protection of critical information infrastructure, etransactions, liability of Internet Service Providers and, potentially, cyber incident reporting obligations.	Monitoring of enforcement of legislative frameworks informs resource allocation and legal reform.	Participation in the development of regional or international cybersecurity cooperation agreements and treaties is a priority.
		Efforts are in place to exceed minimal baselines specified in these treaties where appropriate.
Domestic law recognises fundamental human rights on the Internet, including privacy online, freedom of speech, freedom of information, and freedom of assembly and association.	International and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and associated resource planning.	In order to meet dynamic changes in the application of technology to human rights, procedures are in place to amend and update legal frameworks as needed.
Domestic law specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information in investigations involving electronic evidence.	Research is conducted and measures are in place to exceed minimal baselines specified in international agreements.	Access to the Internet is recognised and enshrined as a human right.
All relevant actors from private sector and civil society are involved in shaping laws and regulations on privacy, freedom of speech, and other human rights online.		The state is an active contributor in the global discourse on human rights on the Internet.
The country has ratified or acceded to international agreements.		Domestic actors, policies and practices actively shape positive international discussions of privacy online.

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
413	Legal and Regulatory Frameworks	Legal Framework	Data Protection Legislation	Data protection legislation is not yet under development.	Data protection legislation is under development.
				Public discourse on data protection issues may have begun and includes multiple stakeholders.	Stakeholders from all key sectors have been consulted to support the development of legislation.
414	Legal and Regulatory Frameworks	Legal Framework	Child Protection Online	Legislation protecting children online is not yet under development.	Legislative provisions protecting children online are under development.
				Public discourse on child protection online may have begun and includes multiple stakeholders.	Stakeholders from all key sectors have been consulted to support the development of legislation.
415	Legal and Regulatory Frameworks	Legal Framework	Consumer Protection Legislation	Legislation protecting consumers against online fraud and other forms of cybercrime is not yet under development.	Legislation protecting consumers online is under development.
					Stakeholders from all key sectors have been consulted to support the development of legislation.
416	Legal and Regulatory Frameworks	Legal Framework	Intellectual Property Legislation	Intellectual property of online products and services might be discussed among multiple stakeholders, but no specific legal provisions are in place.	Legislation on intellectual property online is under development, through consultation with key stakeholders.
				If general law on intellectual property exists, it is not applicable to online products and services yet.	
417	Legal and Regulatory Frameworks	Legal Framework	Substantive Cybercrime Legislation	Specific substantive criminal law on cybercrime does not exist or general criminal law exists, but its application to cybercrime is unclear.	Partial legislation exists that addresses some aspects of cybercrime or cybercrime legal provisions are under development.
				Specific substantive criminal provisions on cybercrime might be discussed among lawmakers, but the development of the provisions has not yet commenced.	
418	Legal and Regulatory Frameworks	Legal Framework	Procedural Cybercrime Legislation	Specific procedural criminal law for cybercrime does not exist and general criminal procedural law is not applicable to cybercrime investigations, prosecutions, and electronic evidence.	Development of specific procedural cybercrime legislation or amendment of general procedural criminal law to adapt to cybercrime cases has begun.
				Procedural criminal legislation for cybercrime might be discussed among lawmakers, but development of the legislation has not yet begun.	
421	Legal and Regulatory Frameworks	Criminal Justice System	Law Enforcement	Law enforcement does not have sufficient capacity to prevent and combat cybercrime and does not receive specialised training on cybercrime investigations.	Traditional investigative measures are applied to cybercrime investigations, with limited digital forensics capacity.
					If law enforcement officers receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.
422	Legal and Regulatory Frameworks	Criminal Justice System	Prosecution	Prosecutors do not receive adequate training and resources to review electronic evidence or prosecute cybercrime.	A limited number of specialised cybercrime prosecutors have the capacity to build a case based on electronic evidence, but this capacity is largely ad-hoc and uninstitutionalised.
				There are no specialised cybercrime prosecutors, but consultation may have begun to consider this capacity within the criminal justice community.	If prosecutors receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.

Established	Strategic	Dynamic
Comprehensive data protection legislation has been adopted and enforced, which includes conditions for the collection of personal data and protection from misuse.	Legal mechanisms are in place that enable strategic decision making that determines the timeframe in which personal data is no longer required as evidence for investigation and must be deleted.	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
	International and regional trends and good practices inform the assessment and amendment of data protection laws and associated resource planning.	
Comprehensive legislation on the protection of children online has been adopted and enforced, and ensures that data protection and privacy rules for legal minors apply to the online environment.	The country continuously seeks to improve national child protection online legislation to comply with regional and international law and standards.	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
Comprehensive legislation protecting consumers from business malpractice online has been adopted and is enforced.	The country continuously seeks to improve national consumer protection legislation to address national needs and comply with regional and international consumer protection standards.	In order to meet dynamic changes in the application of technology to consumer protection, procedures are in place to amend and update legal frameworks as needed.
A lead agency responsible for the protection of consumers online has been designated.		
Comprehensive legislation addressing intellectual property of online products and services has been adopted and is enforced.	Legislation on intellectual property online is regularly reviewed and amended accordingly to reflect changes in national priorities and the international ICT landscape.	Decisions to update legislation are based on the balance between intellectual property and open access policies, through multi-stakeholder discussion.
	Legislative amendments are informed by multistakeholder consultations and public discourse.	
Substantive cybercrime legal provisions are contained in specific legislation or a general criminal law.	Measures are in place to exceed minimal baselines specified in international treaties where appropriate, which includes procedures to amend substantive legal frameworks as needed.	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties.
The country has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.		Laws, where needed, are amended to reflect changes in the international ICT environment.
Comprehensive criminal procedural law containing provisions on the investigation of cybercrime and evidentiary requirements has been adopted and is enforced.	In the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully investigate cybercrime.	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties.
The state has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.	Measures are in place to exceed minimal baselines specified in international treaties where appropriate, which includes procedures to amend procedural legal frameworks as needed.	Procedural law, where needed, is amended to adapt to the changing cybercrime landscape and emerging investigative challenges.
A comprehensive institutional capacity with sufficient human, procedural and technological resources to investigate cybercrime cases has been established.	Resources dedicated to fully operational cybercrime units have been allocated based on strategic decision making.	All law enforcement officers receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
Digital chain of custody and evidence integrity is established including formal processes, roles and responsibilities.	Advanced investigative capabilities allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.	Law enforcement can utilise sophisticated digital forensic tools, and these technologies are consistently updated.
Standards for the training of law enforcement officers on cybercrime exist and are implemented.	Law enforcement agencies have the resources to maintain the integrity of data to meet international evidential standards in cross-border investigation.	The institutional capacity of law enforcement is frequently reviewed and revised based on an assessment of effectiveness.
	Statistics and trends on cybercrime investigations are collected and analysed.	
A comprehensive institutional capacity, including sufficient human, training and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established.	Institutional structures are in place, with a clear distribution of tasks and obligations within the prosecution services at all levels of the state.	There is national capacity to prosecute complex domestic and cross-border cybercrime cases.
	Statistics and trends on cybercrime prosecutions are constantly collected and analysed.	A dedicated cybercrime prosecution unit might have been established.
	A mechanism exists that enables the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.	All prosecutors receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
423	Legal and Regulatory Frameworks	Criminal Justice System	Courts	A separate court structure or specialized judges for cybercrime cases and cases involving electronic evidence do not exist.	A limited number of judges have the capacity to preside over a cybercrime case, but this capacity is largely adhoc and not systematic.
				Consultation may have begun to consider this capacity in the judicial community.	If judges receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.
431	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	No or minimal forms of international cooperation exist to prevent and combat cybercrime.	Formal mechanisms of international cooperation have been established, but the application to cybercrime is ad-hoc or only possible in some cases.
				There is no formal mechanism that promotes the exchange of information between domestic public and private sectors on cybercrime and cooperation is limited.	Exchange of information on cybercrime between domestic public and private sectors is ad-hoc and unregulated.
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Informal Cooperation	There is minimal interaction between government and criminal justice actors.	Exchange of information between government and criminal justice actors is limited and ad-hoc.
				Cooperation between Internet Service Providers and law enforcement has not been established.	Ad-hoc cooperation between Internet Service Providers and law enforcement exists, but is not always effective.
				Law enforcement cooperation with foreign counterparts is not effective.	Law enforcement cooperates with foreign counterparts on an ad-hoc basis, but is not integrated in regional and international networks.
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	No standards or good practices have been identified for use in securing data, technology or infrastructure, by the public and private sectors.	Information risk management standards have been identified for use and there have been some initial signs of promotion and take-up within public and private sectors.
				Or, initial identification of some appropriate standards and good practices has been made by the public and private sectors, possibly some ad hoc implementation, but no concerted endeavour to implement or change existing practice in a measurable way.	There is some evidence of measurable implementation and adoption of international standards and good practices.
512	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	No standards or good practices have been identified for use in guiding procurement processes by the public and private sector.	Cybersecurity standards and good practices guiding procurement processes have been identified for use.
				If they are recognised, implementation is ad hoc and uncoordinated.	Evidence of promotion and adoption of cybersecurity standards and good practices in defining procurement practices exists within public sectors and private sectors.

Established	Strategic	Dynamic
Sufficient human and technological resources are available to ensure effective and efficient legal proceedings regarding cybercrime cases, and cases involving electronic evidence.	The court system has organised itself to ensure a central management of cybercrime cases, with clear distribution of tasks and obligations within the court system at all levels of the state.	Judges receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
Judges receive specialised training on cybercrime and electronic evidence.	Statistics and trends on cybercrime convictions are collected and analysed.	The institutional capacity of the court system is frequently reviewed and revised based on an assessment of effectiveness.
Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution.	Formal international cooperation mechanisms are fully functional, with established communication channels.	Formal international cooperation mechanisms are regularly reviewed to determine effectiveness, and are revised accordingly to reflect the changing cybercrime landscape.
Mutual legal assistance and extradition agreements and mechanisms have been established and are applied to cybercrime cases.	Strategic decisions are made to expand and enhance formal cooperation mechanisms on cybercrime as needed.	Formal and informal international cooperation mechanisms complement each other and are interoperable.
Legislative requirements for the exchange of information between domestic public and private sectors have been determined.	Resources are allocated to support the exchange of information between public and private sectors domestically and enhance legislative requirements and communication mechanisms.	Formal mechanisms that enable the exchange of information between domestic public and private sectors are adapted in accordance with identified needs and changing threat environment.
Informal relationships between government and criminal justice actors have been established, resulting in the regular exchange of information on cybercrime issues.	A strategic relationship between government actors, prosecutors, judges and law enforcement agencies has been established relating to cybercrime.	Government and criminal justice actors exchange information timely and efficiently, and cooperation is adapted to the changing cybercrime environment and associated requirements.
Effective informal cooperation mechanisms between Internet Service Providers and law enforcement have been established, with clear communication channels.	Law enforcement cooperates with domestic and foreign ISPs in combatting cybercrime.	A routinized relationship between law enforcement and ISPs, domestically and across borders, has been established and is adaptable to emerging forms of cybercrime.
Domestic law enforcement agencies are informally integrated with regional and international counterparts and networks, such as Interpol or 24/7 networks.	Law enforcement agencies work jointly with foreign counterparts, potentially through joint task forces, resulting in successful crossborder cybercrime investigations and prosecutions.	Formal and informal international cooperation mechanisms complement each other and are interoperable.
Nationally agreed baseline of cybersecurity related standards and good practices has been identified, and adopted widely across public and private sectors.	Government and organisations promote adoption of standards and good practises according to assessment of national risks and budgetary choices.	The choice of adopted standards and good practices and their implementation is continuously improved.
Some body within government exists to assess level of adoption across public and private sectors.	There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drive standard adoption.	Adoption of standards and non-compliance decisions are made in response to changing threat environments and resource drivers across sectors and CI through collaborative risk management.
Government schemes exist to promote continued enhancements, and metrics are being applied to monitor compliance.	Evidence of contribution to international standards' bodies exists and contributes to thought leadership and sharing of experience by organisations.	Evidence exists of debate within all sectors on compliance to standards and good practices, based on continuous needs assessments.
Consideration is being given to how standards and good practices can be used to address risk within supply chains within the CI, by both government and CI.		
Procurement practices meet international IT guidelines, standards and good practices.	Cybersecurity standards and good practices in guiding procurement processes are being adhered to widely within public and private sectors.	Organisations have the ability to monitor use of standards and good practices in procurement processes and support deviations and noncompliance decisions in real-time through risk-based decision making and quality assurance.
Adoption and compliance of standards in procurement practices within the public and private sectors, is evidenced through measurement and assessments of process effectiveness.	Critical aspects of procurement and supply, such as prices and costs, quality, timescales and other value adding activities are continuously improved, and procurement process improvements are made in the context of wider resource planning.	
	Organisations are able to benchmark the skills of their procurement professionals against the competencies outlined in procurement standards and identify any skills and capability gaps.	
	Internal stakeholders have been trained in the secure use of E-sourcing or E-tendering systems and purchase-to-pay systems (P2P) in order to implement these tools in performing key tasks in procurement and supply.	

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
513	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	No standards or good practices for software development have been identified for use relating to integrity and resilience in public and private sectors.	Core activities and methodologies for software development processes focused on integrity and resilience are being discussed within professional communities.
				Or, there is some identification, but only limited evidence of take-up.	Government promotes relevant standards in software development, but there is no widespread use of these standards yet.
					Some organisations supply or seek to adopt standards in code development.
521	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	Affordable and reliable Internet services and infrastructure in the country may have not yet been established; if they have been, adoption rates of those services are a concern.	Limited Internet services and infrastructure are available, but may not be reliable.
				There is little or no national control of network infrastructure; networks and systems are outsourced, with potential adoption from unreliable third-party markets.	Resilience of Internet infrastructure in public and private sectors has been discussed by multiple stakeholders, but has not been fully addressed.
					There may be regional support to secure Internet infrastructure in the country.
531	Standards, Organisations, and Technologies	Software Quality	Software Quality	Quality and performance of software used in the country is a concern, but functional requirements are not yet fully monitored.	Software quality and functional requirements in public and private sectors are recognised and identified, but not necessarily in a strategic manner.
				A catalogue of secure software platforms and applications within the public and private sectors does not exist.	A catalogue for secure software platforms and applications within the public and private sectors is under development.
				Policies and processes regarding updates of software applications have not yet been formulated.	Policies and processes on software updates and maintenance are now under development.
					Evidence of software quality deficiencies is being gathered and assessed regarding its impact on usability and performance.
541	Standards, Organisations, and Technologies	Technical Security Controls	Technical Security Controls	There is minimal or no understanding or deployment of the technical security controls offered in the market, by users, public and private sectors.	Technical security controls are deployed by users, public and private sectors, but inconsistently.
				Internet Service Providers (ISPs) may not offer any upstream controls to their customers.	The deployment of up-todate technical security controls is promoted in an ad-hoc manner and all sectors are being incentivised to their use.
					ISPs may be offering antimalware software as part of their services but possibly in an ad-hoc manner.
					ISPs recognise the need to establish policies for technical security control deployment as part of their services.
					Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed but not necessarily in a consistent manner.

Established	Strategic	Dynamic
Government has an established programme for promoting and monitoring standard adoption in software development – both for public and commercial systems.	Security considerations are incorporated in all stages of software development.	Software development projects continuously assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions.
Evidence of public and private sector organisations adopting standards in their software development processes.	Core development activities, including configuration and documentation management, security development and lifecycle planning have been adopted.	Procurement of software includes on-going assessments of the value of standards in delivering software quality – throughout the lifetime of the contract (as opposed to simply initially at procurement stage).
Evidence that high integrity systems and software development techniques are present within the educational and training offerings in the country.	Procurement of software developed according to required standards is considered based on an assessment of risk in investment decisions.	Requirements are built into contracts with suppliers.
Reliable Internet services and infrastructure have been established.	Regular assessment of processes according to international standards and guidelines are conducted together with assessment of national information infrastructure security and critical services that drive investment in new technologies.	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics.
Internet is used for ecommerce and electronic business transactions; authentication processes are established.		Costs for infrastructure technologies are continually assessed and optimised.
Technology and processes deployed for Internet infrastructure meet international IT guidelines, standards, and good practices.		There is effectively controlled acquisition of critical technologies with managed strategic planning and service continuity processes in place.
National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.		Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain the country's independent resilience.
Software quality and functional requirements in public and private sectors are recognised and established.	Quality of software used in public and private sectors is monitored and assessed.	Software applications of high level performance, reliability and usability are available, with service continuity processes fully automated.
Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors.	Policies and processes on software updates and maintenance are being improved based on risk assessments and the criticality of services.	Requirements of software quality are being systematically reviewed, updated, and adapted to the changing cybersecurity environment.
Policies on and processes for software updates are established.	Benefits to businesses from additional investment in ensuring software quality and maintenance are measured and assessed.	
Software applications are characterised as to their reliability, usability and performance in adherence to international standards and good practices.	Software defects are manageable in a timely manner and service continuity is ensured.	
Up-to-date technical security controls, including patching and backups, are deployed in all sectors.	Penetration of technical security controls leads to effective upstream protection of users and public/private sectors.	All sectors have the capacity to continuously assess the security controls deployed for their effectiveness and suitability according to their changing needs.
Users have an understanding of the importance of anti-malware software and network firewalls across devices.	Within the public and private sectors, technical security controls are being kept up-to-date, monitored for effectiveness and reviewed on a regular basis.	The understanding of the technical security controls being deployed extends to its impact on organisational operations and budget allocation.
Physical security controls are employed to prevent unauthorized personnel from entering computing facilities.	The public and private sector have the capacity to critically assess and upgrade cybersecurity controls according to their appropriateness and suitability for use.	ISPs supplement technical security controls with multi factor authentication, digital certificates and whitelisting to ensure prevention of access of non-trusted sites or web addresses and maintain a safe Internet environment.
ISPs establish policies for technical security control deployment as part of their services.		
The technical cybersecurity control set is based on established cybersecurity frameworks, such as the SANS top 20 cybersecurity controls, the CESG 10 steps to cybersecurity, or PAS 55.		

Appendix A

#	Dimension	Factor	Aspect	Start-Up	Formative
551	Standards, Organisations, and Technologies	Cryptographic Controls	Cryptographic Controls	Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit may be a concern but are not yet deployed within the government, private sector or the general public.	Cryptographic controls for protecting data at rest and in transit are recognised and deployed ad-hoc by multiple stakeholders and within various sectors.
					State of the art tools, such as SSL or TLS, are deployed ad-hoc by web service providers to secure all communications between servers and web browsers.
561	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cybersecurity Technologies	Few or no cybersecurity technologies are produced domestically; but international offerings may be available.	The domestic market may provide non-specialised cybersecurity products, but these are not marketdriven.
					Cybersecurity is considered in software and infrastructure development.
562	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cyber Insurance	The need for a cyber insurance market may have been identified, but no products and services are available.	The need for a market in cyber insurance has been identified through the assessment of financial risks for public and private sectors, and development of products is now being discussed.
571	Standards, Organisations, and Technologies	Responsible Disclosure	Responsible Disclosure	The need for a responsible disclosure policy in public and private sector organisations is not yet acknowledged.	Technical details of vulnerabilities are shared informally with other stakeholders who can distribute the information more broadly.
					Software and service providers are able to address bug and vulnerability reports.

Established	Strategic	Dynamic
Cryptographic techniques are available for all sectors and users for protection of data at rest or in transit.	The public and private sectors critically assess the deployment of cryptographic controls, according to their objectives and priorities.	The relevance of cryptographic controls deployed for securing data at rest and data in transit is continuously assessed through risk assessments.
There is a broad understanding of secure communication services, such as encrypted/signed email.	The public and private sectors have developed encryption and cryptographic control policies based on the previous assessment, and regularly review the policies for effectiveness.	The public and private sector adapt encryption and cryptographic control policies based on the evolution of technological advancement and changing threat environment.
The cryptographic controls deployed meet international standards and guidelines accordingly for each sector and are kept up-to-date.		
State of the art tools, such as SSL or TLS, are deployed routinely by web service providers to secure all communications between servers and web browsers.		
Cybersecurity products are now being produced by domestic providers in accordance with market needs.	Cybersecurity technology development abides by secure coding guidelines, good practices and adhere to internationally accepted standards.	Security functions in software and computer system configurations are automated in the development and deployment of technologies.
National dependence on foreign cybersecurity technologies is increasingly mitigated through enhanced domestic capacity.	Risk assessments and market incentives inform the prioritisation of product development to mitigate identified risks.	Domestic cybersecurity products are exported to other nations and are considered superior products.
A market for cyber insurance is established and encourages information sharing among participants of the market.	Cyber insurance specifies a variety of coverages to mitigate consequential losses.	The cyber insurance market is innovative and adapts to emerging risks, standards and practices, while addressing the full scope of cyber harm.
First-party insurance typically covers damage to digital assets, business interruptions and, potentially, reputational harm.	These coverages are selected based on strategic planning needs and identified risk.	Insurance premiums are offered for consistent cybersecure behaviour.
Third-party insurance covers liability and the costs of forensic investigations, customer notification, credit monitoring, public relations, legal defence, compensation and regulatory fines.	Products suitable for SMEs are also on offer.	
A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report.	Responsible disclosure processes for all involved stakeholders (product vendors, customers, security vendors and public) are set.	Responsible disclosure policies are continuously reviewed and updated based on the needs of all affected stakeholders.
Organisations have established processes to receive and disseminate vulnerability information.	An analysis of the technical details of vulnerabilities is published and advisory information is disseminated according to individual roles and responsibilities.	Responsible disclosure frameworks are shared internationally, so that best practice in this area can be created.
Software and service providers commit to refrain from legal action against a party disclosing information responsibly.	The large majority of products and services are updated within predetermined deadlines.	All affected products and services are routinely updated within deadline.
		Processes are in place to review and reduce deadlines.

Appendix B ANC3T

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	111L1-1	Outline of strategy	An outline/draft national cybersecurity strategy has been articulated.	111L2-1	Strategy established
				111L1-2	Development process of strategy	Processes for strategy development have been initiated.	111L2-2	Stakeholders' consultation in strategy
				111L1-3	Stakeholders involved in strategy development	Consultation processes have been agreed for key stakeholder groups, including international partners.	111L2-3	Implementation of strategy
112	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Organisation	112L1-1	Cybersecurity programme under development	A coordinated cybersecurity programme is being developed through a multistakeholder consultative process.	112L2-1	Cybersecurity programme agreed
							112L2-2	Coordinating body of cybersecurity programme
							112L2-3	Goals & measurement of cybersecurity programme
							112L2-4	Discrete budget for cybersecurity
113	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Content	113L1-1	Risk priorities of cybersecurity defined in strategy	Content includes links established between cybersecurity, national risk priorities and business development,	113L2-1	National objectives of cybersecurity defined in strategy
							113L2-2	Minimum coverage of strategy contents
121	Cybersecurity Policy and Strategy	Incident Response	Identification of Incidents	121L1-1	Recording incidents	Certain cybersecurity incidents have been categorised and recorded as national-level threats.	121L2-1	Central registry of incidents

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A national cybersecurity strategy has been published.	111L3-1	Reviewing process of strategy	Strategy review and renewal processes are confirmed.	111L4-1	Continual revision of strategy	Continual revision and refinement of cybersecurity strategy is conducted proactively to adapt to changing socio-political, threat and technology environments.
Multi-stakeholder consultation processes have been followed and observations fed back to the identified strategy 'owners'.	111L3-2	Cyber exercises considered in strategy	Regular scenario and realtime cyber exercises that provide a concurrent picture of national cyber resilience are considered a strategic priority.	111L4-2	Contributing to international debate of strategy	The country is a leader within the international community and the debate shaping the development of global cybersecurity strategy.
National cybersecurity strategy is promoted and implemented by multiple stakeholders across government and other sectors.	111L3-3	Measurement of cybersecurity defined in strategy	Relevant metrics, measurement, and monitoring processes, data, and historic trends are evaluated and inform decision-making.			
	111L3-4	Capacity building & investment considered in strategy	Cybersecurity strategic plans, aligned with national strategic priorities, drive capacity building and investments in security.			
The single agreed cybersecurity programme	112L3-1	PDCA processes of cybersecurity programme	Evidence exists of iterative application of metrics and resulting refinements to operations and strategy across government, including resource allocation considerations.	112L4-1	Reassignment & reallocation of resources for cybersecurity programme	A singular national cybersecurity posture exists with the ability to reassign tasks and budgets dynamically according to changing risk assessments.
has a designated coordinating body with a mandate to consult across public and private sectors, and civil society.	112L3-2	Consolidated budget for cybersecurity	A consolidated cybersecurity budget has been administered in order to allocate resources.	112L4-2	Dissemination & feedbacks about cybersecurity programme	A designated national body disseminates and receives feedback on the strategy from wider society to continuously enhance the national cybersecurity posture.
The programme is defined according to goals and objectives, using metrics to measure progress.						
Discrete budget for cybersecurity exists,						
The content of the national cybersecurity strategy is linked explicitly and directly to national risks, priorities and objectives, as well as business development.	113L3-1	Measurement of cybersecurity defined in strategy	Metrics and measurements are utilised to update national cybersecurity strategy content to help leaders evaluate the success of the various cybersecurity objectives and guide resource investment.	113L4-1	Continual revision of strategy	New content is periodically incorporated in the strategy in response to evolving threat landscapes.
Content at a minimum should seek to raise public awareness, mitigate cybercrime, establish incident response capability and protect critical infrastructure from external and internal threats.	113L3-2	Protection of critical infrastructures defined in strategy	Content now also seeks to protect critical infrastructure internal threats.	113L4-2	Contributing to international cooperation	Content of the national cybersecurity strategy leads, promotes and encourages national and international cooperation to ensure a secure, resilient and trusted cyberspace.
A central registry of national-level cybersecurity incidents is operational.	121L3-1	Regular revision of incident registry	Regular, systematic updates to the national-level incident registry are made.	121L4-1	Adapted analysis of incidents	Focus on incident identification and analysis is adapted in response to environmental changes.
	121L3-2	Incident analysis	Resources are allocated for analysing incidents in order to prioritise which incidents are most urgent.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
122	Cybersecurity Policy and Strategy	Incident Response	Organisation	122L1-1	Key incident response organisations in private sector identified	Private sector organisations key to national cybersecurity have been identified,	122L2-1	National CSIRT
				122L1-2	N/A	but no formal coordination and information sharing mechanisms exist between public and private sectors.	122L2-2	Roles & responsibilities of national CSIRT
				122L1-3	Ad-hoc responses	Dispersed public and private sector bodies detect and respond to incidents as they occur		
123	Cybersecurity Policy and Strategy	Incident Response	Coordination	123L1-1	Leading incident response organisation designated	Leads for incident response have been designated at the operational level,	123L2-1	Coordination established
							123L2-2	Communication lines for crisis
							123L2-3	International cooperation in incident response
124	Cybersecurity Policy and Strategy	Incident Response	Mode of Operation	124L1-1	Key incident response processes	Key incident response processes have been identified,	124L2-1	Incident response processes & tools established
				124L1-2	CSIRT member training	Members of CSIRTs receive training in an ad-hoc manner.	124L2-2	Regular training for CSIRT members
							124L2-3	Limited response to national level incidents
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	131L1-1	List of CI assets	A list of general CI assets has been created.	131L2-1	Audit of CI assets
							131L2-2	CI assets audit list

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A funded national body for incident response has been established (such as CSIRTs or CERTs),	122L3-1	Formal roles & responsibilities allocated	Distinct and formal security roles and responsibilities are allocated across government, critical infrastructure, enterprise, and individual systems.	122L4-1	Sustainability of incident response capability	National incident response capability is fully financially sustainable, from a single or multiple sources.
with specified roles and responsibilities.	122L3-2	Adequate resources for incident response	Human and financial resources allocated to incident response are adequate to the cybersecurity threat environment and enhance effectiveness of the organisation.	122L4-2	Early warning capability	An early warning capacity is incorporated into the mission of the incident response organisation,
				122L4-3	Capability to manage threat landscape	which seeks to shape and manage the threat landscape before responding to specific incidents.
Routine and coordinated national incident response is established and published between public and private sectors,	123L3-1	Subnational / sectorial incident response organisations	The national incident response organisation coordinates and collaborates with subnational/ sectorial incident response organisations.	123L4-1	Coordinating all levels / sectors	Multi-level and inclusive national and international coordination between all levels and sectors is internalised as vital for continuous and effective incident response.
with lines of communication prepared for times of crisis.	123L3-2	International coordination	Technical capabilities now go beyond coordinating response and include strategically focusing resources in coordinating international incident and threat intelligence analysis/support.	123L4-2	Regional coordination	Regional coordination exists to resolve incidents as they occur.
International cooperation for incident response between organisations exists to resolve incidents as they occur.	123L3-3	Information sharing across sectors	A platform for the reporting and sharing of incidents across sectors is promoted.			
Key incident response processes and tools are defined, documented and functional.	124L3-1	Training & accreditation for CSIRT members established	Incident response teams have established a training policy for their members; members are being trained in specialised subjects and accredited by internationally recognised bodies on a regular basis.	124L4-1	Scenario testing of incident response processes	The results of testing key processes through case scenarios are being analysed and are incorporated into the updating of processes.
Members of CSIRTs receive training regularly in order to understand key concepts of cybersecurity incident response.	124L3-2	Sophisticated incident analysis	Team members are able to carry out a sophisticated incident analysis investigation quickly and efficiently.	124L4-2	Evaluating effectiveness of CSIRT members training	The benefits of training and accreditation are being evaluated and inform the future training planning.
National-level incident response is limited in scope and still reactive.	124L3-3	Regular review of incident response processes	Key processes (detection, resolution, prevention, etc.) are being monitored and reviewed in regular basis, and tested with different case scenarios.	124L4-3	Tools against zero-day vulnerabilities	Tools for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities are embedded in incident response organisation(s).
	124L3-4	Forensics	Forensics services are offered.	124L4-4	Regional coordination	Mechanisms for regional cooperation in incident response have been established.
	124L3-5	International coordination	National incident response teams coordinate with international counterparts.			
A detailed audit of CI assets as it relates to cybersecurity is performed on a regular basis.	131L3-1	Priority of CI risks	CI risks and assets have been prioritised according to vulnerability and impact, which guides strategic investment.	131L4-1	Regular review of CI risk priorities	Priority listing of CI assets is regularly re-appraised to capture changes in the threat environment.
CI asset audit lists are disseminated to relevant stakeholders.	131L3-2	Vulnerability & asset management of CI assets	Vulnerability/asset management processes are in place so that incremental security improvements can be made.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	132L1-1	Informal information sharing between CI & government	There is informal and ad-hoc threat and vulnerability disclosure among CI owners as well as between CI and the government,	132L2-1	Information sharing established between CI & government
							132L2-2	Formal & consistent information sharing between CI & government
							132L2-3	Point of contact
							132L2-4	Government engagement in CI protection
133	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Risk Management and Response	133L1-1	Access control implemented in CI	Physical and virtual access control is implemented.	133L2-1	Standards & best practices in CI
				133L1-2	Basic capacity against cyber threat in CI	CI has basic capacity to detect, identify, respond to and recover from cyber threats,	133L2-2	Risk management processes in CI
				133L1-3	Data security policy in CI	Protection of CI assets includes basic level cybersecurity awareness and data security policies,	133L2-3	National CI incident response plan

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A mechanism is established for regular vulnerability disclosure with defined scope for reporting incidents (either mandatory or voluntary) between CI asset owners and the government.	132L3-1	Centralised management of CI protection	There is a clear understanding of which threats to CI are managed centrally, and which are managed locally.	132L4-1	Ability to adjust of CI protection	Owners of critical infrastructure and assets are able to rapidly respond to the changing threat landscape.
Formal internal and external CI communication strategies have been defined and are consistent across sectors,	132L3-2	Public awareness campaign of CI protection	A public awareness campaign to facilitate the CI communication strategy is established with a point of contact for this information.	132L4-2	Trust between CI & government	Trust has been established between the government and CIs with respect to cybersecurity and exchange of threat information, which is fed into the strategic decision-making process.
with clear points of contact.	132L3-3	Supply chain management of CI	Cybersecurity requirements and vulnerabilities in CI supply chains are clearly identified, mapped and managed.			
Strategic engagement between government and CI is agreed and promoted.						
Best practices in security measures, guidelines, and standards for CI cybersecurity have been established and adopted.	133L3-1	Cybersecurity oriented risk management in CI	Cybersecurity is firmly embedded into general risk management practice.	133L4-1	Regular audit of CI	Audit practices to assess network and system dependencies and vulnerabilities (i.e. unmitigated dependencies) are implemented on a regular basis and inform continuous reassessment of CI risk portfolio, technologies, policies and processes.
Cybersecurity risk management processes have been established, supported by adequate technical security solutions, communication links, and harm mitigation measures.	133L3-2	Regular review of impact analysis of CI	Assessment of the breadth and severity of harm incurred by CI assets is regularly conducted	133L4-2	Indirect costs inclusive in impact analysis of CI incidents	The impact of cybersecurity risk on the business operations of CI, including direct and opportunity costs, impact on revenue, and hindrance to innovation, are understood and incorporated into future planning and executive decision making.
CI risk management procedures are used to create a national response plan including the participation of all vital entities.	133L3-3	Regular review of CI incident response plans	and response planning is tailored to that assessment to ensure business continuity.			
	133L3-4	Regular review of resource allocation for CI protection	Resources are allocated in proportion to the assessed impact of an incident to ensure rapid and effective incident response.			
	133L3-5	Insider threat detection in CI	Insider threat detection is accounted for.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
141	Cybersecurity Policy and Strategy	Crisis Management	Crisis Management	141L1-1	Assessment of exercise of national incident	A preliminary cybersecurity needs assessment of measures and techniques that require testing has been undertaken,	141L2-1	National incident exercise done
				141L1-2	Exercise planning organisation designated for national incident	An exercise planning authority has been designated, and has outlined the steps to be taken in order to conduct the cybersecurity exercise.	141L2-2	Appropriate resources for national incident exercise
				141L1-3	Stakeholders' participation in national incident exercise	Key stakeholders and other subject matter experts, such as think tanks, academics, civil leaders and consultants are included in the planning process.	141L2-3	Roles in national incident exercise defined
							141L2-4	Incentives to participate in national incident exercise
							141L2-5	Trained monitors of national incident exercise
							141L2-6	Evaluation of national incident exercise
151	Cybersecurity Policy and Strategy	Cyber Defence	Strategy	151L1-1	National-level threats identified	Specific threats to national security in cyberspace have been identified, such as external threat actors (both state and non-state), insider threats, supply chain vulnerabilities, and threats to military operational capacity,	151L2-1	Cyber defence strategy exists
152	Cybersecurity Policy and Strategy	Cyber Defence	Organisation	152L1-1	Dispersed cyber operations	Cyber operations units are incorporated into the different branches of the armed forces, but no central command and control structure exists.	152L2-1	Defined responsibility of cyber defence organisation

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A cybersecurity exercise, with limited size and geographic scope has been conducted involving all relevant stakeholders in all sectors.	141L3-1	High-level scenario of national incident exercise	A realistic high-level scenario informs a plan to test information flows, decision-making and resource investment at the national level.	141L4-1	Peer observance of national incident exercise	The exercise involves neutral peer stakeholders to observe,
Appropriate resources have been allocated to the exercises.	141L3-2	Trust between participants of national incident exercise	Trust is developed well in advance via the recruitment and pre-exercise briefing process and through guaranteed confidentiality control.	141L4-2	National incident exercise contributing to international challenges	and, where appropriate, contribute, and addresses international challenges to produce scalable results for international policy- and decision-making.
Planning process includes the engagement of participants, an outline of their role in the exercise,	141L3-3	SMART objectives & KPI of national incident exercise	Specific, Measurable, Attainable, Relevant, and Time-Bound (SMART) objectives and performance key indicators (PKI) inform decisions in crisis management,	141L4-3	Internationally shared result of national incident exercise	An evaluation of the crisis management exercise is provided for the international community, so that lessons learnt can contribute toward a global understanding of crisis management.
and the articulation of benefits and incentives for participation.	141L3-4	Evaluation of national incident exercise informing investment	and evaluation results inform future investment in national cybersecurity capacity.	141L4-4	National crisis management established	Crisis management is embedded in risk analysis, review and management.
Trained internal or external monitors facilitate the exercise.	141L3-5	National crisis management aligned with international best practices	Findings are evaluated against international crisis management good practice.			
The exercise is evaluated and commentary is provided by participants and stakeholders.	141L3-6	Tailored reports of national incident exercise	Tailored, sector-specific reports are prepared for each stakeholder, while ensuring sensitive information is secured.			
National cyber Defence policy or strategy exists and outlines the country's position in its response to different types and levels of cyber-attacks (for example, cyber-enabled conflict producing a kinetic effect and offensive cyber-attacks aimed to disrupt infrastructure).	151L3-1	Dedicated resources for cyber defence	Resources dedicated toward Cyber Defence are allocated based on national strategic objectives.	151L4-1	Rules of engagement in cyberspace	The policy or strategy drives the international discussion on rules of engagement in cyberspace.
	151L3-2	Capturing landscape of national-level threat	The evolving threat landscape in cybersecurity is captured through repeated review	151L4-2	Military doctrine in cyberspace	Rules of engagement are clearly defined and the military doctrine that applies to cyberspace is fully developed and takes note of significant shifts in the cybersecurity environment.
	151L3-3	Cyber defence strategy meets objectives	in order to ensure that cyber Defence ways and means continue to meet national security objectives.			
There is a defined organisation within the Defence apparatus responsible for conflict using cyber means.	152L3-1	Advanced capabilities & situational awareness	Highly specialised expertise with advanced capabilities and full situational awareness are integrated into the national defence posture.	152L4-1	Cross-border response ability	The Defence apparatus contributes to the debate in developing a common international understanding of the point at which a cyber-attack might trigger a cross-domain response.
Enhancement	152L3-2	***Counter-cyber intelligence activities***	***There exist activities for detecting and/or defending against intelligence assessment through cyber-space from other nations.***	152L4-2	***Established counter-cyber intelligence capability***	***Counter-cyber intelligence activities are centrarised and have capability to defend effectively.***

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
153	Cybersecurity Policy and Strategy	Cyber Defence	Coordination	153L1-1	Cyber defence capability requirements agreed	Cyber Defence capability requirements are agreed between the public and private sector in order to minimise the threat to national and international security.	153L2-1	Coordination between CI & defence
							153L2-2	Intelligence sharing between CI & defence
161	Cybersecurity Policy and Strategy	Communications Redundancy	Communications Redundancy	161L1-1	Gaps in emergency communication identified	Stakeholders convene to identify gaps and overlaps in emergency response asset communications and authority links.	161L2-1	Emergency response assets hardwired
				161L1-2	Emergency procedures established	Emergency response assets, priorities and standard operating procedures are mapped and identified in the event of a communications disruption along any node in the emergency response network.	161L2-2	Communication between emergency response functions distributed
							161L2-3	Testing, training, drills of emergency response
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	211L1-1	Leading agencies only have mind-set	Leading agencies have begun to place priority on cybersecurity, by identifying risks and threats.	211L2-1	Most officials have mind-set
212	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	212L1-1	Leading firms only have mind-set	Leading firms have begun to place priority on a cybersecurity mind-set by identifying high-risk practices.	212L2-1	Most private sector actors have mind-set
				212L1-2	Materials for best practices available	Programmes and materials have been made available to train and improve cybersecurity practices.		
213	Cyber Culture and Society	Cybersecurity Mind-set	Users	213L1-1	Limited users only have mind-set	A limited proportion of Internet users have begun to place priority on cybersecurity, by identifying risks and threats.	213L2-1	Growing number of users have mind-set

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
The entity in charge of cyber Defence coordinates integration regarding cyber events between government, military and critical infrastructure and identifies clear roles and responsibilities.	153L3-1	Analytical capability in cyber defence	Analytical capacity exists to support the coordination of resource allocation for national cyber Defence; possibly including a cyberdefence research centre.	153L4-1	Leading international debate about cyber defence	The country is leading the international debate on cyber Defence
Defence organisations and critical infrastructure providers have established a mechanism to report threat intelligence.	153L3-2	Strengths & weaknesses of cyber defence understood	The understanding of strengths and weaknesses within the coordination mechanism then feeds into the re-evaluation of the national security posture of the nation.	153L4-2	Intelligence shared with allies	and systematically shares intelligence with allies.
Emergency response assets are hardwired into a national emergency communication network.	161L3-1	Redundant communications for key stakeholders	Outreach and education of redundant communications protocols is undertaken for key stakeholders and is tailored to their unique roles and responsibilities.	161L4-1	Optimised for extended outages	Optimised efficiency is in place to mediate extended outages of systems.
Communication is distributed across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.	161L3-2	Interoperability & functionality under compromised situation	Emergency response assets practice interoperability and function effectively under compromised communications scenarios.	161L4-2	Assisting neighbours	National-level assets can act to assist neighbours in the event of an international level crisis or incident.
Appropriate resources are allocated to hardware integration, technology stress testing, personnel training and crisis simulations drills.	161L3-3	Evaluation of national incident exercise informing investment	The results of these scenarios then inform strategic investment in future emergency response assets.			
	161L3-4	Contribution to international communications' redundancy	Stakeholders contribute to international efforts on redundancy communication planning.			
Most government officials at all levels are aware of cybersecurity good practices.	211L3-1	Mind-set spread in public sector	Agencies across all levels of government have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit.	211L4-1	Mind-set commonplace in public sector	The cybersecurity mind-set serves as a foundation for government official’s operational practices and is evidenced as global good practice.
	211L3-2	Mind-set based strategy in public sector	Cybersecurity mind-set informs strategic planning.			
Most private sector actors at all levels are aware of cybersecurity good practices.	212L3-1	Mind-set spread in private sector	Most private sector actors, including SMEs, have routinized a cybersecurity mind-set, employing good (proactive) practices as a matter of habit.	212L4-1	Mind-set commonplace in private sector	The cybersecurity mind-set serves as a foundation for private sector operational practices, informs all IT related initiatives and is evidenced as global good practice.
	212L3-2	Mind-set based strategy in private sector	Cybersecurity mind-set, informs strategic planning.			
A growing number of users feel it is a priority for them to employ good cybersecurity practices and make conscious efforts to securely use online systems.	213L3-1	Most users have mind-set	Most users have routinized a cybersecurity mind-set, employing secure practices as a matter of habit.	213L4-1	Users' mind-set reducing threat	Cybersecurity mind-set of users is related to a reduction of the overall threat landscape of the country.

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
221	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	221L1-1	A few users can use internet securely	A very limited proportion of Internet users critically assess what they see or receive online and believe that they have the ability to use the Internet and protect themselves online.	221L2-1	Growing number of users can use internet securely
				221L1-2	Promotion of online trust exists	Operators of Internet infrastructure develop measures to promote trust in online services but have not established them.	221L2-2	Promotion of online trust established
							221L2-3	User assistance available
222	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-government Services	222L1-1	Government's recognition of needs for security in e-gov	Government continues to increase e-service provision, but also recognises the need for the application of security measures to establish trust in these services.	222L2-1	E-gov established
				222L1-2	Stakeholders' recognition of needs for security in e-gov	The need for security in e-government services is recognised by stakeholders and users.	222L2-2	Risk reduction in e-gov
				222L1-3	A few users can use e-gov securely	A limited proportion of users trust in the secure use of e-government services.	222L2-3	Promotion of e-gov
				222L1-4	Security measures in e-gov	Some e-government services are informing users of the utility of deployed security solutions.	222L2-4	Growing number of users can use e-gov securely
							222L2-5	Incident disclosure in e-gov

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A growing proportion of Internet users critically assess what they see or receive online, based on identifying possible risks.	221L3-1	Most users can use internet securely	Most Internet users critically assess what they see or receive online, based on identifying possible risks.	221L4-1	Users can evaluate risk & adjust behaviour	Individuals assess the risk in using online services, including changes in the technical and cybersecurity environment and continuously adjust their behaviour based on this assessment.
Internet infrastructure operators have established programmes to promote trust in online services.	221L3-2	Users' ability to control providing personal information	Most Internet users feel confident while using the Internet, have the ability to recognise non-legitimate websites (including mimicry attempts), and have a sense of control over providing personal data online.	221L4-2	Promotion of online trust revised	Internet infrastructure operators assess trust promotion services and integrate findings into programme and policy revision.
User-consent policies are in place designed to notify practices on the collection, use or disclosure of sensitive personal information.	221L3-3	Promotion of online trust evaluated	Programmes to promote trust in the use of online services are assessed based on measures of effectiveness which informs resource allocation.			
E-government services have been fully developed.	222L3-1	Disclosures of activities of government agencies	Public authorities are routinely publishing certain information about their activities.	222L4-1	Promotion of e-gov revised	E-government services and promotion thereof are continuously improved and expanded to enhance transparent/open and secure systems and user trust.
High-level risks affecting egovernment services are prioritised in order to reduce occurrences.	222L3-2	Privacy-by-default in e-gov	Privacy-by-default is promoted as a tool for transparency in e-government services.	222L4-2	Data protection measures of e-gov	Impact assessments on data protection in e-government services are consistently taking place and feed back into strategic planning.
The public sector promotes use of e-government services and trust in these services through a coordinated programme, including the compliance to web standards that protect the anonymity of users.	222L3-3	Most users can use e-gov securely	The majority of users trust in the secure use of e-government services and make use of them.			
A growing proportion of users trust in the secure use of e-government services.	222L3-4	User feedbacks for e-gov	Processes are employed for gathering user feedback in order to ensure efficient management of online content.			
Possible breaches in egovernment services are being identified, acknowledged, and disclosed in an ad-hoc manner.						

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
223	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-commerce Services	223L1-1	Limited e-commerce provided	E-commerce services are being provided to a limited extent.	223L2-1	E-commerce established
				223L1-2	Private sectors' recognition of need for security in e-commerce	The private sector recognises the need for the application of security measures to establish trust in e-commerce services.	223L2-2	Secure payment
				223L1-3	A few users can use e-commerce securely	A limited proportion of users trust in the secure use of e-commerce services.	223L2-3	Growing number of users can use e-commerce securely
				223L1-4	Security measures in e-commerce	Some e-commerce services are informing users of the utility of deployed security solutions.	223L2-4	Promotion of trust of e-commerce
							223L2-5	Terms & conditions of e-commerce accessible
231	Cyber Culture and Society	User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	231L1-1	Users have only general knowledge about personal information protection	Users and stakeholders within the public and private sectors may have general knowledge about how personal information is handled online; and may employ good (proactive) cybersecurity practices to protect their personal information online.	231L2-1	Growing number of users can secure personal information online
				231L1-2	Discussions on protecting personal information	Discussions have begun regarding the protection of personal information and about the balance between security and privacy,	231L2-2	Discussions on balance between security & privacy
241	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	241L1-1	Reporting channels of incidents	The public and/or private sectors are providing some channels for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents,	241L2-1	Incident reporting mechanisms established
							241L2-2	Promotion of incident reporting channels

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
E-commerce services are fully established by multiple stakeholders in a secure environment.	223L3-1	Resource allocation for e-commerce	E-commerce service providers recognise the need for building trust in order to ensure business continuity, and resources are allocated accordingly.	223L4-1	Continuous improvement of e-commerce	E-commerce services are continuously improved in order to promote transparent, trustworthy and secure systems.
Security solutions are updated and reliable payment systems have been made available.	223L3-2	Most users can use e-commerce securely	The majority of users trust in the secure use of e-commerce services and make use of them.	223L4-2	Clear terms & conditions of e-commerce	Terms and conditions provided by e-commerce services are clear and easily comprehensible to all users.
A growing proportion of users trust in the secure use of e-commerce services.	223L3-3	Investment for e-commerce	Stakeholders invest in establishing enhanced service functionality of e-commerce services, protection of personal information and the provision of feedback mechanisms for users.	223L4-3	User feedbacks for e-commerce	User feedback mechanisms are integrated into e-commerce services in order to enhance trust between users and providers.
The private sector promotes use of e-commerce services and trust in these services.						
Terms and conditions of use of e-commerce services are easily accessible.						
A growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others.	231L3-1	Measures to protect personal information online	All stakeholders have the information, confidence and the ability to take measures to protect their personal information online and to maintain control of the distribution of this information.	231L4-1	Users can adapt to changing environments	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment.
There is constant public debate regarding the protection of personal information and about the balance between security and privacy, which informs privacy policies within public and private sectors.	231L3-2	Privacy rights	Users and stakeholders within the public and private sectors widely recognise the importance of protection of personal information online, and are sensitised to their privacy rights.	231L4-2	Wide recognition about personal information protection	There is a wide recognition of the need to ensure security and protection of personal information.
	231L3-3	Security & privacy balanced	Mechanisms are in place in private and public sectors to ensure that privacy and security are not competing.	231L4-3	Security & privacy balanced in changing environment	Policies are in place in private and public sectors to ensure that privacy and security are not competing in a changing environment and are informed by user feedback and public debate.
	231L3-4	Privacy-by-default	Privacy by default as a tool for transparency is promoted.	231L4-4	Regular assessment of privacy protection	Assessments of personal information protection in eservices are regularly conducted and feed back into policy revision.
Reporting mechanisms have been established and are regularly used.	241L3-1	Coordination of incident reporting channels	Coordinated reporting mechanisms are widely used.	241L4-1	Regular enhancement of incident reporting	All relevant stakeholders actively collaborate and share good practice to enhance existing reporting mechanisms and there is a clear distribution of roles and responsibilities, including regarding the response to reported incidents.
Programmes to promote the use of these mechanisms have been established by public and private sectors.	241L3-2	Promotion of incident reporting channels prioritised	Programmes to promote the use of these mechanisms are prioritised by public and private sectors and are considered as an investment in loss prevention and risk control.	241L4-2	Coordination of response to reported incidents	Mechanisms have been developed to coordinate response to reported incidents between law enforcement and the national incident response capability.
	241L3-3	Metrics of incident reporting	Effectiveness metrics of reporting mechanisms are applied and findings inform the revision and promotion of the mechanisms.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
251	Cyber Culture and Society	Media and Social Media	Media and Social Media	251L1-1	Media coverage of cybersecurity	There is ad-hoc media coverage of cybersecurity, with limited information provided and reporting on specific issues that individuals face online, such as online child protection or cyber-bullying.	251L2-1	Cybersecurity as common subject in media
				251L1-2	Discussion on social media security	There is limited discussion on social media about cybersecurity.	251L2-2	Wide range of issues of cybersecurity in media
							251L2-3	Broad discussion on social media security
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	311L1-1	Awareness raising programmes	Awareness raising programmes, courses, seminars and online resources are available for target demographics from public, private, academic, and/or civil society sources,	311L2-1	National programme of awareness raising
				311L1-2	Awareness raising programmes affected by international initiatives	Awareness raising programmes may be informed by international initiatives but are not linked to national strategy.	311L2-2	Consultation with stakeholders in national programme of awareness raising
							311L2-3	Cybersecurity information portal

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Cybersecurity is a common subject across mainstream media, and information	251L3-1	Media coverage of information about cybersecurity measures	Media coverage extends beyond threat reporting and can inform the public of proactive and actionable cybersecurity measures, as well economic and social impacts.	251L4-1	Discussion changing policy & society	The broad discussion of personal experiences and personal attitudes of individuals across mainstream and social media inform policy making and facilitate societal change.
and reports on a wide range of issues, including security breaches and cybercrime are widely disseminated.	251L3-2	Frequent discussion on social media security	There is frequent discussion on social media about cybersecurity and individuals regularly exchange experiences online using social media.			
There is broad discussion on social media about cybersecurity.						
A national programme for cybersecurity awareness raising, led by a designated organisation (from any sector) is established, which addresses a wide range of demographics and issues,	311L3-1	Sector specific programmes of awareness raising	The national awareness raising programme is coordinated and integrated with sector-specific, tailored awareness raising programmes, such as those focusing on government, industry, academia, civil society, and/or children.	311L4-1	Awareness raising programmes adapted according to effectiveness	Awareness raising programmes are adapted in response to performance evidenced by monitoring which results in the redistribution of resources and future investments.
Consultation with stakeholders from various sectors informs the creation and utilisation of programmes and materials.	311L3-2	Metrics for effectiveness of awareness raising programmes	Metrics for effectiveness are established and evidence of application and lessons learnt are fed into future programmes.	311L4-2	Revision of national awareness raising programme	Metrics contribute toward national cybersecurity strategy revision processes.
A single online portal linking to appropriate cybersecurity information exists and is disseminated via that programme.	311L3-3	Evolution of awareness raising programmes	The evolution of the programme is supported by the adaptation of existing materials and resources, involving clear methods for obtaining a measure of suitability and quality.	311L4-3	Entire society involved in awareness raising	Awareness programme planning gives explicit consideration to national demand from the stakeholder communication (in the widest sense), so that campaigns continue to impact the entire society.
	311L3-4	Contribution to international awareness raising	Programmes contribute toward expanding and enhancing international awareness raising good practice and capacitybuilding efforts.	311L4-4	Overall threat reduced by awareness raising	The national awareness raising programme has a measurable impact on reduction of the overall threat landscape.

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
312	Cybersecurity Education, Training and Skills	Awareness Raising	Executive Awareness Raising	312L1-1	Executives' awareness about general cybersecurity issues	Executives are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisation.	312L2-1	Executives' basic understandings of cybersecurity
				312L1-2	Executives of particular sectors have awareness	Executives of particular sectors, such as finance and telecommunications, have been made aware of cybersecurity risk in general and how the organisation deals with cybersecurity issues, but not of strategic implications.	312L2-2	Limited executives' understandings of cybersecurity's affect
							312L2-3	Raising programmes for awareness of crisis management
321	Cybersecurity Education, Training and Skills	Framework for Education	Provision	321L1-1	Qualification programme for cybersecurity educators	Qualification programmes for cybersecurity educators are being explored,	321L2-1	Qualification for cybersecurity educators established
				321L1-2	Professional cybersecurity educators	with a small cadre of existing professional educators.	321L2-2	University level courses for cybersecurity
				321L1-3	Educational courses for cybersecurity	Some educational courses exist in cybersecurity related fields, such as information security, network security and cryptography,	321L2-3	Degrees in cybersecurity
				321L1-4	Demand exists for cybersecurity education	A demand for cybersecurity education is evidenced through course enrolment and feedback.	321L2-4	Seminars for non-specialist
							321L2-5	Research & development in cybersecurity promoted

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Awareness raising of executives in the public, private, academic and civil society sectors address cybersecurity risks in general, some of the primary methods of attack, and how the organisation deals with cyber issues (usually abdicated to the CIO).	312L3-1	Executives' understandings of cybersecurity measures	Executive awareness raising efforts in nearly all sectors include the identification of strategic assets, specific measures in place to protect them, and the mechanism by which they are protected.	312L4-1	Cybersecurity as common agenda in board meetings	Cybersecurity risks are considered as an agenda item at every executive meeting, and funding and attention is reallocated to address those risks.
Select executive members are made aware of how cybersecurity risks affect the strategic decision making of the organisation, particularly those in the financial and telecommunications sectors.	312L3-2	Executives' ability to reallocate resources	Executives are able to alter strategic decision making, and allocate specific funding and people to the various elements of cyber risk, contingent on their company's prevailing situation.	312L4-2	Executives' attitude as international role model	Executives are regarded regionally and internationally as a source of good practice in responsible and accountable corporate cybersecurity governance.
Awareness raising efforts of cybersecurity crisis management at the executive level is still reactive in focus.	312L3-3	Executives' understanding of crisis management plans	Executives are made aware of what contingency plans are in place to address various cyber-based attacks and their aftermath.			
	312L3-4	Mandatory cybersecurity education for executives	Executive awareness courses in cybersecurity are mandatory for nearly all sectors.			
Qualifications for and supply of educators are readily available in cybersecurity.	321L3-1	Business experts' participation in cybersecurity education	Cybersecurity educators are not only drawn from the academic environment, but incentives are in place so that industry and/or government experts take these positions as well.	321L4-1	Internationally forerunning in cybersecurity education	National courses, degrees, and research are at the forefront of cybersecurity education internationally.
Specialised courses in cybersecurity are offered and accredited at the university level.	321L3-2	Mandatory cybersecutity courses for computer science degrees	Accredited cybersecurity courses are embedded in all computer science degrees.	321L4-2	Balance between core components & adaptive processes	Cybersecurity education programmes maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cybersecurity environment.
Degrees in cybersecurity related fields are offered by universities.	321L3-3	Cybersecurity specific degree	Degrees are offered in cybersecurity specifically, which encompasses courses and models in various other cybersecurity-related fields, including technical and nontechnical elements such as policy implications, and multi-disciplinary education.	321L4-3	Cybersecurity education adapting to changing needs	Prevailing cybersecurity requirements are considered in the redevelopment of all general curricula.
Universities and other bodies hold seminars/lectures on cybersecurity issues aimed at non-specialists.	321L3-4	Cybersecurity as focusing area	Cybersecurity educational offerings are weighted and focused based on an understanding of current risks and skills requirements.			
Research and development is a leading consideration in cybersecurity education.	321L3-5	Cybersecurity education from primary to post-graduate	Cybersecurity education is not limited to universities, but ranges from primary to post-graduate levels, including vocational education.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
322	Cybersecurity Education, Training and Skills	Framework for Education	Administration	322L1-1	Cybersecurity education needs recognised	The need for enhancing cybersecurity education in schools and universities has been identified by leading government, industry, and academic stakeholders.	322L2-1	Broad discussion for enhancing cybersecurity education
				322L1-2	Ad-hoc supply of resources for cybersecurity education	Schools, government, and industry collaborate in an ad-hoc manner to supply the resources necessary for providing cybersecurity education.	322L2-2	Budget for research & education for cybersecurity
							322L2-3	Attractiveness of cybersecurity career
331	Cybersecurity Education, Training and Skills	Framework for Professional Training	Provision	331L1-1	Cybersecurity training needs recognised	The need for training professionals in cybersecurity has been documented at the national level.	331L2-1	Structured cybersecurity training programmes
				331L1-2	Cybersecurity training for general IT staff	Training for general IT staff is provided on cybersecurity issues so that they can react to incidents as they occur, but no training for dedicated security professionals exists.	331L2-2	Security professional certification
				331L1-3	ICT certification with some cybersecurity issues	ICT professional certification is offered, with some security modules or components.	331L2-3	Cybersecurity training requirements listed
				331L1-4	Training courses for cybersecurity	Ad-hoc training courses, seminars and online resources are available for cybersecurity professionals through public or private sources, with limited evidence of take-up.	331L2-4	Cybersecurity training programmes for non-professionals
332	Cybersecurity Education, Training and Skills	Framework for Professional Training	Uptake	332L1-1	Metrics of uptake of cybersecurity trainings	Metrics evaluating take-up of ad-hoc training courses, seminars, online resources, and certification offerings exist, but are limited in scope.	332L2-1	Cybersecurity trained & certified employees
							332L2-2	Knowledge transfer in cybersecurity
							332L2-3	Job creation in cybersecurity

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Broad consultation across government, private sector, academia and civil society stakeholders informs cybersecurity education priorities and is reflected in national cybersecurity strategy.	322L3-1	Cybersecurity education demand/supply monitored	Metrics are developed to ensure that educational investments meet the needs of the cybersecurity environment across all sectors.	322L4-1	International CoE in cybersecurity	International cybersecurity centres of excellence are established through twinning programmes led by world class institutions.
National budget is dedicated to national cybersecurity research and laboratories at universities.	322L3-2	Adapted budget for cybersecurity education	Government budget and spending on cybersecurity education is managed based on the national demand.	322L4-2	Cooperation between all stakeholders in cybersecurity education	Routinized cooperation between all stakeholders in cybersecurity education can be evidenced.
Competitions and initiatives for students are promoted by government and/or industry in order to increase the attractiveness of cybersecurity careers.	322L3-3	International cooperation in cybersecurity education	Leading national cybersecurity academic institutions share their lessons learnt with other national and international counterparts.	322L4-3	Cybersecurity education aligned with practical problems	Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges, and provides a mechanism for enhancing curriculum based on the evolving landscape.
	322L3-4	CoE in cybersecurity	Government has established academic centres of excellence in cybersecurity.			
Structured cybersecurity training programmes exist to develop skills towards building a cadre of cybersecurity-specific professionals.	331L3-1	Cybersecurity training aligned with international best practices	A range of cybersecurity training courses is tailored toward meeting national strategic demand and aligns with international good practice.	331L4-1	Collaboration between public & private in cybersecurity training	The public and private sector collaborate to offer training, constantly adapting and seeking to build skillsets drawn from both sectors.
Security professional certification is offered across sectors within the country.	331L3-2	Cybersecurity training aligned with national strategy	The training programme outlines the priorities in the national cybersecurity strategy.	331L4-2	Coordination between cybersecurity training & education	Training offerings coordinate with education programmes so that the foundation established in schools can enable training programmes to build a highly skilled workforce.
The needs of society are well understood and a list of training requirements is documented.	331L3-3	Communication skills in cybersecurity training	Training programmes are offered to cybersecurity professionals that focus on the skills necessary to communicate technically complex challenges to nontechnical audiences, such as management and general employees.	331L4-3	Incentives for cybersecurity trained workforce	Programmes and incentive structures are in place to ensure the retention of trained workforce within the country.
Training programmes for non-cybersecurity professionals are recognised and initially offered.	331L3-4	Metrics of effectiveness of cybersecurity training	Metrics of effectiveness assess the modes and procedures of training.			
There is an established cadre of certified employees trained in cybersecurity issues, processes, planning and analytics.	332L3-1	Review of cybersecurity training programmes	The uptake of cybersecurity training is used to inform future training programmes.	332L4-1	Cybersecurity trained professionals internationally contributing	Cybersecurity professionals not only fulfil national requirements, but domestic professionals are consulted internationally to share lessons learnt and good practice.
Knowledge transfer from employees trained in cybersecurity to untrained employees is ad hoc.	332L3-2	Coordination of cybersecurity training across sectors	Coordination of training across all sectors ensures the national demand for professionals is met.			
Job creation initiatives for cybersecurity within organisations are established and encourage employers to train staff to become cybersecurity professionals.						

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	411L1-1	Discussion of establishing cybersecurity legal framework	Experienced stakeholders from all sectors may have been consulted to support the establishment of a legal and regulatory framework.	411L2-1	Cybersecurity legal framework established
				411L1-2	Priorities identified in cybersecurity legal framework	Key priorities for creating cybersecurity legal frameworks have been identified through multistakeholder consultation, potentially resulting in draft legislation,	411L2-2	Coverages of cybersecurity legal framework
412	Legal and Regulatory Frameworks	Legal Framework	Privacy, Freedom of Speech & Other Human Rights Online	412L1-1	Partial privacy protection legislation	Domestic legislation partially recognises privacy,	412L2-1	Online privacy protected
				412L1-2	Freedom of expression	freedom of information, freedom of assembly and association, and freedom of expression online.	412L2-2	Freedom of expression protected
				412L1-3	Discussion of establishing digital human rights legislation	Stakeholders from all key sectors have been consulted for the development of legislation addressing human rights online.	412L2-3	Privacy protected during investigation
							412L2-4	Stakeholders' participation to discuss digital human rights legislation
							412L2-5	Participation to international agreements
413	Legal and Regulatory Frameworks	Legal Framework	Data Protection Legislation	413L1-1	Partial data protection legislation	Data protection legislation is under development.	413L2-1	Data protection legislation established
				413L1-2	Stakeholders' participation in data protection legislation	Stakeholders from all key sectors have been consulted to support the development of legislation.	413L2-2	Personal data protected

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been adopted.	411L3-1	Regular review of cybersecurity legal framework	The country reviews existing legal and regulatory mechanisms for ICT security, identifies where gaps and overlaps exist, and amends laws accordingly or enacts new laws.	411L4-1	Balance between cybersecurity legal framework & best practices	Mechanisms are in place for continuously harmonising ICT legal frameworks with national cybersecurity related ICT policies, international law, standards and good practices.
Laws address the protection of critical information infrastructure, e-transactions, liability of Internet Service Providers and, potentially, cyber incident reporting obligations.				411L4-2	Participation to international cooperation agreements	Participation in the development of regional or international cybersecurity cooperation agreements and treaties is a priority.
				411L4-3	Exceeding minimum requirement of international cooperation agreement	Efforts are in place to exceed minimal baselines specified in these treaties where appropriate.
			Enhancement	411L4-4	***International and/or regional cooperation of establishing legislative framework***	***The nation cooperates internationally and/or regionally in supporting other nations in establishing legislative framework for ICT security.***
Domestic law recognises fundamental human rights on the Internet, including privacy online,	412L3-1	Cybersecurity legal framework aligned with international best practices	International and regional trends and good practices inform the assessment and amendment of domestic legal frameworks protecting human rights online and associated resource planning.	412L4-1	Amendment procedures for cybersecurity legal framework	In order to meet dynamic changes in the application of technology to human rights, procedures are in place to amend and update legal frameworks as needed.
freedom of speech, freedom of information, and freedom of assembly and association.	412L3-2	Exceeding minimum requirement of international agreement	Research is conducted and measures are in place to exceed minimal baselines specified in international agreements.	412L4-2	Internet access as human right	Access to the Internet is recognised and enshrined as a human right.
Domestic law specifies safeguards to protect the individual's right to privacy during the collection, use and disclosure of personal information in investigations involving electronic evidence.				412L4-3	Contributing to international digital human rights	The state is an active contributor in the global discourse on human rights on the Internet.
All relevant actors from private sector and civil society are involved in shaping laws and regulations on privacy, freedom of speech, and other human rights online.				412L4-4	Contributing to international privacy protection online	Domestic actors, policies and practices actively shape positive international discussions of privacy online.
The country has ratified or acceded to international agreements.						
Comprehensive data protection legislation has been adopted and enforced,	413L3-1	Timeframe of storing personal data during investigation	Legal mechanisms are in place that enable strategic decision making that determines the timeframe in which personal data is no longer required as evidence for investigation and must be deleted.	413L4-1	Amendment procedures for data protection legislation	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
which includes conditions for the collection of personal data and protection from misuse.	413L3-2	Data protection legislation aligned with international best practices	International and regional trends and good practices inform the assessment and amendment of data protection laws and associated resource planning.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
414	Legal and Regulatory Frameworks	Legal Framework	Child Protection Online	414L1-1	Partial online child protection legislation	Legislative provisions protecting children online are under development.	414L2-1	Online child protection legislation established
				414L1-2	Stakeholders' participation in online child protection legislation	Stakeholders from all key sectors have been consulted to support the development of legislation.	414L2-2	Legal minors protected
415	Legal and Regulatory Frameworks	Legal Framework	Consumer Protection Legislation	415L1-1	Partial consumer protection legislation	Legislation protecting consumers online is under development.	415L2-1	Consumer protection legislation established
				415L1-2	Stakeholders' participation in consumer protection legislation	Stakeholders from all key sectors have been consulted to support the development of legislation.	415L2-2	Responsible agency designated for consumer protection
416	Legal and Regulatory Frameworks	Legal Framework	Intellectual Property Legislation	416L1-1	Partial intellectual property legislation	Legislation on intellectual property online is under development,	416L2-1	Intellectual property legislation established
				416L1-2	Stakeholders' participation in intellectual property legislation	through consultation with key stakeholders.		
417	Legal and Regulatory Frameworks	Legal Framework	Substantive Cybercrime Legislation	417L1-1	Partial substantive cybercrime legislation	Partial legislation exists that addresses some aspects of cybercrime or cybercrime legal provisions are under development.	417L2-1	Substantive cybercrime legislation exists
							417L2-2	Participation to international agreements on cybercrime
418	Legal and Regulatory Frameworks	Legal Framework	Procedural Cybercrime Legislation	418L1-1	Partial procedural cybercrime legislation	Development of specific procedural cybercrime legislation or amendment of general procedural criminal law to adapt to cybercrime cases has begun.	418L2-1	Procedural cybercrime legislation exists
							418L2-2	Participation to international agreements on cybercrime

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Comprehensive legislation on the protection of children online has been adopted and enforced,	414L3-1	Online child protection legislation aligned with international best practices	The country continuously seeks to improve national child protection online legislation to comply with regional and international law and standards.	414L4-1	Amendment procedures for online child protection legislation	In order to meet dynamic changes in the technological environment, procedures are in place to amend and update legal frameworks as needed.
and ensures that data protection and privacy rules for legal minors apply to the online environment.						
Comprehensive legislation protecting consumers from business malpractice online has been adopted and is enforced.	415L3-1	Consumer protection legislation aligned with international best practices	The country continuously seeks to improve national consumer protection legislation to address national needs and comply with regional and international consumer protection standards.	415L4-1	Amendment procedures for consumer protection legislation	In order to meet dynamic changes in the application of technology to consumer protection, procedures are in place to amend and update legal frameworks as needed.
A lead agency responsible for the protection of consumers online has been designated.						
Comprehensive legislation addressing intellectual property of online products and services has been adopted and is enforced.	416L3-1	Intellectual property legislation aligned with international best practices	Legislation on intellectual property online is regularly reviewed and amended accordingly to reflect changes in national priorities and the international ICT landscape.	416L4-1	Balance between intellectual property & open access policy	Decisions to update legislation are based on the balance between intellectual property and open access policies, through multi-stakeholder discussion.
	416L3-2	Stakeholders' participation in amendment of intellectual property legislation	Legislative amendments are informed by multistakeholder consultations and public discourse.			
Substantive cybercrime legal provisions are contained in specific legislation or a general criminal law.	417L3-1	Exceeding minimum requirement in international agreements on cybercrime	Measures are in place to exceed minimal baselines specified in international treaties where appropriate,	417L4-1	Contributing to international cybercrime treaties	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties.
The country has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.	417L3-2	Amendment procedures for substantive cybercrime legislation	which includes procedures to amend substantive legal frameworks as needed.	417L4-2	Regular review of substantive cybercrime legislation	Laws, where needed, are amended to reflect changes in the international ICT environment.
Comprehensive criminal procedural law containing provisions on the investigation of cybercrime and evidentiary requirements has been adopted and is enforced.	418L3-1	Procedural cybercrime legislation enables cross-border investigation	In the case of cross-border investigation, procedural law stipulates what actions need to be conducted under particular case characteristics, in order to successfully investigate cybercrime.	418L4-1	Contributing to international cybercrime treaties	The country is an active contributor in the global discourse on developing and improving international cybercrime treaties.
The state has ratified regional or international instruments on cybercrime and consistently seeks to implement these measures into domestic law.	418L3-2	Exceeding minimum requirement in international agreements on cybercrime	Measures are in place to exceed minimal baselines specified in international treaties where appropriate,	418L4-2	Regular review of procedural cybercrime legislation	Procedural law, where needed, is amended to adapt to the changing cybercrime landscape and emerging investigative challenges.
	418L3-3	Amendment procedures for procedural cybercrime legislation	which includes procedures to amend procedural legal frameworks as needed.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
421	Legal and Regulatory Frameworks	Criminal Justice System	Law Enforcement	421L1-1	Limited digital forensics capabilities in law enforcement	Traditional investigative measures are applied to cybercrime investigations, with limited digital forensics capacity.	421L2-1	Comprehensive investigative capabilities for cybercrimes
				421L1-2	Training for law enforcement officers	If law enforcement officers receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.	421L2-2	Established chain of custody of digital evidence
							421L2-3	Standards for training for law enforcement officers
422	Legal and Regulatory Frameworks	Criminal Justice System	Prosecution	422L1-1	Limited capabilities to prosecute cybercrimes	A limited number of specialised cybercrime prosecutors have the capacity to build a case based on electronic evidence,	422L2-1	Comprehensive prosecutorial capabilities for cybercrimes
				422L1-2	Training for prosecutors	If prosecutors receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.		
423	Legal and Regulatory Frameworks	Criminal Justice System	Courts	423L1-1	Limited capabilities to judge cybercrimes	A limited number of judges have the capacity to preside over a cybercrime case,	423L2-1	Sufficient jurisdictional capabilities for cybercrimes
				423L1-2	Training for judges	If judges receive training on cybercrime and digital evidence, it is ad-hoc and not specialised.	423L2-2	Specialised training for judges

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A comprehensive institutional capacity with sufficient human, procedural and technological resources to investigate cybercrime cases has been established.	421L3-1	Dedicated investigative resources for cybercrimes	Resources dedicated to fully operational cybercrime units have been allocated based on strategic decision making.	421L4-1	Specialised and continuous training for law enforcement officers	All law enforcement officers receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
Digital chain of custody and evidence integrity is established including formal processes, roles and responsibilities.	421L3-2	Advanced investigative capabilities for cybercrimes	Advanced investigative capabilities allow the investigation of complex cybercrime cases,	421L4-2	Sophisticated digital forensic tools	Law enforcement can utilise sophisticated digital forensic tools, and these technologies are consistently updated.
Standards for the training of law enforcement officers on cybercrime exist and are implemented.	421L3-3	Regular training for law enforcement officers	supported by regular testing and training of investigators.	421L4-3	Regular review of investigative capabilities for cybercrimes	The institutional capacity of law enforcement is frequently reviewed and revised based on an assessment of effectiveness.
	421L3-4	Cross-border investigation of cybercrimes	Law enforcement agencies have the resources to maintain the integrity of data to meet international evidential standards in cross-border investigation.			
	421L3-5	Statistics & analysis of cybercrime investigations	Statistics and trends on cybercrime investigations are collected and analysed.			
A comprehensive institutional capacity, including sufficient human, training and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established.	422L3-1	Institutional structures in prosecution services	Institutional structures are in place, with a clear distribution of tasks and obligations within the prosecution services at all levels of the state.	422L4-1	Prosecution of cross-border cybercrimes	There is national capacity to prosecute complex domestic and cross-border cybercrime cases.
	422L3-2	Statistics & analysis of cybercrime prosecutions	Statistics and trends on cybercrime prosecutions are constantly collected and analysed.	422L4-2	Dedicated prosecutorial resources for cybercrimes	A dedicated cybercrime prosecution unit might have been established.
	422L3-3	Exchange of best practices between prosecutors & judges	A mechanism exists that enables the exchange of information and good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.	422L4-3	Specialised and continuous training for prosecutors	All prosecutors receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
Sufficient human and technological resources are available to ensure effective and efficient legal proceedings regarding cybercrime cases, and cases involving electronic evidence.	423L3-1	Centralised judges for cybercrimes	The court system has organised itself to ensure a central management of cybercrime cases,	423L4-1	Specialised and continuous training for judges	Judges receive specialised and continuous training based on relative responsibilities and new, evolving threat landscapes.
Judges receive specialised training on cybercrime and electronic evidence.	423L3-2	Institutional structures of courts	with clear distribution of tasks and obligations within the court system at all levels of the state.	423L4-2	Regular review of court system capabilities to judge cybercrimes	The institutional capacity of the court system is frequently reviewed and revised based on an assessment of effectiveness.
	423L3-3	Statistics & analysis of cybercrime convictions	Statistics and trends on cybercrime convictions are collected and analysed.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
431	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	431L1-1	Formal international cooperation against cybercrimes	Formal mechanisms of international cooperation have been established,	431L2-1	Established formal international cooperation
				431L1-2	Exchange of information between public & private sectors about cybercrimes	Exchange of information on cybercrime between domestic public and private sectors is ad-hoc and unregulated.	431L2-2	Mutual legal assistance & extradition
							431L2-3	Legislative requirements on information exchange between public & private sectors
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Informal Cooperation	432L1-1	Exchange of information between government & justice about cybercrimes	Exchange of information between government and criminal justice actors is limited and ad-hoc.	432L2-1	Established informal cooperation between government & justice
				432L1-2	Cooperation between ISPs & law enforcement	Ad-hoc cooperation between Internet Service Providers and law enforcement exists, but is not always effective.	432L2-2	Established informal cooperation between ISPs & law enforcement
				432L1-3	Informal international cooperation in law enforcement	Law enforcement cooperates with foreign counterparts on an ad-hoc basis, but is not integrated in regional and international networks.	432L2-3	Informal international integration in law enforcement

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Formal mechanisms of international cooperation have been established in order to prevent and combat cybercrime by facilitating their detection, investigation, and prosecution.	431L3-1	Communication channels for international cooperation	Formal international cooperation mechanisms are fully functional, with established communication channels.	431L4-1	Regular review of international cooperation	Formal international cooperation mechanisms are regularly reviewed to determine effectiveness, and are revised accordingly to reflect the changing cybercrime landscape.
Mutual legal assistance and extradition agreements and mechanisms have been established and are applied to cybercrime cases.	431L3-2	Strategically expanding international cooperation	Strategic decisions are made to expand and enhance formal cooperation mechanisms on cybercrime as needed.	431L4-2	Interoperability of formal & informal international cooperation	Formal and informal international cooperation mechanisms complement each other and are interoperable.
Legislative requirements for the exchange of information between domestic public and private sectors have been determined.	431L3-3	Resources for information exchange between public & private sectors	Resources are allocated to support the exchange of information between public and private sectors domestically and enhance legislative requirements and communication mechanisms.	431L4-3	Regularly adjusted information exchange between public & private sectors	Formal mechanisms that enable the exchange of information between domestic public and private sectors are adapted in accordance with identified needs and changing threat environment.
Informal relationships between government and criminal justice actors have been established, resulting in the regular exchange of information on cybercrime issues.	432L3-1	Established relationship among government, prosecutors, judges & law enforcement	A strategic relationship between government actors, prosecutors, judges and law enforcement agencies has been established relating to cybercrime.	432L4-1	Adapted cooperation & exchange of information	Government and criminal justice actors exchange information timely and efficiently, and cooperation is adapted to the changing cybercrime environment and associated requirements.
Effective informal cooperation mechanisms between Internet Service Providers and law enforcement have been established, with clear communication channels.	432L3-2	Cooperation between foreign ISPs & law enforcement	Law enforcement cooperates with domestic and foreign ISPs in combatting cybercrime.	432L4-2	Adapted international cooperation	A routinized relationship between law enforcement and ISPs, domestically and across borders, has been established and is adaptable to emerging forms of cybercrime.
Domestic law enforcement agencies are informally integrated with regional and international counterparts and networks, such as Interpol or 24/7 networks.	432L3-3	Joint international investigation & prosecution	Law enforcement agencies work jointly with foreign counterparts, potentially through joint task forces, resulting in successful crossborder cybercrime investigations and prosecutions.	432L4-3	Interoperability of formal & informal international cooperation	Formal and informal international cooperation mechanisms complement each other and are interoperable.
			Enhancement	432L4-4	***International and/or regional cooperation of establishing cybercrime legislation***	***The nation cooperates internationally and/or regionally in supporting other nations in establishing cybercrime legislation.***

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	511L1-1	Standards for information risk management	Information risk management standards have been identified for use	511L2-1	Established standards & best practices
				511L1-2	Standards for information risk management partly used	and there have been some initial signs of promotion and take-up within public and private sectors.	511L2-2	Standards & best practices widely used
				511L1-3	International standards & best practices implemented	There is some evidence of measurable implementation and adoption of international standards and good practices.	511L2-3	Metrics of adoption of standards & best practices
							511L2-4	Promotion of use of standards & best practices
							511L2-5	Metrics of compliance of standards & best practices
							511L2-6	Standards & best practices used by CI supply chains
512	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	512L1-1	Standards & best practices for procurement	Cybersecurity standards and good practices guiding procurement processes have been identified for use.	512L2-1	International standards & best practices for procurement implemented
				512L1-2	Promotion of use of standards & best practices for procurement	Evidence of promotion and adoption of cybersecurity standards and good practices in defining procurement practices exists within public sectors and private sectors.	512L2-2	Metrics of adoption of standards & best practices for procurement
							512L2-3	Metrics of compliance of standards & best practices for procurement

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Nationally agreed baseline of cybersecurity related standards and good practices has been identified,	511L3-1	Risk-based adoption of standards & best practices	Government and organisations promote adoption of standards and good practises according to assessment of national risks and budgetary choices.	511L4-1	Regular review of adoption of standards & best practices	The choice of adopted standards and good practices and their implementation is continuously improved.
and adopted widely across public and private sectors.	511L3-2	Resource allocation based on standards	There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drive standard adoption.	511L4-2	Decision making of non-compliance to standards & best practices	Adoption of standards and non-compliance decisions are made in response to changing threat environments and resource drivers across sectors and CI through collaborative risk management.
Some body within government exists to assess level of adoption across public and private sectors.	511L3-3	Contributing to international standards	Evidence of contribution to international standards' bodies exists and contributes to thought leadership and sharing of experience by organisations.	511L4-3	Risk-based decision making of compliance	Evidence exists of debate within all sectors on compliance to standards and good practices, based on continuous needs assessments.
Government schemes exist to promote continued enhancements,						
and metrics are being applied to monitor compliance.						
Consideration is being given to how standards and good practices can be used to address risk within supply chains within the CI, by both government and CI.						
Procurement practices meet international IT guidelines, standards and good practices.	512L3-1	Standards & best practices for procurement widely used & complied	Cybersecurity standards and good practices in guiding procurement processes are being adhered to widely within public and private sectors.	512L4-1	Realtime monitoring of non-compliance to standards & best practices for procurement	Organisations have the ability to monitor use of standards and good practices in procurement processes and support deviations and noncompliance decisions in real-time
Adoption	512L3-2	Regular review of procurement	Critical aspects of procurement and supply, such as prices and costs, quality, timescales and other value adding activities are continuously improved,	512L4-2	Risk-based decision making of non-compliance	through risk-based decision making and quality assurance.
and compliance of standards in procurement practices within the public and private sectors, is evidenced through measurement and assessments of process effectiveness.	512L3-3	Wider resource planning in procurement	and procurement process improvements are made in the context of wider resource planning.			
	512L3-4	Procurement skills benchmark	Organisations are able to benchmark the skills of their procurement professionals against the competencies outlined in procurement standards and identify any skills and capability gaps.			
	512L3-5	E-sourcing / e-tendering	Internal stakeholders have been trained in the secure use of E-sourcing or E-tendering systems and purchase-to-pay systems (P2P) in order to implement these tools in performing key tasks in procurement and supply.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
513	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	513L1-1	Standards & best practices for development	Core activities and methodologies for software development processes focused on integrity and resilience are being discussed within professional communities.	513L2-1	Metrics of adoption of standards & best practices for development
				513L1-2	Promotion of use of standards & best practices for development	Government promotes relevant standards in software development, but there is no widespread use of these standards yet.	513L2-2	Education & training for development
				513L1-3	Coding standards	Some organisations supply or seek to adopt standards in code development.		
521	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	521L1-1	Limited internet infrastructures	Limited Internet services and infrastructure are available, but may not be reliable.	521L2-1	Reliable internet infrastructures
				521L1-2	Discussion on resilience of internet infrastructures	Resilience of Internet infrastructure in public and private sectors has been discussed by multiple stakeholders, but has not been fully addressed.	521L2-2	Established e-commerce & electronic authentication
							521L2-3	Internet infrastructures compliant to international standards & best practices
							521L2-4	Internet infrastructures formally managed
531	Standards, Organisations, and Technologies	Software Quality	Software Quality	531L1-1	Quality & functional requirement of software	Software quality and functional requirements in public and private sectors are recognised and identified, but not necessarily in a strategic manner.	531L2-1	Established quality & functional requirement of software
				531L1-2	Catalogue of secure softwares	A catalogue for secure software platforms and applications within the public and private sectors is under development.	531L2-2	Softwares complying with international standards
				531L1-3	Software update policies under development	Policies and processes on software updates and maintenance are now under development.	531L2-3	Established software update processes
				531L1-4	Software deficiencies information	Evidence of software quality deficiencies is being gathered and assessed regarding its impact on usability and performance.	531L2-4	Software classification

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Government has an established programme for promoting and monitoring standard adoption in software development – both for public and commercial systems.	513L3-1	Security consideration in all stages	Security considerations are incorporated in all stages of software development.	513L4-1	Risk-based decision making of non-compliance	Software development projects continuously assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions.
Evidence that high integrity systems and software development techniques are present within the educational and training offerings in the country.	513L3-2	Core development activities	Core development activities, including configuration and documentation management, security development and lifecycle planning have been adopted.	513L4-2	Adopting standards throughout life-time	Procurement of software includes on-going assessments of the value of standards in delivering software quality – throughout the lifetime of the contract (as opposed to simply initially at procurement stage).
	513L3-3	Risk-based adoption of standards	Procurement of software developed according to required standards is considered based on an assessment of risk in investment decisions.	513L4-3	Explicit requirements by contract	Requirements are built into contracts with suppliers.
Reliable Internet services and infrastructure have been established.	521L3-1	Metrics of compliance to international standards of internet infrastructures	Regular assessment of processes according to international standards and guidelines are conducted together with assessment of national information infrastructure security and critical services	521L4-1	Controlled acquisition of infrastructures	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics.
Internet is used for ecommerce and electronic business transactions; authentication processes are established.	521L3-2	Investment to new technologies in internet infrastructures	that drive investment in new technologies.	521L4-2	Optimised cost for internet infrastructures	Costs for infrastructure technologies are continually assessed and optimised.
Technology and processes deployed for Internet infrastructure meet international IT guidelines, standards, and good practices.				521L4-3	Controlled acquisition of critical technologies	There is effectively controlled acquisition of critical technologies with managed strategic planning and service continuity processes in place.
National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.				521L4-4	Independency & persistence of internet infrastructure technologies	Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced and perpetuated in order to maintain the country's independent resilience.
Software quality and functional requirements in public and private sectors are recognised and established.	531L3-1	Monitoring software quality	Quality of software used in public and private sectors is monitored and assessed.	531L4-1	High performance, reliability & usability softwares	Software applications of high level performance, reliability and usability are available,
Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors.	531L3-2	Review of software update policies & processes	Policies and processes on software updates and maintenance are being improved based on risk assessments and the criticality of services.	531L4-2	Automated service continuity	with service continuity processes fully automated.
Policies on and processes for software updates are established.	531L3-3	Business benefit from improving software quality	Benefits to businesses from additional investment in ensuring software quality and maintenance are measured and assessed.	531L4-3	Regular review of quality requirement	Requirements of software quality are being systematically reviewed, updated, and adapted to the changing cybersecurity environment.
Software applications are characterised as to their reliability, usability and performance in adherence to international standards and good practices.	531L3-4	Software deficiency handling	Software defects are manageable in a timely manner and service continuity is ensured.			

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
541	Standards, Organisations, and Technologies	Technical Security Controls	Technical Security Controls	541L1-1	Technical security controls deployed	Technical security controls are deployed by users, public and private sectors, but inconsistently.	541L2-1	Latest technical controls & patch managements widely implemented
				541L1-2	Latest technical security controls promoted	The deployment of up-to-date technical security controls is promoted in an ad-hoc manner and all sectors are being incentivised to their use.	541L2-2	Anti-malware softwares & network firewalls
				541L1-3	Anti-malware services by ISPs	ISPs may be offering antimalware software as part of their services but possibly in an ad-hoc manner.	541L2-3	Physical security controls
				541L1-4	ISPs' policies of technical security control	ISPs recognise the need to establish policies for technical security control deployment as part of their services.	541L2-4	Established ISPs' policies of technical security control
				541L1-5	IDS/IPS deployed	Network Intrusion Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed but not necessarily in a consistent manner.	541L2-5	Technical security controls based on international frameworks
551	Standards, Organisations, and Technologies	Cryptographic Controls	Cryptographic Controls	551L1-1	Cryptographic controls deployed	Cryptographic controls for protecting data at rest and in transit are recognised and deployed ad-hoc by multiple stakeholders and within various sectors.	551L2-1	Cryptographic controls widely used
				551L1-2	TLS deployed	State of the art tools, such as SSL or TLS, are deployed ad-hoc by web service providers to secure all communications between servers and web browsers.	551L2-2	Secure communication services
							551L2-3	Cryptographic controls complied to international standards
							551L2-4	TLS widespread
561	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cybersecurity Technologies	561L1-1	Domestic security products market	The domestic market may provide non-specialised cybersecurity products, but these are not marketdriven.	561L2-1	Domestic providers of security products
				561L1-2	Cybersecurity consideration in development	Cybersecurity is considered in software and infrastructure development.	561L2-2	Lowering dependency on foreign cybersecurity technologies

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
Up-to-date technical security controls, including patching and backups, are deployed in all sectors.	541L3-1	User side security controls	Penetration of technical security controls leads to effective upstream protection of users and public/private sectors.	541L4-1	Continuous assess of technical security controls	All sectors have the capacity to continuously assess the security controls deployed for their effectiveness and suitability according to their changing needs.
Users have an understanding of the importance of anti-malware software and network firewalls across devices.	541L3-2	Regular review of technical security controls	Within the public and private sectors, technical security controls are being kept up-to-date, monitored for effectiveness and reviewed on a regular basis.	541L4-2	Business impact by technical security controls understood	The understanding of the technical security controls being deployed extends to its impact on organisational operations and budget allocation.
Physical security controls are employed to prevent unauthorized personnel from entering computing facilities.				541L4-3	Supplemental security services by ISPs	ISPs supplement technical security controls with multi factor authentication, digital certificates and whitelisting to ensure prevention of access of non-trusted sites or web addresses and maintain a safe internet environment.
ISPs establish policies for technical security control deployment as part of their services.						
The technical cybersecurity control set is based on established cybersecurity frameworks, such as the SANS top 20 cybersecurity controls, the CESG 10 steps to cybersecurity, or PAS 55.						
Cryptographic techniques are available for all sectors and users for protection of data at rest or in transit.	551L3-1	Risk-based use of cryptographic controls	The public and private sectors critically assess the deployment of cryptographic controls, according to their objectives and priorities.	551L4-1	Regular review of relevance of cryptographic controls	The relevance of cryptographic controls deployed for securing data at rest and data in transit is continuously assessed through risk assessments.
There is a broad understanding of secure communication services, such as encrypted/signed email.	551L3-2	Regular review of cryptographic control policies	The public and private sectors have developed encryption and cryptographic control policies based on the previous assessment, and regularly review the policies for effectiveness.	551L4-2	Revision of cryptographic control policies	The public and private sector adapt encryption and cryptographic control policies based on the evolution of technological advancement and changing threat environment.
The cryptographic controls deployed meet international standards and guidelines accordingly for each sector and are kept up-to-date.						
State of the art tools, such as SSL or TLS, are deployed routinely by web service providers to secure all communications between servers and web browsers.						
Cybersecurity products are now being produced by domestic providers in accordance with market needs.	561L3-1	Security products complied to International standards	Cybersecurity technology development abides by secure coding guidelines, good practices and adhere to internationally accepted standards.	561L4-1	Automated security functions	Security functions in software and computer system configurations are automated in the development and deployment of technologies.
National dependence on foreign cybersecurity technologies is increasingly mitigated through enhanced domestic capacity.	561L3-2	Risk-based product development	Risk assessments and market incentives inform the prioritisation of product development to mitigate identified risks.	561L4-2	Exporting superior security products	Domestic cybersecurity products are exported to other nations and are considered superior products.

Appendix B

#	Category	Subcategory	Capacity area	Level 1			Level	
				ID	Keywords	Details	ID	Keywords
562	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cyber Insurance	562L1-1	Needs for cybersecurity insurance understood	The need for a market in cyber insurance has been identified through the assessment of financial risks for public and private sectors,	562L2-1	Established cybersecurity insurance market
				562L1-2	Development of cybersecurity insurance	and development of products is now being discussed.	562L2-2	Covering additional costs (ex. Forensic investigation etc.)
571	Standards, Organisations, and Technologies	Responsible Disclosure	Responsible Disclosure	571L1-1	Information sharing of vulnerabilities	Technical details of vulnerabilities are shared informally with other stakeholders who can distribute the information more broadly.	571L2-1	Established vulnerability disclosure framework
				571L1-2	Ability to address vulnerability reports	Software and service providers are able to address bug and vulnerability reports.	571L2-2	Established processes against vulnerability information
							571L2-3	Non legal action

2	Level 3			Level 4		
Details	ID	Keywords	Details	ID	Keywords	Details
A market for cyber insurance is established and encourages information sharing among participants of the market.	562L3-1	Covering various costs	Cyber insurance specifies a variety of coverages to mitigate consequential losses.	562L4-1	Innovative cybersecurity insurance market	The cyber insurance market is innovative
Third-party insurance covers liability and the costs of forensic investigations, customer notification, credit monitoring, public relations, legal defence, compensation and regulatory fines.	562L3-2	Choice of coverages	These coverages are selected based on strategic planning needs and identified risk.	562L4-2	Emerging risks & various cyber harm	and adapts to emerging risks, standards and practices, while addressing the full scope of cyber harm.
	562L3-3	Cybersecurity insurance products for SMEs	Products suitable for SMEs are also on offer.	562L4-3	Premium discount for secure behaviour	Insurance premiums are offered for consistent cybersecure behaviour.
A vulnerability disclosure framework is in place, which includes a disclosure deadline, scheduled resolution, and an acknowledgement report.	571L3-1	Established responsible disclosure processes	Responsible disclosure processes for all involved stakeholders (product vendors, customers, security vendors and public) are set.	571L4-1	Regular review of vulnerability disclosure policies	Responsible disclosure policies are continuously reviewed and updated based on the needs of all affected stakeholders.
Organisations have established processes to receive and disseminate vulnerability information.	571L3-2	Analysis & dissemination processes	An analysis of the technical details of vulnerabilities is published and advisory information is disseminated according to individual roles and responsibilities.	571L4-2	Internationally contributing to responsible disclosure	Responsible disclosure frameworks are shared internationally, so that best practice in this area can be created.
Software and service providers commit to refrain from legal action against a party disclosing information responsibly.	571L3-3	Deadlines of update	The large majority of products and services are updated within predetermined deadlines.	571L4-3	Deadlines of update complied	All affected products and services are routinely updated within deadline.
				571L4-4	Reviewing process of deadlines	Processes are in place to review and reduce deadlines.

Appendix C Japanese Cybersecurity Strategy

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-111ア	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	安全なIoTシステムを活用した新規事業の振興	内閣官房において、IoTシステムに係る新規事業がセキュリティ・バイ・デザインの考え方に基づき取り組まれるよう、経費の見積もりの方針にこうした考え方を盛り込むとともに、各府省庁等において、こうした考え方に基づく取組が行われるよう働きかけを引き続き行う。さらに着実にこの考え方に基づく取組が行われているか適時確認をする。
7-112ア	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る体系及び体制の整備	内閣官房において、IoTシステムに係る大規模な事業のサイバーセキュリティ確保のための取組について、サイバーセキュリティ戦略本部の下で検討を進めるとともに、IT総合戦略本部等においても現在検討が進められているIoTシステムに係る大規模な事業について、関係省庁が適切に協働し、セキュリティ・バイ・デザインの考え方に基づいて必要な対策が整合的かつ遺漏なく実施されていくよう働きかけを行う。さらに、その確認を適時確認していく。また、「安全なIoTシステムのためのセキュリティに関する一般的枠組」を踏まえつつ、官民の連携の下、安全なIoTシステムの創出に向けた取組を推進する。
7-112ア2	↑	↑	↑	↑
7-112イ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る体系及び体制の整備	内閣官房及び関係省庁において、サイバー環境をよりクリーンなものに保つため、官民が連携して「ボット撲滅」に向けた体制を構築し対策を推進するための検討を行う。
7-113ア	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る制度整備	総務省及び経済産業省において、IoT推進コンソーシアムを通じて、IPA及びNICTと連携しつつ、IoTセキュリティガイドラインを様々な産業分野の標準仕様等に反映させるべく、普及展開に努めるとともに、IoTセキュリティに関する研究開発、実証実験、IoTセキュリティの確保に向けた総合的な対策及びIoT製品やシステムにおける「セキュリティ・バイ・デザイン」の国際的展開に向けた活動を行う。
7-113ア2	↑	↑	↑	↑
7-113イ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る制度整備	経済産業省において、IoTシステムの構成要素であるM2M機器等の制御システム向けのセキュリティに係る認証制度であるEDSA認証（2014年4月開始）について、普及・啓発を行うとともに、制御システム全体のセキュリティ評価・認証の仕組みを検討する。
7-113ウ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る制度整備	経済産業省において、JPCERT/CCを通じて、インターネット上の公開情報を分析し、国内の制御システム等で外部から悪用されてしまう危険性のあるシステムの脆弱性や設定の状況について、その保有組織に対して情報を提供する。
7-113エ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る制度整備	経済産業省において、IPA（受付機関）とJPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度により、ソフトウェアに係る脆弱性について、「JVN」をはじめ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」などを通じて利用者に提供する。さらに、能動的な脆弱性の検出とその調整に関わる取組を行う。また、海外の調整機関や研究者とも連携し、国外で発見された脆弱性について、国内開発者との調整、啓発活動をJPCERT/CCにおいて実施する。
7-114ア	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る技術開発・実証	経済産業省において、AIST等を通じ、IoTシステムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、などを両立させるための革新的、先端的技術の基礎研究に取り組む。
7-114イ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る技術開発・実証	経済産業省において、IoTのセキュリティ対策等に関する研究開発を行う。
7-114ウ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る技術開発・実証	経済産業省において、制御システムのテスト環境を用いシステム全体の脅威分析、リスク評価を行う技術開発を行う。
7-114エ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る技術開発・実証	内閣府SIP（戦略的イノベーション創造プログラム）を中心に、経済産業省、総務省をはじめとする関係省庁と連携し、自動車のセキュリティ上の課題について、車両レベル・コンポーネントレベル、制御システム等の研究開発を推進する。
7-114オ	経済社会の活力の向上及び持続的発展	安全なIoTシステムの創出	IoTシステムのセキュリティに係る技術開発・実証	総務省において、「IoTセキュリティ対策の取組方針ver1.0」を踏まえ、既に流通している脆弱性を有するIoT機器のセキュリティ対策に取り組むとともに、今後製造するIoT機器のセキュリティ対策について検討を行う。
7-121ア	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	経営層の意識改革	内閣官房において、関係府省庁と協力して、2016年に決定した「企業経営のためのサイバーセキュリティの考え方」を踏まえ、企業のサイバーセキュリティに係る取組について、現状の把握を行い、さらなるサイバーセキュリティ対策の推進に関する検討を行う。
7-121イ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	経営層の意識改革	経済産業省において、経営層がサイバーリスクを経営上の重要課題として把握し、設備投資、体制整備、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、サイバーセキュリティ経営ガイドラインの普及を図る。
7-121ウ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	経営層の意識改革	経済産業省において、企業のサイバーセキュリティ対策を推進するため、サイバーセキュリティ保険など、情報の保護が必要となる政府の補助事業や研究開発事業等の採択に際して、上記のサイバーセキュリティ経営ガイドラインや第三者認証取得など企業のサイバーセキュリティ対策への取組を、加点要素等として考慮する仕組みなどのインセンティブ策を検討する。

("Cybersecurity 2017" itemised to action items)

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-111a	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Promoting New Business Harnessing Secured IoT Systems	Cabinet Secretariat	Promoting 'Security-by-Design' in new business harnessing IoT systems.
7-112a	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Improving Structural Frameworks for IoT Systems Security	Cabinet Secretariat	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.
7-112a2	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Improving Structural Frameworks for IoT Systems Security	Cabinet Secretariat	Promoting secure IoT systems based on "General Framework for Secure IoT Systems".
7-112b	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Improving Structural Frameworks for IoT Systems Security	Cabinet Secretariat	Considering measures to exterminate 'bot-net'.
7-113a	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	MIC, METI, NICT, IPA	Promoting "IoT Security Guidelines".
7-113a2	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	MIC, METI, NICT, IPA	Promoting "IoT Security Guidelines" as international standard.
7-113b	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	METI	Promoting "EDSA certification" (security certification for control systems).
7-113c	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	METI, JPCERT/CC	Analysing open source information & warning organisations of vulnerable systems.
7-113d	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	METI, IPA, JPCERT/CC	Continuing operation of reporting & dissemination system for vulnerability information.
7-114a	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Implementing Technological Development and Demonstration Related to IoT Systems Security	METI, AIST	Researching innovative & advanced technologies.
7-114b	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Implementing Technological Development and Demonstration Related to IoT Systems Security	METI	Researching technologies for security countermeasures for IoTs.
7-114c	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Implementing Technological Development and Demonstration Related to IoT Systems Security	METI	Developing technologies of threat analysis & risk evaluation for control systems.
7-114d	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Implementing Technological Development and Demonstration Related to IoT Systems Security	Cabinet Secretariat, METI, MIC	Researching & developing technologies for automotive security in "SIP: Cross-ministerial Strategic Innovation Promotion Program".
7-114e	Improvement of Socio-Economic Vitality and Sustainable Development	Creation of Secured IoT Systems	Considering Approaches for Enhanced IoT Systems Security	MIC	Promoting countermeasures against vulnerable IoT products in the market based on "Policy for IoT Security Countermeasures ver.1.0".
7-121a	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Changing the Thinking of Senior Executive Management	Cabinet Secretariat	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of Cybersecurity for Corporate Management".
7-121b	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Changing the Thinking of Senior Executive Management	METI	Promoting "Cybersecurity Management Guidelines".
7-121c	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Changing the Thinking of Senior Executive Management	METI	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring them in national tenders.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-122ア	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	経営能力を高めるサイバーセキュリティ人材の育成	内閣官房において、サイバーセキュリティ人材育成プログラムを踏まえ、経営層、橋渡し人材層、実務者層など、それぞれの人材層向けのさまざまな施策について連携を強化することにより、より効果的かつ効率的に施策が進められるよう、施策間連携を図るためのワーキンググループを通じ、モデルとなる具体的な人材育成のカリキュラムの策定等を行う。
7-123ア	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、JPCERT/CCを通じて、ソフトウェア製品や情報システムの開発段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。
7-123イ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、営業秘密保護や事業継続性の観点からも経営層がサイバーリスクを重要課題として把握し、人材育成等経営資源に係る投資判断を行い、組織能力の向上を図るために、説明会等を通じて、サイバーセキュリティ経営ガイドラインの普及を図る。またIPAを通じて、中小企業における情報セキュリティ対策の実施を促すため、説明会等において中小企業の情報セキュリティ対策ガイドラインの普及を図る。
7-123イ2	↑	↑	↑	↑
7-123ウ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、リスクの高い丸投げ下請や多様化するセキュリティ対策費用の増加に応じた適切な価格設定に向け、セミナー等を通した下請ガイドラインの更なる浸透を図るとともに、業界団体と連携したフォローアップなどを実施し、情報システム開発・運用に係る取引の適正化を図る。
7-123エ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、JPCERT/CCを通じ、企業へのサイバー攻撃等への対応能力向上に向けて、国内における組織内CSIRT設立を促進・支援する。また、CSIRTの構築・運用に関するマテリアルや、インシデント対策・対応に資する脅威情報や攻撃に関する情報、所要の分析を加えた具体的な対策情報等を適切な者の間で共有することにより、CSIRTの普及や、国内外の組織内CSIRTとの間における緊急時及び平常時の連携の強化を図るとともに、巧妙かつ執拗に行われる標的型攻撃への対処を念頭においた運用の普及、連携を進める。
7-123オ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）を実施する。また、2020東京オリンピック・パラリンピック競技大会に向けた大規模演習環境「サイバーコロッセオ」を活用し、同大会のサイバーセキュリティを守る高度な人材の育成を推進する。
7-123オ2	↑	↑	↑	↑
7-123カ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、重要インフラ企業等に対するサイバー攻撃への対処能力向上のため、模擬システム等を用いた実践的なサイバー演習を行う。
7-123キ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、IPAを通じ、我が国経済社会に被害をもたらすおそれが強く、一組織で対処が困難なサイバー攻撃を受けた組織等を支援するため、「サイバーレスキュー隊（J-CRAT）」の活動を増強し、被害組織における迅速な対応・復旧に向けた計画作りを支援する。
7-123ク	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	金融庁において、参加金融機関および金融業界全体のセキュリティレベルの底上げを図るため、攻撃の実例分析を踏まえた金融業界横断的なサイバーセキュリティ演習を引き続き実施する。
7-123ケ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、IPAを通じ、ウェブアプリケーションの脆弱性を早期に発見し、対処に役立てるため、ログを解析し外部からの攻撃の痕跡を検査する「ウェブサイトの攻撃兆候検出ツール」（iLogScanner）を企業のウェブサイト運営者等に提供する。
7-123コ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	経済産業省において、最新の脅威情報やインシデント情報等の共有のためIPAを通じ実施している「サイバー情報共有イニシアティブ」（J-CSIP）の運用を着実に継続し、より有効な活動に発展させるよう参加組織の拡大、共有情報の充実等、民民、官民における一層の情報共有網の拡充を進める。
7-123サ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	総務省において、ISP事業者やICTベンダー等を中心に構成されている「ICT-ISAC」を核として、国際連携を含めてサイバー攻撃に関する情報共有網の拡充を推進する。
7-123シ	経済社会の活力の向上及び持続的発展	セキュリティマインドを持った企業経営の推進	組織能力の向上	金融庁において、金融機関に対し、「金融ISAC」を含む情報共有機関等を通じた情報共有網の拡充を進める。
7-131ア	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	サイバーセキュリティ関連産業の振興	経済産業省において、一定のセキュリティ品質を有するセキュリティサービスを認定する体制を整備することにより競争力強化や活用促進を図るなど、サイバーセキュリティの成長産業化に取り組む。
7-131イ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	サイバーセキュリティ関連産業の振興	総務省及び経済産業省において、クラウドセキュリティガイドライン、クラウドセキュリティ監査制度等の普及促進を行う。
7-131ウ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	サイバーセキュリティ関連産業の振興	経済産業省において、中小企業における情報セキュリティ投資を促進するための施策を推進する。
7-131エ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	サイバーセキュリティ関連産業の振興	文部科学省において、著作権法におけるセキュリティ目的のリバースエンジニアリングに関する適法性の明確化に関する措置を速やかに講ずる。
7-132ア	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	公正なビジネス環境の整備	経済産業省において、産業界及び関係省庁と連携し、企業情報の漏えいに関して、サイバー攻撃など今後ますます高度化・複雑化が予想される最新の手口や被害実態などの情報の共有を行う場として、「営業秘密官民フォーラム」を開催する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-122a	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Fostering Cybersecurity Workforce for Advanced Business Management	Cabinet Secretariat	Promoting human resources development for each category - board members, bridge personnel & working-level - based on "Cybersecurity Human Resources Development Program".
7-123a	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI, JPCERT/CC	Promoting 'Security-by-Design'.
7-123b	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	same as 7-121c2	same as 7-121c2
7-123b2	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI, IPA	Promoting "Cybersecurity Management Guidelines" to SMEs (small-to medium-sized enterprises).
7-123c	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI	Reviewing rules & regulations so as to improve security of whole supply chains of IT development & operation.
7-123d	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI, JPCERT/CC	Encouraging corporates to establish CSIRT.
7-123e	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	MIC, NICT	Performing practical cyber defence exercise "CYDER" at "National Cyber Training Center".
7-123e2	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	MIC, NICT	Performing cyber exercises assuming attacks against Tokyo Olympics/Paralympics in 2020, employing large scale exercise environment "Cyber Colosseo".
7-123f	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI	Performing practical APT exercises.
7-123g	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI, IPA	Enhancing "J-CRAT: Cyber Rescue Team" (activity to assist organisational incident responses).
7-123h	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	FSA	Performing financial industry-wide cyber exercises.
7-123i	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI, IPA	Promoting "iLogScanner: Attack Indication Detecting Tool for Websites".
7-123j	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	METI	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
7-123k	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	MIC	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-ISAC).
7-123l	Improvement of Socio-Economic Vitality and Sustainable Development	Promotion of Enterprise Management with a Security Mindset	Strengthening Organizational Capabilities	FSA	Enhancing "Financial ISAC Japan".
7-131a	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Promoting Cybersecurity-related Businesses	METI	Cultivating cybersecurity-related business to a growth industry by establishing certification for security services.
7-131b	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Promoting Cybersecurity-related Businesses	MIC, METI	Promoting "Cloud Security Guidelines" & "Cloud Audit System".
7-131c	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Promoting Cybersecurity-related Businesses	METI	Promoting security investment of SMEs (small-to medium-sized enterprises).
7-131d	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Promoting Cybersecurity-related Businesses	MEXT	Reconsidering "Copyright Act" about reverse engineering for security purposes.
7-132a	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Developing Fair Business Environment	METI	Continuing "Public & Private Sectors Forum for Trade Secret" to share information about information exfiltration.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-132イ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	公正なビジネス環境の整備	経済産業省において、企業の情報漏えいの防止に資するため、「秘密情報の保護ハンドブック～企業の価値向上に向けて～」及び「秘密情報の保護ハンドブックのてびき～情報管理も企業力～」についての普及啓発を図る。
7-132ウ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	公正なビジネス環境の整備	経済産業省において、IPAを通じ、営業秘密保護に関する対策等を推進するため、組織における内部不正防止のためのガイドラインの普及促進を図る。
7-132エ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	公正なビジネス環境の整備	経済産業省及び外務省において、情報セキュリティなどを理由にしたローカルコンテント要求、国際標準から逸脱した過度な国内製品安全基準、データローカライゼーション規則等、我が国企業が経済活動を行うに当たって貿易障壁となるおそれのある国内規制（「Forced Localization Measures」）を行う諸外国に対し、対話や意見交換を通じ、当該規制が自由貿易との間でバランスがとれたものとなるよう、民間団体とも連携しつつ働きかけを行う。
7-133ア	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	総務省及び経済産業省において、専門機関と連携し、情報セキュリティ分野の国際標準化活動であるISO/IEC JTC1/SC27、ITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて国際標準化を推進する。
7-133イ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、IPAを通じ、情報セキュリティ分野と関連の深い国際標準化活動であるISO/IEC JTC1/SC27が主催する国際会合等へ機構職員を派遣し、暗号技術、暗号・セキュリティ製品やモジュールの認証等の国際標準化において、国内の意見が反映されるよう活動する。
7-133ウ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、情報システム等がグローバルに利用される実態に鑑み、IPA等を通じ、脆弱性対策に関するSCAP、CVSS等の国際的な標準化活動等に参画し、情報システム等の国際的な安全性確保に寄与する。
7-133エ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、IPAを通じ、CCRAなどの海外連携、セキュリティ評価に係る国際基準の作成や各国の情報収集を行うとともに、安全な政府調達のための国際共通プロテクション・プロファイル（PP）の開発、情報収集を実施する。
7-133オ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、アジアでの更なる情報セキュリティ人材の育成を図るため、アジア12か国・地域と相互・認証を行っている「情報処理技術者試験」について、我が国の情報処理技術者試験制度を移入して試験制度を創設した国（フィリピン、ベトナム、タイ、ミャンマー、マレーシア、モンゴル、バングラデシュ）が協力して試験を実施するための協議会であるITPECがアジア統一試験を実施しているところ、ITPECの更なる定着を図る。
7-133カ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、今後、ますますの経済連携が求められるASEAN各国において、我が国企業が安全に活動でき、また、我が国の持つノウハウをASEAN諸国と共有できるよう、セキュリティマネジメント導入のためのノウハウ支援等を行う。
7-133キ	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、JPCERT/CCを通じて、我が国企業が組込みソフトウェア等の開発をアウトソーシングしている先のアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。
7-133ク	経済社会の活力の向上及び持続的発展	セキュリティに係るビジネス環境整備	我が国企業の国際展開のための環境整備	経済産業省において、IoTシステムセキュリティの国際標準規格を視野に入れた認証制度にかかる評価・検討を行う。
7-211ア	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、JPCERT/CCを通じて、ソフトウェア製品や情報システムの開発段階において、製品開発者が情報セキュリティ上の観点から配慮すべき事項を、解説資料やセミナーの形で公開し、普及を図る。
7-211イ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、IPAを通じ、IoT機器、サービスを支える組込み産業の高度化に向け、産業動向の把握・分析を行うとともに、「セキュリティ・バイ・デザイン」の産業展開の観点から、セキュリティとセーフティ設計プロセスの整合化やシステムアプローチによるセキュリティ分析手法の検討を進め、組込みコーディングスタンダードの整備普及を図る。
7-211ウ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、IPAを通じ、ウェブサイト運営者や製品開発者が脆弱性対策の必要性及び対策手法等を自ら学習することを支援するため、「安全なウェブサイトの作り方」を引き続き公開するとともに、体験的かつ実践的に学ぶツール「AppGoat」についてセミナー等を開催することで更なる普及啓発を図る。
7-211ウ2	↑	↑	↑	↑
7-211エ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、IPAを通じ、情報処理システムや組込みシステム等におけるソフトウェアの不具合や脆弱性が社会に与える混乱や被害を防止する観点から、企画・設計段階からセキュリティ配慮が行われるようIoTセキュリティガイドラインの普及・国際標準化の取り組みを進めるとともに、ソフトウェアによって中核機能が実現される製品、システム及びサービスについて第三者がその安全性・信頼性等を利用者に対し十分に説明できるよう、設計プロセス・利用時体験・流通するデータ等多面的な観点から利用者への品質説明力を強化する。
7-211エ2	↑	↑	↑	↑
7-211エ3	↑	↑	↑	↑
7-211オ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、経済産業省告示に基づき、IPA（受付機関）とJPCERT/CC（調整機関）により運用されている脆弱性情報公表に係る制度を着実に実施するとともに、関係者との連携を図りつつ、「JVNiPedia」（脆弱性対策情報データベース）や「MyJVN」の運用などにより、脆弱性関連情報をより確実に利用者に提供する。
7-211カ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、JPCERT/CCを通じて、ソフトウェア等の脆弱性に関する情報を、マネジメントツールが自動的に取り込める形式で配信する等、ユーザー組織における、ソフトウェア等の脆弱性マネジメントの重要性の啓発活動及び脆弱性マネジメント支援を実施する。
7-211キ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、IPAを通じ、情報システムの脆弱性に対して、プロアクティブに脆弱性を検出する技術の普及・啓発活動を行う。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-132b	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Developing Fair Business Environment	METI	Promoting "Handbook for Confidential Information Protection" & "Guide for Handbook for Confidential Information Protection".
7-132c	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Developing Fair Business Environment	METI, IPA	Promoting guidelines for deterrence/prevention of internal misconduct within organisations.
7-132d	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Developing Fair Business Environment	METI, MOFA	Communicating & negotiating with countries who apply 'Forced Localization Measures'.
7-133a	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	MIC, METI	Supporting international standardization in security through participation to ISO/IEC JTC1/SC27, ITU-T SG17 etc.
7-133b	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI, IPA	Supporting international standardization in cryptography, certification for cryptograph & security products.
7-133c	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI, IPA	Supporting international standardization in vulnerability management like SCAP, CVSS etc.
7-133d	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI, IPA	Supporting international standardization in security evaluation like PP (Protection Profile) etc.
7-133e	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI	Assisting ITPEC (IT Professionals Examination Council: organisation for a common IT examination in Asian countries) by 'exporting' "Japan Information-Technology Engineers Examination".
7-133f	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI	Assisting security management in ASEAN countries.
7-133g	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI, JPCERT/CC	Assisting establishment of 'secure development' in countries where Japanese corporates outsource software development.
7-133h	Improvement of Socio-Economic Vitality and Sustainable Development	Improvement of Cybersecurity Business Environment	Improving Environment for Japanese Enterprises' Global Operations	METI	Researching international standards & evaluation system for IoT systems.
7-211a	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	Same as 7-123b	Same as 7-123b
7-211b	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Promoting 'Security-by-Design' in IoT & embedded systems.
7-211c	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Promoting "How to Secure Your Web Site".
7-211c2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Promoting "AppGoat" (training tool for secure development).
7-211d	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Researching technologies for securer development & more sophisticated evaluation.
7-211d2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	Same as 7-113a3	Same as 7-113a3
7-211d3	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	Same as 7-113a4	Same as 7-113a4
7-211e	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	Same as 7-113h	Same as 7-113h
7-211f	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, JPCERT/CC	Supporting vulnerability management in organisations, by promoting structured languages for vulnerability information.
7-211g	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Promoting 'fuzz testing' for pro-active vulnerability detection.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-211ク	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	総務省において、NICTを通じ、運用するサイバー攻撃観測網（NICTER）について、センサーの高度化等による観測機能の強化を図るとともに、NISCをはじめとする政府機関等への情報提供等を通じた連携強化を図る。
7-211ケ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	総務省において、高度化・巧妙化するマルウェアの被害を防止するため、マルウェアに感染したユーザーを検知し、マルウェアの除去を促す取組（感染駆除）及び閲覧することでマルウェアに感染する悪性サイトへアクセスする利用者に注意喚起を行う取組（感染防止）等を行う実証（ACTIVE）を引き続き実施する。
7-211コ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、JPCERT/CCがインシデント対応支援活動等において解析したマルウェア検体及びその解析結果について、同様の情報を有する国内外の関係機関との適切な相互共有やインターネット定点観測システム（TSUBAME）の運用との連動等の有効活用やその高度化を進める。
7-211サ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、フィッシング対策協議会及びJPCERT/CCを通じてフィッシングに関するサイト閉鎖依頼その他の対策実施に向けた取組等を実施する。
7-211シ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	経済産業省において、IPAを通じ、ソフトウェア等の脆弱性に関する情報をタイムリーに発信するサイバーセキュリティ注意喚起サービス「icat」を提供する。また、各種セミナーやイベントで利用方法を紹介することにより「icat」の普及を図る。
7-211ス	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	警察庁において、公衆無線LANを悪用したサイバー犯罪に対する事後追跡可能性の確保に必要な対策が適切に講じられるよう、必要な対応を行う。
7-211セ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	総務省において、安全に無線LANを利用できる環境の整備に向けて、利用者及びアクセスポイント設置者において必要となるセキュリティ対策に関する検討を行うとともに、利用者及びアクセスポイント設置者に対する周知啓発を実施する。
7-211ソ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	安全・安心なサイバー空間の利用環境の構築	内閣官房及び関係省庁において、サイバー空間を安全に利用でき、また安全に発展させるよう、サイバーインシデント情報やその脅威情報を分析し、民間等の関係主体と共有することで着実にそのインシデント等への対応に繋げるため、情報共有・連携ネットワーク（仮称）の構築・運用に向けた検討を進める。
7-212ア	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	内閣官房において、「新・情報セキュリティ普及啓発プログラム」の改訂を行うとともに、同プログラムに基づき、各府省庁や民間の取組主体と協力して、「サイバーセキュリティ月間」をはじめとし、サイバーセキュリティに関する各種イベント等の開催を通じ普及啓発活動を進める。
7-212イ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	警察庁及び都道府県警察において、教育機関、地方公共団体職員、インターネットの一般利用者等を対象として、情報セキュリティに関する意識・知識の向上、サイバー犯罪による被害の防止等を図るため、サイバー犯罪の現状や検挙事例、スマートフォン等の情報端末やSNS等の最新の情報技術を悪用した犯罪等の身近な脅威等について、ウェブサイトへの掲載、講演の全国的な実施等による広報啓発活動を実施するほか、関係省庁との連携によるスマートフォンに関する青少年に対する有害環境対策の徹底等、スマートフォンの安全利用のための環境整備に向けた取組を実施する。
7-212イ2	↑	↑	↑	↑
7-212ウ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	総務省、法務省及び経済産業省において、電子署名の利活用に関するセミナーの開催及びHPを活用した電子署名の利活用策に関する情報提供を行うことで、国民による安全なサイバー空間の利用をサポートするとともに、認定認証事業者に対する説明会の開催、民間事業者等からの電子署名に関する相談対応等を行うことで、企業における電子署名の利活用の普及促進策を検討・実施する。
7-212エ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	総務省において、文部科学省と協力し、青少年やその保護者のインターネットリテラシー向上を図るため、多くの青少年が初めてスマートフォン等を手にする春の卒業・進学・新入学の時期に特に重点を置き、関係府省庁と協力して啓発活動を集中的に展開する「春のあんしんネット・新学期一斉行動」の取組や、「e-ネットキャラバン」等の青少年や保護者等に向けた啓発講座の実施等を行う。また、「インターネットトラブル事例集」の作成や「情報通信の安心安全な利用のための標語」の募集等を通し、インターネット利用における注意点に関する周知啓発の取組を行う。
7-212オ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	文部科学省において、2015年度に作成した動画教材や指導手引書も活用して、学校における情報モラル教育の充実を図るため、指導主事、教員等を対象としたセミナー及びフォーラムを実施する。
7-212カ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	文部科学省において、全国の学校へ配布する普及啓発資料の作成や、ネットモラルキャラバン隊を通じ、スマートフォン等によるインターネット上のマナーや家庭でのルールづくりの重要性の普及啓発を実施する。
7-212キ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、個人情報も含む情報漏えい対策に取り組むため、IPAを通じ、ファイル共有ソフトによる情報漏えいを防止する等の機能を有する「情報漏えい対策ツール」を民間の配布サイトも活用して一般国民に提供する。
7-212ク	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じ、各府省庁と協力し、情報モラル/セキュリティの大切さを児童・生徒が自身で考えるきっかけとなるように、IPA主催の標語・ポスター・4コマ漫画等の募集及び入選作品公表を行い、国内の若年層における情報モラル/セキュリティ意識の醸成と向上を図る。
7-212ケ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	内閣官房において、主体的に普及啓発活動を行う動きが地域レベルでも促進されるよう、「情報セキュリティ社会推進協議会」等を活用しつつ、産学官民の連携・協力を通じて、必要な取組について検討を進める。
7-212コ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じ、各府省庁と協力し、家庭や学校からインターネットを利用する一般の利用者を対象として情報セキュリティに関する啓発を行う安全教室について、全国各地の関係団体と連携し引き続き開催していく。
7-212サ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じ、広く企業及び国民一般に情報セキュリティ対策を普及するため、地域で開催されるセミナーや各種イベントへの出展、普及啓発資料の配布、セキュリティプレゼンター制度の運用などにより情報の周知を行い、セキュリティ啓発サイトや各種ツール類を用いて、対策情報の提供を行う。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-211h	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	MIC, NICT	Upgrading "NICTER: Network Incident Analysis Center for Tactical Emergency Response".
7-211i	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	MIC	Continuing operation of "ACTIVE: Advanced Cyber Threat Response Initiative" (assistance for users to disinfect malwares from compromised PCs).
7-211j	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, JPCERT/CC	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point observation system).
7-211k	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, JPCERT/CC	Continuing operation of "Council of Anti-Phishing Japan".
7-211l	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	METI, IPA	Promoting "icat: IPA Cyber Security Alert Service".
7-211m	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	NPA	Urging public Wi-Fi service providers to prevent cybercrime & to enable effective tracking back.
7-211n	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	MIC	Initiating Wi-Fi service providers & users to safer communication.
7-211o	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Building a Safe and Secure Cyber Environment for Users	Cabinet Secretariat	Considering development of intelligence sharing platform for government & private sectors.
7-212a	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	Cabinet Secretariat	Initiating users to security in cyber space.
7-212b	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	NPA, MPD, Prefectural Polices	Initiating users to secure use of internet, protection from cybercrimes, latest criminal techniques & safety on smartphones.
7-212b2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	NPA, MPD, Prefectural Polices	Initiating educators & staff of local public entities to elimination of cyber environment that is harmful to youth.
7-212c	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC, MOJ, METI	Promoting use of electronic signature.
7-212d	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC, MEXT	Initiating youth to secure use of internet & smartphones.
7-212e	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MEXT	Continuing moral education for information usage at school.
7-212f	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MEXT	Continuing promotion of moral education for internet usage.
7-212g	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Promoting "Information Leakage Prevention Tool" (tool to prevent data exfiltration through file sharing softwares).
7-212h	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Arousing security awareness of youth.
7-212i	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	Cabinet Secretariat	Assisting local public entities to raise public awareness of security.
7-212j	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Continuing "Safety Class" to raise public awareness of secure internet usage.
7-212k	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Assisting local public entities to raise public awareness of security.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-212シ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じ、中小企業における情報セキュリティ教育担当者や中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ講習講師養成セミナー」を実施するとともに、中小企業団体等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施することで、中小企業のセキュリティレベルの向上、IPA等の作成する啓発資料や情報セキュリティ対策支援サイト等のツール等の利用促進等を図る。
7-212ス	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPA、JPCERT/CCを通じて、情報漏えいの新たな手法や手口の情報収集に努め、一般国民や中小企業等に対し、ウェブサイトやメーリングリスト等を通じて対策情報等、必要な情報提供を行う。
7-212セ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じ、「情報セキュリティ安心相談窓口」、さらに、高度なサイバー攻撃を受けた際の「標的型サイバー攻撃の特別相談窓口」によって、サイバーセキュリティ対策の相談を受け付ける体制を充実させ、一般国民や中小企業等の十分な対策を講じることが困難な組織の取組を支援する。
7-212ソ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	経済産業省において、IPAを通じて、サイバーセキュリティに関する現状把握及び対策を実施する際の参考となる最新の動向の収集・分析・報告書の公表等により、サイバー空間利用者への啓発を推進する。
7-212タ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	文部科学省において、大学等における多岐にわたる情報資産や多様なシステムの利用実態といった特性を踏まえ、大学等のマネジメント面・技術面の取組の強化を促進するとともに、大学等の自律的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る枠組みを整備し、これら取組を支援する。
7-212チ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー空間利用者の取組の促進	個人情報保護委員会において、関係省庁と協力し、2017年5月30日に全面施行された改正個人情報保護法を踏まえ、個人情報取扱事業者における、外部からの不正アクセス等による個人データの漏えい等にかかる対応が適切に実施されるよう、情報セキュリティ関係機関と連携して取り組む。
7-213ア	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、新たな手口の不正アクセスや不正プログラム（スマートフォン等を狙ったものを含む。）の悪用等急速に悪質巧妙化するサイバー犯罪の取締りを推進するため、サイバー犯罪捜査に従事する全国の警察職員に対する部内研修及び民間企業への講義委託の積極的な実施、官民人事交流の推進、技術的に高度な民間資格の活用等、サイバー犯罪への対処態勢を強化する。
7-213イ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、サイバー空間の脅威に対処するため、日本版NCFTAである一般財団法人日本サイバー犯罪対策センター（JC3）や、都道府県警察と関係事業者から成る各種協議会等を通じた産学官連携を促進するとともに、総合セキュリティ対策会議等において官民連携による取組を推進する。
7-213ウ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁、総務省及び経済産業省において、不正アクセス行為の禁止等に関する法律に基づき、不正アクセス行為、フィッシング行為、他人の識別符号を不正に取得・保管する行為等の取締りを強化するとともに、事業者団体に対する不正アクセス行為の手口に関する最新情報の提供や、不正アクセス行為の発生状況及びアクセス制御機能に関する研究開発の状況の公表等を通じ、不正アクセス行為からの防御に関する啓発及び知識の普及を図るなど、官民連携した不正アクセス防止対策を更に推進する。
7-213ウ2	↑	↑	↑	↑
7-213エ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、サイバー空間における犯罪被害防止のための教育等のボランティア活動の促進を図るため、サイバー防犯ボランティアの結成を促すとともに活動の支援を強化することにより、安全で安心なインターネット空間の醸成に向けた取組を推進する。
7-213オ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、スマートフォン利用者等を狙ったサイバー犯罪に関し、情報セキュリティ関連事業者等との連携強化による情報集約等に努め、取締りの強化を図る。また、取締りにより判明した実態等を踏まえ、一般利用者等の情報セキュリティ対策の向上に資する情報発信等を推進する。
7-213カ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、警察大学校サイバーセキュリティ対策研究・研修センターを通じ、サイバー犯罪等の取締りのための情報技術の解析に関する研究及びサイバー犯罪等の取締りに必要な専門的知識・技術に関する研修を実施する。
7-213キ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	経済産業省において、フィッシング詐欺被害の抑制のため、フィッシング対策協議会を通じて、海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及び提供を行う。
7-213ク	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁において、全国の情報技術解析部門で効果的かつ効率的な解析を推進することにより、多様化・複雑化が著しいサイバー犯罪に的確に対処する。また、家電、電気メーター、自動車等の日常生活に近い機器に係るオンライン化等の新たな技術やサービスの開発が次々に進められている背景を踏まえ、デジタルフォレンジックに係る対処能力をより一層強化する。
7-213ケ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	法務省において、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査能力の充実を図る。
7-213コ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	検察当局及び都道府県警察において、サイバー犯罪に適切に対処するとともに，サイバー犯罪に関する条約を締結するための「情報処理の高度化等に対処するための刑法等の一部を改正する法律」（サイバー刑法）の適正な運用を実施する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-212l	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Supporting SMEs (small-to medium-sized enterprises) to enhance security by training security personnel in SMEs & counsellors for SMEs.
7-212m	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA, JPCERT/CC	Providing public & SMEs (small-to medium-sized enterprises) with intelligence of security incidents & countermeasures.
7-212n	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Supporting incident response of public & SMEs (small-to medium-sized enterprises) through "Information Security Consultation Counter" & "APT Special Consultation Counter".
7-212o	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	METI, IPA	Collecting, analysing & reporting cybersecurity information.
7-212p	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MEXT	Urging universities to enhance information security.
7-212q	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	PPC	Taking course of action to implement newly effected "Amended Act on the Protection of Personal Information".
7-213a	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Strengthening capability of investigation of cybercrime.
7-213b	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Enhancing cooperation between public, private & academic sectors, with "JC3: Japan Cybercrime Control Center" (Japanese version of NCFTA (National Cyber-Forensics & Training Alliance) playing the central role.
7-213c	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA, MIC, METI	Strengthening capability of investigation of unauthorized access, phishing & illegal acquisition/retention of third party IDs.
7-213c2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA, MIC, METI	Providing corporates with intelligence of latest criminal techniques, etc.
7-213d	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Supporting establishment of anti-cybercrime voluntary corps.
7-213e	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Strengthening capability of investigation of crimes targeting smartphone users.
7-213f	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA, NPAc Research and Training Center for Cybersecurity Countermeasures	Training investigators specialized in cybercrime.
7-213g	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	METI,	Collecting & disseminating information about phishing through operation of "Council of Anti-Phishing Japan".
7-213h	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Making the most of High-Tech Crime Technology Division to tackle complicated & diversified cybercrimes.
7-213i	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	MOJ	Training prosecutors for cybercrimes.
7-213j	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	MOJ, NPA, Prefectural Police	Taking a course of action against cybercrimes upon effectuation of "Cyber Criminal Law".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-213サ	国民が安全で安心して暮らせる社会の実現	国民・社会を守るための取組	サイバー犯罪への対策	警察庁及び総務省において、安全・安心なサイバー空間を構築するため、通信履歴等に関するログの保存の在り方については、「電気通信事業における個人情報保護に関するガイドライン」の解説を踏まえ、関係事業者における適切な取組を推進するなど必要な対応を行う。
7-213サ2	↑	↑	↑	↑
7-220ア	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	内閣官房及び重要インフラ所管省庁等において、「重要インフラの情報セキュリティ対策に係る第4次行動計画」に基づき、安全基準等の整備及び浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化の5つの施策を実施する。 ・「安全基準等の整備及び浸透」については、重要インフラ各分野に横断的な指針の策定とそれに基づく、各分野の「安全基準」等の整備・浸透を促進する。 ・「情報共有体制の強化」については、連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化を行う。 ・「障害対応体制の強化」については、官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化を行う。 ・「リスクマネジメント及び対処態勢の整備」については、リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援を行う。 ・「防護基盤の強化」については、重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等を推進する。
7-220イ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	重要インフラ事業者等及び重要インフラ所管省庁は、重要インフラ全体の防護能力の維持・向上を目的とし、各重要インフラ事業者等の対策の経験から得た知見等をもとに、継続的に安全基準等を改善する。加えて、内閣官房及び重要インフラ所管省庁は、情報セキュリティを更に高めるため、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等における保安規制として位置付けることや、機能保証の観点から適切な情報セキュリティ対策を実施できるようサービス維持レベルを関係法令等において具体化することなど、制度的枠組みを適切に改善する取組を継続的に進める。内閣官房は、重要インフラ所管省庁による安全基準等の改善状況を年度ごとに調査し、その結果を公表する。
7-220イ2	↑	↑	↑	↑
7-220ウ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	内閣官房において、重要インフラサービスを安全かつ持続的に提供できるよう、重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、情報セキュリティ対策に関する取組を推進する。また、この取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。 ・迅速かつ効率的な情報共有に資するため、情報共有システム構築に係る調査検討を行う。 ・重要インフラ事業者等における平時のリスクアセスメントへの利活用のための「機能保証に向けたリスクアセスメント・ガイドライン」の一般化を行う。 ・事業継続計画及びコンティンジェンシープランに盛り込まれるべき要点等を整理する。 ・事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の整理等を行う。
7-220ウ2	↑	↑	↑	↑
7-220エ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	総務省において、重要インフラにおけるサービスの持続的な提供に向け、重要無線通信妨害事案の発生時の対応強化のため、申告受付の夜間・休日の全国一元化を継続して実施するとともに、妨害原因の排除を迅速に実施する。また、重要無線通信への妨害を未然に防ぐための周知啓発を実施するほか、必要な電波監視施設の整備、電波監視技術に関する調査研究を実施する。
7-220オ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	総務省において、ネットワークIP化の進展に対応して、ICTサービスのより安定的な提供を図るため、電気通信に関する事故の発生状況等の分析・評価等を行い、その結果を公表する。また、事故再発防止のため、「情報通信ネットワーク安全・信頼性基準」等の見直しの必要性について検討する。
7-220カ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	情報共有体制その他の重要インフラ防護体制を実効性のあるものにするため、官民の枠を超えた関係者間での演習・訓練を次のとおり実施する。 ・内閣官房において、重要インフラ事業者等の障害対応能力の向上を図るため、重要インフラ分野や所管省庁等が横断的に参加する演習を実施する。 ・総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、重要インフラにおけるサイバー攻撃への対処能力を向上させるための実践的サイバー防御演習（CYDER）を実施する。 ・経済産業省において、重要インフラ等企業におけるサイバー攻撃に対する対応能力を向上させるため、模擬システムを活用した実践的なサイバー演習を実施する。 ・金融庁において、金融業界横断的なサイバーセキュリティ演習を引き続き実施する。
7-220カ2	↑	↑	↑	↑
7-220カ3	↑	↑	↑	↑
7-220カ4	↑	↑	↑	↑
7-220キ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	ー	経済産業省において、IPAに、2017年4月に「産業サイバーセキュリティセンター」を設立し、我が国の重要インフラ等におけるサイバーセキュリティ対策の中核を担う人材の育成に向けて、7月に教育カリキュラムを開始する。さらに、センターにおいて、重要インフラ等における実際の制御システム等の安全性・信頼性を検証する事業も実施し、対策強化に繋げる。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-213k	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA, MOC	Promoting "Guidelines Regarding the Protection of Personal Information in the Telecommunications Business".
7-213k2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Enhancing Measures against Cybercrimes	NPA	Enhancing capabilities to analyse IoTs.
7-220a	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	N/A Promoting 5 action plans (specified below) based on "The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)".
7-220b	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	Considering & preparing for legislation of security countermeasures for CIIs.
7-220b2	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	Monitoring & publishing improvement of security standards annually.
7-220c	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	Improving security standards for CIIs including risk assessment, functionality assurance, BCPs & internal audit.
7-220c2	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	Researching for development of information sharing platform for CIIs.
7-220d	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	MIC	Improving countermeasures against interference in critical wireless communication.
7-220e	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	MIC	Improving stability of telecommunication by analysing incidents in telecommunication.
7-220f	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	Cabinet Secretariat	Improving incident response ability of CII operators by performing cross-sectional exercises.
7-220f2	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	MIC, NICT	Performing practical cyber defence exercise "CYDER" for CIIs at "National Cyber Training Center".
7-220f3	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	METI	Performing practical cyber defence exercises with CII operators.
7-220f4	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	FSA	Performing cyber defence exercises in financial services sector.
7-220g	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	-	METI, IPA	Establishing "ICSCoE: Industrial Cyber Security Center of Excellence".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-221ア	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	重要インフラ防護の範囲等の不断の見直し	内閣官房において、重要インフラ所管省庁の協力の下、第4次行動計画に基づく施策を、中小事業者へ拡大すると共に、継続的に重要インフラに係る防護範囲の見直しに取り組む。
7-222ア	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	内閣官房において、重要インフラ所管省庁の協力の下、第4次行動計画に従い、情報共有体制の強化について次のとおり検討を進める。 ・ サービス障害の深刻度判断基準の導入に向けた検討を進める。 ・ 連絡形態の多様化（連絡元の匿名化、セプター事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除、及び分野横断的な情報を内閣官房に集約する仕組みの検討を進める。 ・ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）の検討を進める。
7-222イ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	経済産業省において、官民における最新の脅威情報やインシデント情報等の共有のため、IPAが情報ハブとなり実施している「サイバー情報共有イニシアティブ」（J-CSIP）について参加組織の拡大、共有情報の充実を行う。また、重要インフラ事業者等における信頼性・安全性向上の取組を支援するため、IPAを通じ、障害事例や提供情報の分析結果等を重要インフラ事業者等へ提供する。
7-222ウ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	経済産業省において、JPCERT/CCを通じ、重要インフラ事業者等からの依頼に応じ、国際的なCSIRT間連携の枠組みも利用しながら、攻撃元の国に対する調整等の情報セキュリティインシデントへの対応支援や、攻撃手法の解析の支援を行う。また、重要インフラ事業者等において対策が必要となる可能性のある脅威情報及びその対策に関する情報を、事前の合意に基づき、早期警戒情報として、JPCERT/CCから重要インフラ事業者等へ提供する。
7-222エ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	内閣官房において、情報セキュリティ関係機関等と協力関係を構築・強化していくと共に、引き続き、得られた情報を適切に重要インフラ事業者等に情報提供する。また、情報セキュリティ関係機関を情報共有体制のメインプレーヤの一つとして活用していくことについて、具体的な検討を行う。
7-222オ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	総務省において、NICTを通じ、標的型攻撃に関する情報の収集・分析能力の向上に向け、官公庁・大企業のLAN環境を模擬した実証環境を用いて標的型攻撃の解析を実施する。また、サイバー攻撃に関する情報を収集・分析・共有するための基盤となるプラットフォームの整備・構築に向けた検討を行う。
7-222カ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	警察庁において、サイバー攻撃を受けたコンピュータや不正プログラムの分析、関係省庁との情報共有等を通じて、サイバー攻撃事案の攻撃者や手口の実態解明を推進する。また、都道府県警察において、サイバー攻撃特別捜査隊を中心として、サイバー攻撃に関する情報の収集及び整理並びに犯罪の予防及び捜査を推進するとともに、重要インフラ事業者等の意向を尊重し、以下の取組を実施することにより、緊急対処能力の向上を図る。 ・ 重要インフラ事業者等への個別訪問を行い、各事業者等の特性に応じた情報提供や保有するシステムに対するぜい弱性試験を実施する。 ・ 事案発生を想定した共同対処訓練を実施する。 ・ サイバーテロ対策協議会を通じて、参加事業者間の情報共有を実施する。
7-222カ2	↑	↑	↑	↑
7-222カ3	↑	↑	↑	↑
7-222カ4	↑	↑	↑	↑
7-222キ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	効果的かつ迅速な情報共有の実現	経済産業省において、安全・安心なクレジットカードの利用環境の整備を目的とする「割賦販売法の一部を改正する法律（平成28年法律第99号）」の成立を受け、2018年6月までの円滑な施行に向けて、政省令等の整備を進める。また、クレジットカード取引に関係する事業者等で構成されているクレジット取引セキュリティ対策協議会において、2017年3月に改訂された「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画-2017-」に基づく関係事業者等の取組を更に推進するとともに、進捗状況等を踏まえて、必要な見直しを行う。
7-223ア	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	内閣官房及び総務省において、サイバーセキュリティ基本法等に基づいて、地方公共団体に対する情報の提供など、地方公共団体におけるサイバーセキュリティの確保のために必要とされる協力を行う。
7-223イ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	総務省において、関係機関と協力の上、地方公共団体職員が情報セキュリティ対策について習得することを支援するため、情報セキュリティ監査セミナー、情報セキュリティマネジメントセミナーを集合研修で、その他情報セキュリティ関連研修をeラーニングで実施する。また、マイナンバー制度における情報連携の状況等を踏まえつつ、地方公共団体における情報セキュリティポリシーに関するガイドラインの改定を実施する。
7-223イ2	↑	↑	↑	↑
7-223ウ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	総務省において、関係機関と協力の上、情報セキュリティ対策の取組事例の収集、情報セキュリティ事故情報の収集・分析の充実を図り、総合行政ネットワーク（LGWAN）内のポータルサイトに、情報セキュリティに関する解説等を提供するなど、その運営を支援し、更なる利用を促進する。
7-223エ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	総務省において、関係機関と協力の上、サーバやネットワーク機器等における脆弱性診断を地方公共団体自らが実施できるよう支援する。2016年度に作成・提供した訓練ツールを活用し、地方公共団体のインシデント即応体制の強化を図る。
7-223エ2	↑	↑	↑	↑

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-221a	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Conducting Constant Review on the Scope of CIIP	Cabinet Secretariat	Extending action plans based on "The Basic Policy of Critical Information Infrastructure Protection (4th Edition)" to SMEs (small-to medium-sized enterprises).
7-222a	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	Cabinet Secretariat	Enhancing information sharing mechanism for CIIs specifically; Considering introduction of severity grades for service failure. Diversifying communication method. Establishing information sharing platform.
7-222b	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	METI, IPA	Increasing participants & enhancing shared information of "J-CSIP: Cyber Intelligence Sharing Initiative".
7-222c	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	METI, JPCERT/CC	Assisting CII operators to respond cyber attacks from abroad.
7-222d	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	Cabinet Secretariat	N/A Intra-government cooperation.
7-222e	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	MIC, NICT	Enhancing analysis of targeted attacks by using proving environment simulating large scale LAN.
7-222f	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	NPA	Enhancing information gathering & analysis on cyber attacks & malwares.
7-222f2	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	Prefectural Police	Enhancing information gathering on cyber attacks.
7-222f3	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	Prefectural Police	Enhancing information sharing & cooperation with CII operators.
7-222f4	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	MPD	Enhancing information sharing with CII operators through "Cyber Terrorism Council".
7-222g	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Ensuring Effective and Prompt Information Sharing	METI	Enhancing security countermeasures of credit card settlement system.
7-223a	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, MIC	Supporting local public entities for their cybersecurity.
7-223b	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC	Supporting local public entities to educate & train their personnel for security by holding seminars & e-learning.
7-223b2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC	Supporting local public entities to revise security policies.
7-223c	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC	Providing local public entities with intelligence of security incidents & countermeasures through "LGWAN: Local Government Wide Area Network".
7-223d	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC	Providing local public entities with services of vulnerability scanning & malware detection.
7-223d2	Building a Safe and Secure Society for the People	Measures for the Protection of the People and Society	Promoting Security Measures Taken by Users of Cyberspace	MIC	Providing local public entities with tools for incident response exercises.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-223オ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	内閣官房及び総務省において、総合行政ネットワーク（LGWAN）に設けた集中的にセキュリティ監視を行う機能（LGWAN-SOC)などにより、GSOCとの情報連携を通じた、国・地方全体を俯瞰した監視・検知を行うとともに、地方公共団体のセキュリティ強化対策を推進するため、情報システムの強靭性の向上や自治体情報セキュリティクラウドの構築に係るフォローアップ及び、2017年度予算を活用し、地方公共団体の情報セキュリティ対策に係るLGWAN環境の健全性を補完する新たなプラットフォームの構築により、マイナンバー制度を含めたセキュリティ確保を徹底する。また、情報提供ネットワークシステム等のマイナンバー関係システムについて、インターネットから独立する等の高いセキュリティ対策が講じられたものとなるよう、管理・監督・支援等を行う。加えて、個人情報保護委員会において、関係省庁等と連携しつつ、特定個人情報の適正な取扱いに関するガイドラインの遵守、特定個人情報に係るセキュリティの確保を図るため、専門的・技術的知見を有する体制を拡充するとともに、監視・監督機能を強化し、情報提供ネットワークシステムに係る監視を適切に行う。
7-223オ2	↑	↑	↑	↑
7-223オ3	↑	↑	↑	↑
7-223オ4	↑	↑	↑	↑
7-223カ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	内閣府において、2017年7月に試行運用を開始し、2017年秋頃に本格運用を開始するマイナポータルを活用し、官民の認証連携をより一層推進していく。
7-223キ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	内閣官房において、我が国で使用される制御系機器・システムに関する脆弱性情報やサイバー攻撃情報などの有益な情報について、非制御系の情報共有体制と整合性のとれた情報共有体制により、収集・分析・展開していく。また、経済産業省において、IPAとJPCERT/CCと連携し、制御システムに係る脆弱性情報の提供収集・分析・展開にも取り組む。
7-223ク	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、セキュリティ対策に関する知見を収集し、それに基づいた実践的な演習を実施する。
7-223ケ	国民が安全で安心して暮らせる社会の実現	重要インフラを守るための取組	各分野の個別事情への支援	経済産業省において、制御機器のセキュリティ評価・認証の利用促進を図るとともに、制御システムのセキュリティに関する評価・認証制度の検討を行う。
7-230ア	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	ー	内閣官房において、新たに直面した脅威・課題への対応について、統一基準群を始めとした規程に適時反映するため、統一基準群の次期改定に向けた検討を進める。
7-231ア	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）により、政府機関情報システムのサイバー攻撃等に関する情報を24時間365日収集・分析し、政府機関等に対する新たなサイバー攻撃の傾向や情勢等について、分析結果を各政府機関等に対して適宜提供する。
7-231イ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、サイバー攻撃への対処に関する政府機関全体としての体制を強化するため、各府省庁のインシデント対処に関わる要員による情報共有及び連携の促進に資するコミュニティの更なる活性化を図る。
7-231ウ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、2016年度に改定した統一基準群に基づき、クラウドを利用する際の意識向上を図るとともに、政府機関等の情報システムの調達におけるセキュリティ・バイ・デザインを推進するため、情報システムの調達仕様書の策定段階において適切に定めるべきセキュリティ対策要件について検討を行い、各府省庁におけるセキュリティ・バイ・デザインの取組を促進する。また、各府省庁共通的に取り組むべき事項については、規程への反映に向けた検討を行う。
7-231ウ2	↑	↑	↑	↑

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-223e	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, Cabinet Office, MIC, GSOC	Establishing integrated cybersecurity network monitoring for government & local public entities.
7-223e2	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, MIC	Supporting local public entities to enhance cybersecurity of their ICTs & to establish cloud network with FY2017 budget.
7-223e3	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, MIC	Urging local public entities to isolate "My Number" (Japanese version of Social Security Number) related systems/networks from internet.
7-223e4	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, MIC, PPC	Urging local public entities to comply with "Guidelines for Proper Handling of Specific Personal Information".
7-223f	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Office	Promoting collaboration of public & private sectors on authentication using "My Number Portal".
7-223g	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	Cabinet Secretariat, METI, IPA, JPCERT/CC	Incorporating vulnerability information for control systems into existing operation of reporting & dissemination system for vulnerability information.
7-223h	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	METI	Performing practical exercises for control systems of CIIs.
7-223i	Building a Safe and Secure Society for the People	Measures for Critical Information Infrastructure Protection	Offering Tailored Support to CII Sectors	METI	Promoting security assessment & certification for control systems.
7-230a	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	-	Cabinet Secretariat	Preparing for next revision of "Common Standards Group for Information Security Measures for Government Agencies and Related Agencies".
7-231a	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat, GSOC	Monitoring & analysing ICT networks of government agencies @24/7.
7-231b	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Strengthening incident response capabilities of government agencies by enhancing cooperation between CSIRT of public organisations.
7-231c	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Urging government agencies to adopt 'security by design' in procurement.
7-231c2	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Urging government agencies to consider security upon utilisation of cloud network.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-231エ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	経済産業省において、政府調達等におけるセキュリティの確保に資するため、IPAを通じ、「IT製品の調達におけるセキュリティ要件リスト」の記載内容（製品分野、製品に対する脅威、脅威に対する要件としてのプロテクション・プロファイルなど）の見直しを行うとともに、政府機関の調達担当者等に対し、最新のプロテクション・プロファイル（翻訳版）を含む情報の提供や普及啓発を行う。
7-231エ2	↑	↑	↑	↑
7-231オ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	経済産業省において、IPAを通じ、JISEC（ITセキュリティ評価及び認証制度）の利用者の視点に立った評価・認証手続の改善、積極的な広報活動等を実施するとともに、政府調達を推進するため、調達関係者に対する勉強会やヒアリングを実施するとともに必要に応じて手順等の見直しを実施する。
7-231カ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	経済産業省において、安全性の高い暗号モジュールの政府機関における利用を推進するためIPAの運用する暗号モジュール試験及び認証制度（JCMVP）の普及を図る。
7-231キ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、各府省庁の情報システムにおけるセキュリティ対策の点検・改善を行うため、実際の攻撃手法を用いて情報システム内部への侵入及び侵入後の被害状況について検証を行うペネトレーションテストを行い、その結果を踏まえて、問題点の改善に向けた助言等を行う。
7-231ク	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、巧妙化する情報セキュリティに関する脅威、動向等を踏まえ、各府省庁の情報システムにおける対策の実施状況の点検・改善を行うため、公開された脆弱性等への対応やサイバー攻撃に係る対策の実施状況の調査を行う。調査結果は、マネジメント監査により確認された課題等も踏まえ、統一基準群を始めとした規程への反映や改善に向けた取組について検討を行う。
7-231ケ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、2020年東京オリンピック・パラリンピック競技大会及びその後を見据えて、インシデント発生前及び発生時の情報提供の迅速化・高度化に資するGSOCシステムの検知・解析機能を始めとした機能強化、GSOCセンサーの増強等の検討を行うとともに、将来のGSOCシステムにおける監視の在り方を検討する。
7-231コ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能の強化を図るため、情報システムにおけるログの取得や活用の在り方について、サイバー攻撃を受けた際の影響範囲の特定、原因究明等の観点から更なる検討を行う。
7-231サ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、各府省庁におけるサイバー攻撃に係る事態の把握・対処機能が強化されるよう、CSIRT体制の強化やインシデント対処の改善に関する各府省庁の取組状況及び課題を把握し、府省庁CSIRTの対処能力の更なる強化のために必要な施策を検討する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-231d	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	METI, IPA	Reviewing "List of Requirements for Ensuring Security in Procurement of IT Products".
7-231d2	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	METI, IPA	Disseminating information including PP (protection profiles) to procurement professionals of government agencies.
7-231e	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	METI, IPA	Reviewing & promoting "JISEC: Japan Information Technology Security and Certification Scheme".
7-231f	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	METI, IPA	Promoting "JCMVP: Japan Cryptographic Module Validation Program".
7-231g	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Performing penetration testing to ICT systems of government agencies.
7-231h	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Performing vulnerability scanning & examining cybersecurity measures of government agencies.
7-231i	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat, GSOC	Speeding up detecting & informing incidents to government agencies by enhancing GSOC censors/systems. Considering next generation system of GSOC.
7-231j	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Reviewing policies for obtaining & storing ICT systems logs to enhance incident response capabilities.
7-231k	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Examining CSIRT of government agencies & urging them to enhance incident response capabilities.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-231シ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	政府機関におけるサイバー攻撃に係る対処要員の能力及び連携の強化を図るため、以下の訓練・演習を実施する。 ・内閣官房において、各府省庁における情報セキュリティインシデント対処に関わる要員を対象として、最高情報セキュリティ責任者及びサイバーセキュリティ・情報化審議官等をはじめとした幹部による指揮の下での組織的かつ適切な対処の実現を目指し、これまでの訓練や調査等により明らかになった課題や近年のサイバー攻撃動向等を踏まえた訓練を実施する。また、府省庁、独立行政法人及び指定法人における情報セキュリティインシデント対処に関わる要員を対象として、研修を年間を通じて実施する。さらに、政府機関等において自組織の環境に最適化した訓練を独自に実施できるようにするために必要な支援の実施を検討する。 ・内閣官房において、サイバー攻撃等により発生した支援対象機関等の情報システム障害又はその発生が予想される場合等、政府一体となった対応が必要となる情報セキュリティインシデントに対応できる人材を養成・維持するため、情報セキュリティ緊急支援チーム（CYMAT）要員等に対する訓練等を実施する。 ・総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、政府機関におけるサイバー攻撃への対処能力の向上に向け、新たなシナリオによる実践的なサイバー防御演習（CYDER）を実施する。 ・内閣官房及び総務省において、政府機関のインシデント対処能力の向上のため、府省間の競技形式による演習（NATIONAL 318(CYBER) EKIDEN）を実施する。
7-231シ2	↑	↑	↑	↑
7-231シ3	↑	↑	↑	↑
7-231シ4	↑	↑	↑	↑
7-231ス	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	文部科学省において、国立情報学研究所（NII）を通じ、国立大学法人及び大学共同利用機関法人（以下「国立大学法人等」という）のインシデント対応体制を高度化するために、国立大学法人等へのサイバー攻撃の情報提供と情報セキュリティ担当者の研修を実施する。
7-231ス2	↑	↑	↑	↑
7-231セ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、政府職員のインシデント対処能力等を向上させていくため、サイバー攻撃対処能力を競うNATIONAL 318(CYBER) EKIDENを、さらに発展させていくべく取り組む。
7-231ソ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、サイバーセキュリティ基本法に基づく重大インシデント等に係る原因究明調査をより適切に実施するため、デジタルフォレンジック調査に当たる職員の技術力の向上に引き続き取り組むとともに、民間事業者の知見を活用するための方策を講じる。
7-231タ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	攻撃を前提とした情報システムの防御力の強化・多層的な対策の推進	内閣官房において、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の運用等を通じて標的型攻撃に対する多重防御の取組を引き続き推進する。
7-232ア	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	しなやかな組織的対応能力の強化	内閣官房において、政府機関における統一基準群等に基づく施策の取組状況について、セキュリティ対策を強化するための体制等が有効に機能しているかとの観点を中心とした検証を通じて、自律的なセキュリティ水準の向上を促す仕組みを確立するため、国の行政機関に対して監査を実施する。監査の実施に当たっては、2年間で全府省庁に対して監査を実施する計画とし、国の行政機関のサイバーセキュリティ対策及びその維持改善の体制の整備及び運用状況に係る現状を把握し、改善のために必要な助言等を行う。2017年度の監査については、前回までの監査の結果を踏まえるとともに前回対象としなかった部局・システムを対象とした内容とした監査テーマで実施する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-231l	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Performing cybersecurity exercises for incident response personnel of government agencies.
7-231l2	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat, CYMAT	Performing cybersecurity exercises for CYMAT members.
7-231l3	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	MIC, NICT	Performing practical cyber defence exercise "CYDER" for government agencies with "National Cyber Training Center".
7-231l4	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat, MIC	Performing "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).
7-231m	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	MEXT, NII	Sharing cybersecurity intelligence with national universities.
7-231m2	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	MEXT, NII	Supporting national universities to enhance cybersecurity by training security personnel.
7-231n	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Considering to enhance "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).
7-231o	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Training digital forensics professionals.
7-231p	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks	Cabinet Secretariat	Promoting "Guidelines for Risk Assessment of Advanced Cyber Attacks Measurements".
7-232a	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Achieving More Resilient Organizational Response Capabilities	Cabinet Secretariat	Performing audit of all government agencies & related agencies during 2 years based on "Common Standards Group for Information Security Measures for Government Agencies and Related Agencies".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-232イ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	しなやかな組織的対応能力の強化	内閣官房及び各府省庁において、最高情報セキュリティ責任者及びサイバーセキュリティ・情報化審議官等をはじめとした幹部による指揮の下で、「サイバーセキュリティ人材育成総合強化方針」に基づき策定した「各府省庁セキュリティ・IT人材確保・育成計画」の推進を始めとし、体制の整備、有意な人材の確保、一定の専門性を有する人材の育成、適切な処遇の確保を含む政府内部のセキュリティ人材の充実に係る諸施策を推進する。
7-232ウ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	しなやかな組織的対応能力の強化	内閣官房において、サイバーセキュリティ・情報化審議官等の研修等を通じて政府機関内における相互の事例共有、意見交換等の継続的な実施を促進する。
7-232エ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	しなやかな組織的対応能力の強化	内閣官房において、引き続き、府省庁、独立行政法人及び指定法人を対象に、昨今のサイバーセキュリティの動向や課題等に応じたテーマによる勉強会等を開催する。また、人事院と協力し、政府職員の採用時の合同研修にサイバーセキュリティに関する事項を盛り込むことによる教育機会の付与に取り組む。
7-232オ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	しなやかな組織的対応能力の強化	内閣官房及び総務省において、各府省庁のセキュリティ・IT人材の育成・確保のため、現行の研修体系の抜本的整理を進めるとともに、研修修了者にスキル認定を行う枠組みを構築し、研修修了者等に対するスキル認定の実施に向けて取り組む。
7-233ア	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	技術の進歩や業務遂行形態の変化への対応	内閣官房において、各府省庁におけるクラウドサービス等の利用や対策の状況について調査するとともに、各府省庁と共有し、統一的な対策の必要性が把握された場合は統一基準群等への反映に向けた検討を行う。
7-233イ	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	技術の進歩や業務遂行形態の変化への対応	内閣官房において、ITを活用した政府機関全体としての行政事務について、関係機関と連携し、サイバーセキュリティの確保が前提となった遂行形態の実現を図る。
7-234ア	国民が安全で安心して暮らせる社会の実現	政府機関を守るための取組	監視対象の拡大等による総合的な対策強化	内閣官房において、IPAとの連携等により、引き続き、日本年金機構を含む独立行政法人・指定法人に対して監査を行う。監査の実施に当たっては、2020年東京オリンピック・パラリンピック競技大会までに、全ての法人に対し監査を行う計画とする。また、IPAの実施する、独立行政法人・指定法人に係る監視業務の監督を行うとともに、監視に係る能力や機能の向上の観点から、攻撃情報の共有等の連携を図る。
7-310ア	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	ー	内閣官房において、国民の生命等に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態（大規模サイバー攻撃事態等）発生時における政府の初動対処態勢の整備及び対処要員の能力の強化を図るため、関係府省庁、重要インフラ事業者等と連携した初動対処訓練を実施する。
7-310イ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	ー	防衛省において、高度なサイバー攻撃からの防護を目的として、国内外におけるサイバー攻撃関連情報を収集・分析する体制を強化するとともに、必要な機材の拡充を実施する。
7-311ア	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	内閣官房において、「カウンターインテリジェンス機能の強化に関する基本方針」に基づき、各府省庁と協力し、サイバー空間におけるカウンターインテリジェンスに関する情報の集約・分析を行い各府省との共有化を図る。また、政府機関が保有する機密情報が保護されるよう適切な措置を実施する。
7-311イ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	警察庁及び法務省において、サイバーインテリジェンス対策に資する取組を実施する。
7-311ウ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	警察庁において、大規模産業型制御システムに対するサイバー攻撃及び当該システムの脆弱性の調査等を目的とした不正なアクセスが国内外で多数確認されている背景を踏まえ、こうした攻撃の未然防止活動、有事の緊急対処に係る能力向上に資する訓練、サイバー空間に関する観測機能の強化等に取り組むことで、サイバーフォースセンターの技術力の向上等を図る。また、大規模産業型制御システムに対するサイバー攻撃対策に係る訓練を実施する。さらに、サイバー攻撃の実態解明に必要不可欠な不正プログラム等の解析を推進する。
7-311ウ2	↑	↑	↑	↑
7-311ウ3	↑	↑	↑	↑
7-311エ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	警察庁において、警察部内の高度な専門性を有する人材等の確保・育成を図る方策を検討する。
7-311オ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	防衛省において、対処機関としてのサイバー攻撃対処能力向上のため、サイバー防護分析装置、サイバー情報収集装置、各自衛隊の防護システムの機能の拡充を図るとともに、多様な事態において指揮命令の迅速かつ確実な伝達を確保するため、防衛情報通信基盤（DII）のクローズ系及びネットワーク監視器材へ常続監視等を強化するための最新技術を適用していく。
7-311オ2	↑	↑	↑	↑

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-232b	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Achieving More Resilient Organizational Response Capabilities	Cabinet Secretariat, Government Agencies	Training cybersecurity personnel & experts based on "General Policy for Cybersecurity Human Resources Development". Each government agency establishes own plan for build security & IT human resources.
7-232c	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Achieving More Resilient Organizational Response Capabilities	Cabinet Secretariat	Continuing information sharing in cybersecurity community across government.
7-232d	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Achieving More Resilient Organizational Response Capabilities	Cabinet Secretariat	Supporting government agencies to develop cybersecurity human resources by training non-security personnel & providing with educational materials.
7-232e	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Achieving More Resilient Organizational Response Capabilities	Cabinet Secretariat, MIC	Reviewing & reconstructing education & training systems for IT human resources.
7-233a	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Adapting to Technological Advancement and Change in Business Performance Styles	Cabinet Secretariat	Researching & developing security measures for cloud services, standardising if necessary.
7-233b	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Adapting to Technological Advancement and Change in Business Performance Styles	Cabinet Secretariat	Promoting 'security-by-design' in obtainment of new ICT systems for administrative operation.
7-234a	Building a Safe and Secure Society for the People	Measures for the Protection of Governmental Bodies	Comprehensively Enhancing Measures through the Extended Scope of Monitoring and Others	Cabinet Secretariat, IPA	Performing audit of related agencies (besides government agencies) on cybersecurity.
7-310a	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	-	Cabinet Secretariat	Performing initial response exercises in preparation for potential large-scale cyber attack.
7-310b	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	-	MOD	Enhancing resources for collection & analysis of cyber attack intelligence from homeland & abroad.
7-311a	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	Cabinet Secretariat	Enhancing counter-intelligence capabilities.
7-311b	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	NPA, MOJ	N/A Not referring to specific action plans.
7-311c	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	NPA	Enhancing capability of Cyber Force Center by performing exercises & upgrading monitoring equipment.
7-311c2	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	NPA	Performing cybersecurity exercises for large-scale industrial control systems.
7-311c3	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	NPA	Enhancing analytic capabilities of malwares.
7-311d	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	NPA	Considering education & training of highly professional human resources.
7-311e	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD	Enhancing protection & analysis equipment & cyber intelligence collection equipment.
7-311e2	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD	Enhancing security of "DII: Defense Information Infrastructure".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-311カ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。
7-311キ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。
7-311ク	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	防衛省・自衛隊が保有する情報通信ネットワーク等に対する侵入試験（ペネトレーションテスト）について、次年度の実施に向けた所要の準備を進める。
7-311ケ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	対処機関の能力強化	防衛省において、サイバー攻撃等によって防衛省・自衛隊の情報通信基盤の一部が損なわれた場合においても、運用継続を実現する研究を実施する。
7-312ア	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	我が国の先進技術の活用・防護	防衛省において、サイバーセキュリティの更なる確保のため、調達する情報システムに係る情報セキュリティ上のサプライチェーンリスク対策として、調達仕様書に係る関連規則の整備を行うとともに、引き続き調査研究等を通じて必要な関連規則等の整備を進める。
7-312イ	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	我が国の先進技術の活用・防護	科学技術競争力や安全保障等に係る技術情報を保護する観点から、以下の取組を行う。 ・ 内閣官房において、先端的な技術を保有する国立研究開発法人について、当該法人のマネジメント・技術面の取組を促進するとともに、これら法人相互の協力による自立的活動の向上に向けた取組を促す。また、情報セキュリティ対策を支える制度面に係る支援を本格化させる。 ・ 文部科学省において、先端的な技術情報を保有する大学等に対して、サイバー攻撃による当該情報の漏えいを防止するための取組を促すとともに、支援する。
7-312イ2	↑	↑	↑	↑
7-313ア	国際社会の平和・安定及び我が国の安全保障	我が国の安全の確保	政府機関・社会システムの防護	防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための具体的・実効的連携要領の確立等に向けた取組を実施する。また、任務保証の観点から、任務遂行上依拠する社会インフラへのサイバー攻撃の影響に関する知見を向上し、関係主体との連携を深化させていく。
7-320ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	ー	経済産業省において、JPCERT/CCを通じて、主にアジア太平洋地域等を対象としたインターネット定点観測システム（TSUBAME）に関し、運用主体のJPCERT/CCと各参加国関係機関等との間での共同解析やマルウェア解析連携との連動等の取組を進める。また、アジア太平洋地域以外への観測点の拡大を進める。
7-321ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間における国際的な法の支配の確立	内閣官房、警察庁、総務省、外務省、経済産業省及び防衛省において、各二国間協議や国連政府専門家会合、APEC、OECD会合等の多国間協議に参画し、我が国の意見表明や情報発信に努め、サイバー空間における国際法の適用や国際的なルール・規範作り等に積極的に関与し、それらに我が国の意向を反映させる。
7-321イ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間における国際的な法の支配の確立	警察庁及び法務省において、容易に国境を越えるサイバー犯罪に効果的に対処するため、原則として共助を義務的なものとする日・米、日・韓、日・中、日・香港、日・EU、日・露間の刑事共助条約・協定及びサイバー犯罪に関する条約の発効を受け、これらの条約・協定の下で、中央当局を設置し、外交ルートを経由せずに直接中央当局間で共助実施のための連絡を行うことで共助の迅速化を図る。今後は、更なる刑事共助条約の締結について検討していく。
7-321ウ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間における国際的な法の支配の確立	警察庁において、迅速かつ効果的な捜査共助等の法執行機関間における国際連携の強化を目的とし、我が国のサイバー犯罪情勢に関係の深い国々の各法執行機関と効果的な情報交換を実施するとともに、G7/G8、ICPO等のサイバー犯罪対策に係る国際的な枠組みへの積極的な参加、アジア大洋州地域サイバー犯罪捜査技術会議の主催等を通じた多国間における協力関係の構築を推進する。また、外国法執行機関等に派遣した職員を通じ、当該機関等との連携強化を推進する。さらに、証拠の収集等のため外国法執行機関からの協力を得る必要がある場合について、外国の法執行機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。
7-321ウ2	↑	↑	↑	↑
7-321ウ3	↑	↑	↑	↑
7-321エ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間における国際的な法の支配の確立	外務省において、我が国が2012年7月にサイバー犯罪に関する条約を締結し、同年11月から我が国について同条約の効力が生じたことを受け、引き続きアジア地域初の締約国として同条約の普及等に積極的に参画する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-311f	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD	Performing practical exercises on environment simulating defence information systems.
7-311g	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD	Training CSIRT members for response against highly advanced attacks.
7-311h	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD, JSDF	Preparing for penetration testing of defence information network.
7-311i	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Enhancing Response Capabilities of Relevant Governmental Bodies	MOD	Researching contingency operation of defence information infrastructures.
7-312a	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Utilizing and Protecting Japan's Advanced Technology	MOD	Implementing cybersecurity measures of supply chains of defence equipment.
7-312b	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Utilizing and Protecting Japan's Advanced Technology	Cabinet Secretariat	Backing-up National Research and Development Agencies with leading technologies especially in information security area.
7-312b2	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Utilizing and Protecting Japan's Advanced Technology	MEXT	Supporting universities with leading technologies to enhance countermeasures against information exfiltration by cyber attacks.
7-313a	Ensuring Peace and Stability of the International Community and National Security	Ensuring National Security	Protecting Governmental Bodies and Social Systems	MOD	Enhancing cooperation between MOD & defence industry.
7-320a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	-	METI, JPCERT/CC	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point observation system). Extending observation points to other regions.
7-321a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	Cabinet Secretariat, NPA, MIC, MOFA, METI, MOD	Positively contributing to international debate of international laws, rules & codes for cyberspace.
7-321b	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	NPA, MOJ	Speeding up international assistance in investigation of cybercrimes under treaty for mutual legal assistance. Considering further conclusion of treaty.
7-321c	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	NPA	Exchanging information with law enforcement of those countries who are related to Japanese cybercrime circumstances.
7-321c2	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	NPA	Positively contributing to international framework for cooperation of anti-cybercrime.
7-321c3	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	NPA	Enhancing relationship with neighbouring countries by holding Asian Pacific Regional Cyber Crime Investigation Technical Conferences.
7-321d	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Establishing the International Rule of Law in Cyberspace	MOFA	Positively contributing to promotion of "Budapest Convention on Cybercrime" (the first international treaty seeking to address Internet and computer crime by harmonizing national laws), improving investigative techniques, & increasing cooperation among nations.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-322ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	国際的な信頼醸成措置	内閣官房、外務省及び関係府省庁において、サイバー攻撃を発端とした不測事態の発生を未然に防止するため、国連の場を活用したルール作りに携わるとともに、二国間協議等を通じて、脅威認識やサイバーセキュリティ戦略等の政策について共有し、国際的な連絡体制等を平素から構築する。これらの取組に当たっては、関係府省庁が共同して対外的な情報発信を強化すると共に、把握したサイバーセキュリティに関する情報を国内の関係機関と共有する。
7-322ア2	↑	↑	↑	↑
7-322イ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	国際的な信頼醸成措置	内閣官房及び関係府省庁において、各二国間協議やIWWN等のサイバー空間に関する多国間の国際会議等に参画し、それぞれの取組においてインシデント対応演習や机上演習等を通じて、各国との情報共有や国際連携、信頼醸成を推進し、インシデント発生時の国外との情報連絡体制を整備する。
7-322ウ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	国際的な信頼醸成措置	経済産業省において、JPCERT/CCを通じて、インシデント対応調整や脅威情報の共有に係るCSIRT間連携の窓口を運営するとともに、各国の窓口チームとの間のMOU/NDAに基づく継続的な連携関係の維持を図り、迅速かつ効果的なインシデントへの対処を継続する。また、JPCERT/CCのFIRST、IWWNやAPCERTにおける活動、及びアジア太平洋地域におけるインシデント対応演習等の活動等を通じた各国CSIRTとJPCERT/CCとのインシデント対応に関する連携を行う。
7-323ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間を悪用した国際テロ組織の活動への対策	内閣官房において、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析の強化等により、全体として、テロの未然防止に向けた多角的かつ隙の無い情報収集・分析を推進するとともに、関連情報の内閣情報官の下での集約・共有を強化する。
7-323イ	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー空間を悪用した国際テロ組織の活動への対策	警察庁及び法務省において、サイバー空間における国際テロ組織等の動向把握及びサイバー攻撃への対策を強化するため、サイバー空間における攻撃の予兆等の早期把握を可能とする態勢を拡充し、人的情報収集やオープンソースの情報を幅広く収集する等により、攻撃主体・方法等に関する情報収集・分析を強化する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-322a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Building International Confidence Measures	Cabinet Secretariat, MOFA	Contributing to UN effort to establish international rules to prevent contingencies from arising out of cyber attacks.
7-322a2	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Building International Confidence Measures	Cabinet Secretariat, MOFA	Sharing information about cyber threat & cybersecurity strategies through bilateral meetings.
7-322b	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Building International Confidence Measures	Cabinet Secretariat	Enhancing international relationship & cooperation through participating international conferences like "IWWN: International Watch and Warning Network" (established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities).
7-322c	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Building International Confidence Measures	METI, JPCERT/CC	Continuing & enhancing international coordination & cooperation in incident responses,
7-323a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Tackling Activities of International Terrorist Organizations Maliciously Using Cyberspace	Cabinet Secretariat	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace under direction of Director of Cabinet Intelligence.
7-323b	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Tackling Activities of International Terrorist Organizations Maliciously Using Cyberspace	NPA, MOJ	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-324ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	サイバー分野における能力構築（キャパシティビルディング）への協力	内閣官房、警察庁、総務省、外務省、経済産業省、その他関係府省庁・機関が相互に連携、情報共有を行い、ASEAN加盟国をはじめとする各国における能力構築支援に積極的に取り組む。取組に際しては、内閣官房を中心に、「サイバーセキュリティ分野における開発途上国に対する能力構築支援（基本方針）」（2016年10月）を踏まえ、政府及び関係機関が一体となって対応していく。 ・ 内閣官房において、日・ASEAN情報セキュリティ政策会議を通じた人材育成の取組やASEAN加盟国と連携したサイバーセキュリティに関する国際キャンペーンの取組を通じて、ASEAN加盟国の能力構築に貢献する。 ・ 警察庁において、アジア大洋州地域サイバー犯罪捜査技術会議やJICA課題別研修（サイバー犯罪対処能力向上）の開催等を通じ、アジア大洋州地域をはじめとする各国における能力構築に貢献する。 ・ 総務省において、APEC電気通信・情報産業大臣会合を通じて、情報通信分野に関してAPEC域内各国・地域との間でのネットワークセキュリティ分野における意識啓発等の連携を推進する。また、APT（アジア・太平洋電気通信共同体）における取組やITU-D等の取組を通じて、研修やセミナーを開催することにより、諸外国に対する意識啓発に取り組む。 ・ 外務省において、警察庁等とも協力しつつ、第2回日・ASEANサイバー犯罪対策対話やUNODCプロジェクトへの拠出を通じて、ASEAN加盟国のサイバー犯罪対策能力構築支援を行う。その他国際機関などと連携したプロジェクトについても検討する。 ・ 経済産業省において、ASEAN加盟国に対し、ISMS、CSMSに関する研修・セミナー等を通じて、我が国のセキュリティマネジメントに関するノウハウを共有することで、ASEAN加盟国への能力構築支援へ貢献する。 ・ 経済産業省において、JPCERT/CCを通じ、アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担うCSIRTの構築及び運用、連携の支援を行う。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習実施を行う。また、アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施等の活動等を行う。さらに、我が国企業が組込みソフトウェア等の開発をアウトソーシングしている先のアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。
7-324ア2	↑	↑	↑	↑
7-324ア3	↑	↑	↑	↑
7-324ア4	↑	↑	↑	↑
7-324ア5	↑	↑	↑	↑
7-324ア6	↑	↑	↑	↑
7-324ア7	↑	↑	↑	↑
7-325ア	国際社会の平和・安定及び我が国の安全保障	国際社会の平和・安定	国際的な人材育成	内閣官房及び関係府省庁において、各国機関との連携、国際会議への参加や留学の支援、我が国での国際会議の開催、現在国内で開催されている競技イベントを国際レベルで行うこと等を通じ、我が国の情報セキュリティ人材が海外の優秀な技術者等と切磋琢磨しながら研鑽を積む場を増やす。
7-330ア	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	－	内閣官房、外務省及び関係府省庁において、ハイレベルの会談・協議等を通じ、サイバー空間における我が国の利益が達成されるよう、戦略的な取組を進める。
7-330イ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	－	内閣官房及び外務省において、サイバー空間の安全及び安定を促進するため、「G7伊勢志摩サイバーグループ」を含め、G7各国との政策協調及び実務的な協力の強化に向け、G7各国と連携のうえ我が国も引き続きイニシアチブを発揮していく。
7-330ウ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	－	内閣官房、総務省、外務省、経済産業省及び関係府省庁において、これまで二国間対話等を実施してきた各国との枠組を継続するとともに、合意された連携を推進する。また、更なる連携の対象を検討し、必要があれば新たな二国間対話等の立ち上げを図り、国際協力体制を確立する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-324a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	Cabinet Secretariat	Government agencies positively support other nations based on "Basic Policy for Assistance of Cybersecurity Capacity Building in Developing Counties". Supporting ASEAN countries to build cybersecurity capabilities through "ASEAN-Japan Information Security Policy Meeting".
7-324a2	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	NPA	Supporting countries in Asian Pacific region to build cybersecurity capabilities through "Asian Pacific Regional Cyber Crime Investigation Technical Conferences" & JICA's technical training programs.
7-324a3	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	MIC	Contributing to regional cybersecurity awareness raising through "APT: Asia-Pacific Telecommunity", "ITU-D: ITU Telecommunication Development Sector" & "Ministerial Meeting on Telecommunications and Information Industry of APEC: Asia Pacific Economic Cooperation".
7-324a4	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	MOFA	Supporting ASEAN countries to build cybersecurity capabilities through "Asian Pacific Regional Cyber Crime Investigation Technical Conferences" & "UNODC: United Nations Office on Drugs and Crime".
7-324a5	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	METI	Supporting ASEAN countries to build cybersecurity capabilities by holding seminars of ISMS & CSMS.
7-324a6	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	METI, JPCERT/CC	Supporting countries in Asian Pacific & Africa to build & operate national CSIRTs.
7-324a7	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Cooperating for Cybersecurity Capacity Building	METI, JPCERT/CC	Holding seminars for 'secure development' for foreign software suppliers.
7-325a	Ensuring Peace and Stability of the International Community and National Security	Maintaining Peace and Stability of the International Community	Developing World-Class Human Resources	Cabinet Secretariat	Encouraging personnel of government agencies & related agencies to attend international conferences, international CTFs & foreign schools.
7-330a	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Cabinet Secretariat, MOFA	N/A Not a specific action.
7-330b	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Cabinet Secretariat, MOFA	Enhancing coordination & cooperation of G7 through "Ise-Shima Cyber Group".
7-330c	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Cabinet Secretariat, MIC, MOFA, METI	Continuing & extending international cooperation through bilateral meetings.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-330エ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	内閣官房及び外務省において、外国関係機関との情報交換等を緊密に行い、主要国のサイバー攻撃対処や国家の関与が疑われるようなサイバー攻撃の動向等の情報収集・分析に努める。
7-330オ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	内閣官房及び関係府省庁において、「サイバーセキュリティ国際キャンペーン」を実施し、サイバーセキュリティに関する国際的なイベントの開催や各国と連携した意識啓発活動を行うことで、幅広い範囲での国際協力体制を確立し、サイバー空間の安全を確保していく。
7-330カ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	警察庁及び法務省において、サイバー攻撃対策を推進するため、諸外国関係機関との情報交換等国際的な連携を通じて、サイバー攻撃に関する情報収集・分析を継続的に実施する。
7-330キ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	経済産業省において、攻撃者が悪用する、グローバルに広がっている脅威や攻撃基盤等の問題に、各国のCSIRTが連携して対応・対策を実施するために必要となる、サイバーセキュリティに関する比較可能で堅牢な定量評価の仕組み（サイバーグリーン）の検討や、効率的な対処のためのオペレーション連携を実現するための基盤構築に資する開発、運用協力体制の検討を進める。
7-330ク	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	経済産業省において、国際協力体制を確立するという観点から、米NIST等の各国の情報セキュリティ機関との連携を通じて、情報セキュリティに関する最新情報の交換や技術共有等に取組む。
7-330ケ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	経済産業省において、JPCERT/CCを通じ、アジア太平洋地域、アフリカ等において、各国における対外・対内調整を担うCSIRTの構築及び運用、連携の支援を行う。JPCERT/CCの経験の蓄積をもとに開発されたサイバー攻撃に対処するための演習ツールの提供や演習実施等を行う。また、アジア太平洋地域等我が国企業の事業活動に関係の深い国や地域を念頭に、組織内CSIRT構築セミナー等の普及・啓発、サイバー演習の実施等の活動等を行う。さらに、我が国企業が組込みソフトウェア等の開発をアウトソーシングしている先のアジア地域の各国を中心に、脆弱性を作りこまないコーディング手法に関する技術セミナーを実施する。
7-330コ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	―	防衛省において、国家の関与が疑われるような高度なサイバー攻撃に対処するため、防衛省・自衛隊のサイバーセキュリティに係る諸外国との技術面・運用面の協力に関する企画・立案機能を強化する。
7-331ア	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	アジア大洋州	内閣官房、総務省、外務省及び経済産業省において、日ASEAN情報セキュリティ政策会議、二国間協議等の枠組みを通じ、アジア大洋州各国とのサイバー分野における連携を強化する。また、ワークショップの開催等を通じて、我が国とASEAN加盟国のネットワークオペレータによって培われた知見や経験の相互共有を促進する。さらに、ARFを中心とした地域の枠組みによる信頼醸成を進める。
7-331ア2	↑	↑	↑	
7-331イ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	アジア大洋州	警察庁、法務省及び外務省において、国境を越えるサイバー犯罪の脅威に対抗するため、特にアジア太平洋地域諸国におけるサイバー犯罪対策に関する刑事司法制度の整備が進むよう、二国間又は多国間の枠組みを活用した技術援助活動を積極的に推進する。
7-331ウ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	アジア大洋州	防衛省及び関係府省庁において、東南アジア各国との間で、防衛当局間のITフォーラム等の取組を通じ、サイバー分野での連携やこれらの国に対する能力構築への協力、情報の収集や発信を推進していく。また、防衛省において、オーストラリアとのサイバー防衛協力を推進していく。
7-332ア	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	北米	内閣官房、外務省及び関係府省庁において、日米サイバー対話等の枠組みを通じ、幅広い分野における日米協力について議論し、両国間の政策面での協調や体制及び能力の強化、インシデント情報の交換等を推進し、同盟国である米国とのサイバー空間に関する幅広い連携を強化する。
7-332ア2	↑	↑	↑	
7-332イ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	北米	総務省、外務省及び関係府省庁において、米国とのインターネットエコノミーに関する日米政策協力対話にて一致した、産業界及び他の関係者と共同してサイバーセキュリティ上の課題に取り組むことが不可欠であるとの認識に基づき、引き続き米国との情報共有を強化する。また、関連して、総務省において、日米の通信分野のISAC間の連携を推進する。
7-332イ2	↑	↑	↑	
7-332ウ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	北米	防衛省において、日米サイバー防衛政策ワーキンググループ（CDPWG）の開催等を通じて、情報共有、訓練・人材育成等の様々な協力分野において日米サイバー防衛の連携を深めていく。また、新たな日米防衛協力のための指針で示された方向性に基づき、自衛隊と米軍との間における運用面のサイバー防衛協力を深化させていく。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-330d	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Cabinet Secretariat, MOFA	Enhancing intelligence sharing with foreign governments.
7-330e	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Cabinet Secretariat	Contributing to international effort to raise cybersecurity awareness.
7-330f	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	NPA, MOJ	Enhancing intelligence sharing with foreign law enforcement & legal communities.
7-330g	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	METI	Researching technologies for measuring cyber health of countries/regions ("Cyber Green Project").
7-330h	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	METI	Enhancing information sharing with foreign agencies for information security like NIST.
7-330i	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	Same as 7-324a, 7-324b	Same as 7-324a, 7-324b
7-330j	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	-	MOD	Considering possible cooperation in cyberspace between MOD/JSDF & foreign forces.
7-331a	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Asia Pacific	Same as 7-324c	Same as 7-324c
7-331a2	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Asia Pacific	Cabinet Secretariat, MIC, MOFA, METI	Building regional confidence measures through "ARF: ASEAN Regional Forum".
7-331b	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Asia Pacific	NPA, MOJ, MOFA	Supporting countries in Asian Pacific region to establish cybercrime jurisdiction.
7-331c	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Asia Pacific	MOD	Establishing cooperation with South-East Asian countries & Australia in cybersecurity.
7-332a	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	North America	Cabinet Secretariat, MOFA	Enhancing coordination & cooperation with US through "Japan-U.S. Cyber Dialogues".
7-332a2	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Europe	MOD	Enhancing cyber defence cooperation with European countries through "Japan-UK Bilateral Consultations on Cyberspace", "Japan-NATO Staff Talks on Cyber defence" & participation in exercises held by NATO.
7-332b	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	North America	MIC, MOFA	Enhancing information sharing with US based on "U.S.-Japan Policy Cooperation Dialogue on the Internet Economy".
7-332b2	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	North America	MIC	Promoting cooperation between Japan's ICT-ISAC & US IT-ISAC.
7-332c	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	North America	MOD	Enhancing cyber defence cooperation with US through "U.S.-Japan Cyber defence Policy Working Group".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-333ア	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	欧州	内閣官房、外務省及び関係府省庁において、二国間協議の枠組みを通じ、各国との連携を強化する。防衛省において、日英防衛当局間サイバー協議、日NATOサイバー防衛スタッフトークスやNATO主催の演習への参加等を通じ、欧州各国とのサイバー防衛協力を引き続き推進していく。
7-333イ	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	欧州	経済産業省において、IPAを通じ、技術的評価能力の向上に資する最新技術動向の情報収集等を行うため、JIWG及びその傘下のJHAS、JTEMS、JEDSと定期的に協議を行う。
7-334ア	国際社会の平和・安定及び我が国の安全保障	世界各国との協力・連携	中南米、中東、アフリカ	内閣官房、外務省及び関係府省庁において、国際的な会議の場等を活用し、二国間協議を実施していない国との関係も強化する。
7-410ア	横断的施策	研究開発の推進	―	内閣官房において、各府省庁と連携し、信頼性工学、心理学等の様々な社会科学的視点も含めた「サイバーセキュリティ研究開発戦略」を策定する。
7-410イ	横断的施策	研究開発の推進	―	総務省において、NICTを通じ、情報通信ネットワークの安全性を確保する上で、さまざまなシステムで利用されている暗号方式・プロトコル等の安全性評価を行い、システムの安全性維持に向けた研究開発を実施する。
7-411ア	横断的施策	研究開発の推進	サイバー攻撃の検知・防御能力の向上	総務省において、NICTを通じ、政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術の研究開発を行う。また、サイバーセキュリティ関連情報の大規模集約を行うとともに、セキュリティ検証プラットフォームを構築し、サイバーセキュリティ研究の基盤となる環境整備を行う。
7-411ア2	↑	↑	↑	
7-411ア3	↑	↑	↑	
7-411イ	横断的施策	研究開発の推進	サイバー攻撃の検知・防御能力の向上	経済産業省において、制御システムの挙動を解析し、サイバー攻撃を検知・予測する技術開発や、可用性を確保した脆弱性への対処技術に関する研究を行う。
7-411イ2	↑	↑	↑	
7-411ウ	横断的施策	研究開発の推進	サイバー攻撃の検知・防御能力の向上	総務省において、NICTを通じ、サイバーセキュリティの研究開発を促進するため、攻撃トラフィック、マルウェア検体等のデータセットについて、大学等の外部の研究機関の安全な利用を可能にする研究基盤（NONSTOP）を運用する。
7-411エ	横断的施策	研究開発の推進	サイバー攻撃の検知・防御能力の向上	文部科学省において、NIIを通じ、サイバー攻撃耐性を向上させるため、大学等の関係機関において、M2Mを含み学術評価に適したデータを実環境から継続的に収集し、データ解析技術の開発を促進する。
7-412ア	横断的施策	研究開発の推進	サイバーセキュリティと他分野の融合領域の研究	内閣官房において、各府省庁と連携し、信頼性工学、心理学等の様々な社会科学的視点も含めた「サイバーセキュリティ研究開発戦略」を策定する。
7-412イ	横断的施策	研究開発の推進	サイバーセキュリティと他分野の融合領域の研究	経済産業省において、IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会（サイバーフィジカルシステム）の実現・高度化に向け、そうした社会を支えるコア技術の調査・研究開発・実証等を行う。
7-412ウ	横断的施策	研究開発の推進	サイバーセキュリティと他分野の融合領域の研究	文部科学省において、理化学研究所革新知能統合研究センター（AIPセンター）を通じ、革新的な人工知能基盤技術の構築と、サイバーセキュリティを含む社会的課題の解決に向けた応用研究等を進めていく。
7-413ア	横断的施策	研究開発の推進	サイバーセキュリティのコア技術の保持	総務省において、NICTを通じ、情報理論的安全性（暗号が情報理論的な意味で無条件に安全である性質）を具備した量子暗号等を活用した量子情報通信ネットワーク技術の確立に向け、研究開発を実施する。
7-413イ	横断的施策	研究開発の推進	サイバーセキュリティのコア技術の保持	総務省及び経済産業省において、CRYPTREC暗号リストに掲載された暗号技術の監視、安全性及び信頼性の確保のための調査、研究、基準の作成等を行う。また、社会ニーズを見据え、暗号プロトコルを安全に利活用するための取組などについて検討する。さらに、NICT及びIPAを通じ、暗号技術の安全性に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査、暗号の普及促進、セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討を実施するため、暗号技術評価委員会及び暗号技術活用委員会を開催する。
7-413イ2	↑	↑	↑	
7-413イ3	↑	↑	↑	
7-413ウ	横断的施策	研究開発の推進	サイバーセキュリティのコア技術の保持	経済産業省において、AIST等を通じ、IoTシステムに付随する脅威に対応するため、ソフトウェア工学、暗号技術などを用いてシステムのセキュリティ、品質、安全性、効率の向上、などを両立させるための革新的、先端的技術の基礎研究に取り組む。
7-414ア	横断的施策	研究開発の推進	国際連携による研究開発の強化	総務省において、情報セキュリティ分野の国際標準化活動であるITU-T SG17等が主催する国際会合等に参加し、我が国の研究開発成果やIT環境・基準・ガイドライン等を踏まえて、国際規格への反映が行われるよう積極的に参画する。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-333a	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Europe	Cabinet Secretariat, MOFA	Enhancing cooperation through bilateral meetings.
7-333b	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Europe	METI, IPA	Gathering information on latest technologies through consultation with "JIWG: Joint Industry Working Group".
7-334a	Ensuring Peace and Stability of the International Community and National Security	Cooperation and Collaboration with Countries around the World	Latin America and the Caribbean, Middle East and Africa	Cabinet Secretariat, MOFA	Enhancing cooperation through bilateral meetings.
7-410a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	-	Cabinet Secretariat	Establishing "Strategy for Research & Development of Cybersecurity".
7-410b	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	-	MIC, NICT	Researching security assessment of cryptographic algorisms & protocols.
7-411a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	MIC, NICT	Researching technologies for countermeasures against cyber attacks.
7-411a2	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	MIC, NICT	Building up large scale reservoir of cybersecurity related information.
7-411a3	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	MIC, NICT	Improving R&D environment by establishing security validation platform.
7-411b	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	METI	Researching technologies for detection & prediction of cyber attacks on control systems.
7-411b2	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	METI	Researching technologies for vulnerability management on control systems without interruption of services.
7-411c	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	MIC, NICT	Providing with "NONSTOP" (R&D platform for secure handling of malware samples).
7-411d	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Improving Detection and Defense Capabilities against Cyber Attacks	MEXT, NII	Researching technologies for data analysis & resilience against cyber attacks.
7-412a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Promoting Interdisciplinary Research on Cybersecurity	Same as 7-410a2	Same as 7-410a2
7-412b	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Promoting Interdisciplinary Research on Cybersecurity	METI	Researching technologies for creation of cyber-physical system.
7-412c	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Promoting Interdisciplinary Research on Cybersecurity	MEXT, AIP Center	Promoting researching of advanced AI infrastructure & its practical research for cybersecurity area.
7-413a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Securing Cybersecurity Core Technologies	MIC, NICT	Researching for quantum cryptography communication.
7-413b	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Securing Cybersecurity Core Technologies	MIC, METI	Promoting "The List of Ciphers that should be Referred to in the Procurement for the e-Government System" by "CRYPTREC: Cryptography Research and Evaluation Committees".
7-413b2	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Securing Cybersecurity Core Technologies	MIC, METI, NICT, IPA	Researching technologies for secure cryptography.
7-413b3	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Securing Cybersecurity Core Technologies	MIC, METI, NICT, IPA	Promoting use of secure cryptography.
7-413c	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Securing Cybersecurity Core Technologies	METI, AIST	Researching innovative & advanced technologies for balancing security & efficiency of IoTs.
7-414a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Enhancing R&D in International Coordination	MIC	Positively contributing to international debate of standards for information security by participating ITU-T SG17.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-415ア	横断的施策	研究開発の推進	国際機関との連携	内閣府において、戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」により真贋判定技術（機器やソフトウェアの真正性・完全性を確認する技術）を含めた動作監視・解析技術と防御技術の研究開発を行う。
7-420ア	横断的施策	人材の育成・確保	ー	内閣官房において、関係府省庁と連携しつつ、「サイバーセキュリティ人材育成プログラム」に基づき、施策間連携を図りつつ、関係施策を促進していく。
7-421ア	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	文部科学省において、複数の大学や産学の連携によるサイバーセキュリティに係る実践的な演習を推進する体制の構築やPBL（課題解決型学習）の実施を支援する。
7-421イ	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	内閣官房において、産業界や大学、関係省庁等、産学官の連携体制の下、情報共有を行いつつ、モデルとなるカリキュラムの策定をはじめとした施策間連携を推進する。
7-421ウ	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	文部科学省及び経済産業省において、高度なITの知識と経営などその他の領域における専門知識を併せもつハイブリッド型人材の育成を進める。
7-421エ	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	文部科学省において、高等専門学校におけるセキュリティ教育の強化のための施策として、企業等のニーズを踏まえた技術者のセキュリティ教育に必要な教材・教育プログラム開発を進める。また、並行して、2016年より、情報セキュリティ教育の演習拠点を整備（2016年：5拠点、2017年：5拠点（予定）、合計10拠点整備予定）し、全国の高等専門学校生が共同で利用できるサイバーレンジ（実践的な演習環境）の提供に向けた取組を推進する。
7-421オ	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	文部科学省において、IT技術者等のサイバーセキュリティに係る素養の向上を図るため、高等教育機関等における社会人学生の受け入れを促進する。
7-421カ	横断的施策	人材の育成・確保	高等教育段階や職業能力開発における社会ニーズに合った人材の育成	厚生労働省において、離職者や在職者を対象として職業に必要な技能及び知識を習得させるため、サイバーセキュリティに関する内容を含む公共職業訓練を実施するとともに、離職者や在職者を対象とした教育訓練給付制度において、サイバーセキュリティに関する内容を含む教育訓練を指定する。
7-422ア	横断的施策	人材の育成・確保	初等中等教育段階における教育の充実	文部科学省において、次期学習指導要領の実施を見据え、児童生徒の発達の段階に応じた、プログラミング的思考や情報セキュリティ、情報モラル等を含めた情報活用能力を培う教育を一層推進する。特に、各学校における指導の改善・充実に向けて、教科横断的な情報活用能力の育成に係るカリキュラム・マネジメントの在り方や、それに基づく指導方法・教材の利活用等について、実践的な研究を実施する。
7-422イ	横断的施策	人材の育成・確保	初等中等教育段階における教育の充実	文部科学省において、教員研修センターと連携し、情報通信技術を活用した指導や情報モラルに関する指導力の向上を図るため、各地域で情報教育の中核的な役割を担う教員等を対象とした研修を実施する。また、教員等を対象とした情報モラル教育セミナー・フォーラム等を開催する。
7-423ア	横断的施策	人材の育成・確保	突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保	経済産業省において、若年層のセキュリティ意識向上と突出した人材の発掘・育成を目的としてIPAと「セキュリティ・キャンプ実施協議会」にて共催しているセキュリティ・キャンプについて、サイバーセキュリティを取り巻く状況の変化への更なる対応を図る。
7-423イ	横断的施策	人材の育成・確保	突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保	経済産業省において、情報セキュリティをテーマとした様々な競技を通して、攻撃・防御両者の視点を含むセキュリティの総合力を試すハッキングコンテスト「CTF」について、NPO日本ネットワークセキュリティ協会及び企業が共同で開催地域拡大や競技内容の向上を図り、更なる人材候補者を増やすべく、大学等との連携や多用なコンテストの在り方を検討するとともに、同協会で実施するコンテスト（「SECCON CTF 2017」）について経済産業省において普及・広報の支援を行う。
7-423ウ	横断的施策	人材の育成・確保	突出した能力を有しグローバルに活躍できる人材の発掘・育成・確保	経済産業省において、ITを駆使してイノベーションを創出することのできる独創的なアイディア・技術を有する人材の発掘・育成に向け、「未踏IT人材発掘・育成事業」を実施する。
7-424ア	横断的施策	人材の育成・確保	人材が将来にわたって活躍し続けるための環境整備	内閣官房及び経済産業省において、情報セキュリティ人材を含めた高度IT人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の周知及び普及を図る。
7-424イ	横断的施策	人材の育成・確保	人材が将来にわたって活躍し続けるための環境整備	経済産業省において、国家試験である情報処理技術者試験において、組織のセキュリティポリシーの運用等に必要となる知識を問う「情報セキュリティマネジメント試験」の普及を図る。
7-424ウ	横断的施策	人材の育成・確保	人材が将来にわたって活躍し続けるための環境整備	経済産業省において、情報サービスの提供に必要な実務能力を明確化、体系化した共通指標であるITスキル標準の全面的な改訂に向け、第4次産業革命に伴い主流となる新技術に対応するIT人材に焦点を当てたスキル標準の検討を引き続き行う。
7-424エ	横断的施策	人材の育成・確保	人材が将来にわたって活躍し続けるための環境整備	経済産業省において、情報セキュリティに係る最新の知識・技能を備えた専門人材の国家資格として2016年に開始した情報処理安全確保支援士（登録セキスペ）制度の着実な実施に向けて必要な措置を講じるとともに、当該制度の普及のため、企業や団体への周知等を積極的に行う。

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-415a	Cross-Cutting Approaches to Cybersecurity	Advancement of R&D	Partnering with Relevant Entities	Cabinet Office, NEDO	Researching technologies for monitoring & analysis of control & communication systems through "Cyber-Security for Critical Infrastructure" of "SIP: Cross-ministerial Strategic Innovation Promotion Program".
7-420a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	-	Cabinet Secretariat	Promoting human resources development based on "Cybersecurity Human Resources Development Program".
7-421a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	MEXT	Promoting practical exercise & PBL (problem based learning) on cybersecurity by collaboration of multiple universities and/or academia-industry.
7-421b	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	Cabinet Secretariat	Promoting collaboration of industry, government & academia on practical cyber exercises.
7-421c	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	MEXT, METI	Developing human resources with hybrid careers.
7-421d	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	MEXT	Enhancing cybersecurity education at colleges of technology ("Kosen") based on needs from industry. Providing with cyber ranges
7-421e	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	MEXT	Promoting cybersecurity education for working adults at universities.
7-421f	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training	MHLW	Incorporating cybersecurity education into public vocational training.
7-422a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Expanding Elementary and Secondary Education for Cybersecurity	MEXT	Promoting education at elementary, middle & high schools about IT, information security & information moral based on individual ability of use of IT.
7-422b	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Expanding Elementary and Secondary Education for Cybersecurity	MEXT	Training teachers for IT skills & information moral
7-423a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Discovering, Fostering, and Acquiring the Best Brains as Global Players	METI, IPA	Continuing to hold "Security Camp" to raise awareness of youth & to discover prominent human resources.
7-423b	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Discovering, Fostering, and Acquiring the Best Brains as Global Players	METI	Jointly promoting CTFs with "JNSA: Japan Network Security Association".
7-423c	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Discovering, Fostering, and Acquiring the Best Brains as Global Players	METI	Conducting "MITOU Program: Exploratory IT Human Resources Project" to discover innovative talents.
7-424a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Building Long Term Career Paths for Cybersecurity Experts	Cabinet Secretariat, METI, IPA	Promoting "Information Technology Engineers Examination" to develop highly skilled IT human resources.
7-424b	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Building Long Term Career Paths for Cybersecurity Experts	METI, IPA	Promoting "Information Security Management Examination" (a subject of "Information Technology Engineers Examination").
7-424c	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Building Long Term Career Paths for Cybersecurity Experts	METI	Supporting young engineers & student to design their career pass in IT industry.
7-424d	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Building Long Term Career Paths for Cybersecurity Experts	METI	Promoting new national qualification "Registered Information Security Specialist".

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-424オ	横断的施策	人材の育成・確保	人材が将来にわたって活躍し続けるための環境整備	総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じて、若年層のICT人材を対象に、高度なセキュリティ技術を本格的に指導し、未来のサイバーセキュリティ研究者・起業家の育成に取り組む。
7-425ア	横断的施策	人材の育成・確保	組織力を高めるための人材育成	防衛省において、巧妙化するサイバー攻撃に適切に対応していくため、CSIRT要員に対するインシデント対処訓練を実施するとともに、国内外の大学院等への留学等を行い、人材育成への取組を実施する。
7-425イ	横断的施策	人材の育成・確保	組織力を高めるための人材育成	総務省において、NICTに組織した「ナショナルサイバートレーニングセンター」を通じ、国の行政機関、独立行政法人、重要インフラ事業者及び地方公共団体等におけるサイバー攻撃への対処能力の向上に向け、新たなシナリオによる実践的サイバー防御演習（CYDER）を実施する。
7-425ウ	横断的施策	人材の育成・確保	組織力を高めるための人材育成	防衛省において、自衛隊のサイバー攻撃対処部隊の対処能力の練度を向上させるため、指揮システムを模擬した環境を構築して、攻撃・防御の機能とこれに対する統裁・評価の機能等を備えた実戦的な演習環境を整備する。
7-425エ	横断的施策	人材の育成・確保	組織力を高めるための人材育成	防衛省において、防衛省と防衛産業との間におけるサイバー攻撃対処のための具体的・実効的連携要領の確立等に向けた取組を実施する。また、任務保証の観点から、任務遂行上依拠する社会インフラへのサイバー攻撃の影響に関する知見を向上し、関係主体との連携を深化させていく。
7-425エ2	↑	↑	↑	

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
7-424e	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Building Long Term Career Paths for Cybersecurity Experts	MIC, NICT	Training youth to cybersecurity expert at "National Cyber Training Center".
7-425a	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Strategizing Human Resources Development for Enhanced Organizational Capacities	MOD	Sending officials to study at graduate schools.
7-425b	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Strategizing Human Resources Development for Enhanced Organizational Capacities	MIC, NICT	Performing upgraded practical cyber defence exercise "(New) CYDER" at "National Cyber Training Center".
7-425c	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Strategizing Human Resources Development for Enhanced Organizational Capacities	MOD	Establishing practical exercise environment of communication system of JSDF.
7-425d	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Strategizing Human Resources Development for Enhanced Organizational Capacities	MOD	Enhancing cooperation between MOD/JSDF & defence industry.
7-425d2	Cross-Cutting Approaches to Cybersecurity	Development and Assurance of Cybersecurity Workforce	Strategizing Human Resources Development for Enhanced Organizational Capacities	MOD	Enhancing cooperation between MOD/JSDF & operators of infrastructures affecting operation.

【原文】サイバーセキュリティ2017				
項番	大項目	中項目	小項目	施策
7-500ア	推進体制	－	－	内閣官房において、JPCERT/CCと締結した国際連携活動及び情報共有等に関するパートナーシップの一層の進化を図るため、2015年度に構築した情報共有システムの機能向上を図るとともに連携体制についても逐次見直しを実施する。中期的には、2020年東京オリンピック・パラリンピック競技大会を見据え、NISC内に専従のCSIRT組織を整備する。また、サイバーセキュリティに関し、司令塔機能を果たすため、総合的分析機能の強化を図る。さらに、NICTと締結した研究開発や技術協力等に関するパートナーシップに基づいてNICTとの協力体制を整備し、サイバーセキュリティ対策に係る技術面の強化を図る。
7-500イ	推進体制	－	－	警察庁において、「セキュリティ情報センターについて」（2015年8月3日セキュリティ幹事会決定）等に基づき、セキュリティ情報センターを設置する。同センターにおいては、国の関係機関の協力を得て、サイバーセキュリティに係るものを含む2020年東京オリンピック・パラリンピック競技大会の安全に関する情報を集約するとともに、大会の安全に対する脅威及びリスクの分析、評価を行い、国の関係機関等に対し必要な情報を随時提供する。
7-500ウ	推進体制	－	－	内閣官房において、「2020年東京オリンピック競技大会・東京パラリンピック競技大会に向けたセキュリティ基本戦略（Ver.1）」（2017年3月21日セキュリティ幹事会決定）に基づくサイバーセキュリティ対策の強化のため、運営に大きな影響を及ぼし得る重要サービス事業者等におけるサイバーセキュリティに係るリスク評価について、大会の詳細や情勢の変化に応じた手順書の見直しを実施するとともに、地方における会場等を勘案し、対象となる事業者の地理的、分野的な拡大を図る。更に、特に重要なサービス事業者については国として横断的リスク評価を実施していく。また、これら重要サービス事業者等に対するサイバー攻撃への対応に係る関係主体との情報共有の中核的役割を果たすサイバーセキュリティ対処調整センター（オリンピック・パラリンピックCSIRT）の2018年度中の構築に向け、情報共有システムの構築を推進するとともに、2018年2月から3月にかけて開催される平昌冬期オリンピック・パラリンピック競技大会等の機会をとらえ関係組織間のさらなる連携の深化を図る。
7-500エ	推進体制	－	－	内閣官房において、サイバー攻撃等の事象に関する政府としての一連の初動対処（検知、判断、対処、報告）を見直し、サイバーセキュリティに係る危機管理対応の一層の強化が図られるよう留意する。

Department Abbreviation

Abbreviation	Full Name
AIST	National Institute of Advanced Industrial Science and Technology
AIP Center	Center for Advanced Intelligence Project (@ RIKEN: National Research & Development Agency, Institute of Physical and Chemical Reseach)
Cabinet Office	Cabinet Office
Cabinet Secretariat	Cabinet Secretariat
CSSC	Cotrol System Security Center
CYMAT	Cyber Incident Mobile Assistant Team
FSA	Financial Services Agency
GSOC	Government Security Operation Coodination Team
IPA	Information-Technology Promotion Agency
JICA	Japan International Cooperation Agency
JPCERT/CC	Japan Computer Emergency Response Team Cordination Center
JSDF	Japan Self-Defense Forces
METI	Ministry of Economy, Trade and Industry
MEXT	Ministry of Education, Culture, Sports, Science and Technology
MHLW	Ministry of Health, Labour and Welfare
MIC	Ministry of Internal Affairs and Communications
MOD	Ministry of Defense
MOFA	Ministry of Foreign Affairs
MOJ	Minstry of Jastice
MPD	Metropolitan Police Department
NEDO	New Energy and Industrial Technology Development Organization
NICT	National Institute of Information and Communications Technology
NII	National Institute of Informatics
NISC	National Center of Incident Readiness and Strategy for Cybersecurity
NPA	National Police Agency
NPAc	National Police Academy
PPC	Personal Information Protection Commission
Prefectural Police	Prefectural Police

Itemised					
#	Category	Sub-category	Strategy	Agency	Action Item
					N/A
					N/A
					N/A
					N/A

Appendix D U.K. Cybersecurity Strategy ("National Cyber Security Strategy 2016 - 2023" itemised to action items)

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection		Objective/Approach/Measuring	#	Action Item
5. DEFEND			5.0.1. The DEFEND elements of this strategy aim to ensure that UK networks, data and systems in the public, commercial and private spheres are resilient to and protected from cyber attack. It will never be possible to stop every cyber attack, just as it is not possible to stop every crime.		None
			However, together with citizens, education providers, academia, businesses and other governments, the UK can build layers of defence that will significantly reduce our exposure to cyber incidents, protect our most precious assets, and allow us all to operate successfully and prosperously in cyberspace. Acting to promote cooperation between states and good cyber security practice is also in the interest of our collective security.		None
			5.0.2. The Government will implement measures to ensure that citizens, businesses, public and private sector organisations and institutions have access to the right information to defend themselves. The National Cyber Security Centre provides a unified source of advice in government for threat intelligence and information assurance, ensuring that we can offer tailored guidance for cyber defence and respond quickly and effectively to major incidents in cyberspace.		None
			The Government will work with industry and international partners to define what good cyber security looks like for public and private sectors, for our most important systems and services, and for the economy as a whole. We will build security by default into all new government and critical systems. Law enforcement agencies will collaborate closely with industry and the National Cyber Security Centre to provide dynamic criminal threat intelligence with which industry can better defend itself, and to promote protective security advice and standards.		None
	5.1. ACTIVE CYBER DEFENCE		5.1.1. Active Cyber Defence (ACD) is the principle of implementing security measures to strengthen a network or system to make it more robust against attack. In a commercial context, Active Cyber Defence normally refers to cyber security analysts developing an understanding of the threats to their networks, and then devising and implementing measures to proactively combat, or defend, against those threats. In the context of this strategy, the Government has chosen to apply the same principle on a larger scale: the Government will use its unique expertise, capabilities and influence to bring about a step-change in national cyber security to respond to cyber threats.		None
			The ‘network’ we are attempting to defend is the entire UK cyberspace. The activities proposed represent a defensive action plan, drawing on the expertise of NCSC as the National Technical Authority to respond to cyber threats to the UK at a macro level.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Objectives	5.1.2. In undertaking ACD, the Government aims to:		None
			• make the UK a much harder target for state sponsored actors and cyber criminals by increasing the resilience of UK networks;		None
			• defeat the vast majority of highvolume/ low-sophistication malware activity on UK networks by blocking malware communications between hackers and their victims;		None
			• evolve and increase the scope and scale of Government's capabilities to disrupt serious state sponsored and cyber criminal threats;		None
			• secure our internet and telecommunications traffic from hijacking by malicious actors;		None
			• harden the UK's critical infrastructure and citizen-facing services against cyber threats; and		None
			• disrupt the business model of attackers of every type, to demotivate them and to reduce the harm that their attacks can cause.		None
		Approach	5.1.3. In pursuit of these aims, the Government will:		None
			• work with industry, especially Communications Service Providers (CSPs), to make it significantly harder to attack UK internet services and users, and greatly reduce the prospect of attacks having a sustained impact on the UK. This will include tackling phishing, blocking malicious domains and IP addresses, and other steps to disrupt malware attacks. It will also include measures to secure the UK's telecommunications and internet routing infrastructure;		None
			• increase the scale and development of GCHQ, Ministry of Defence and NCA capabilities to disrupt the most serious cyber threats to the UK, including campaigns by sophisticated cyber criminals and hostile foreign actors; and		None
			• better protect government systems and networks, help industry build greater security into the CNI supply chain, make the software ecosystem in the UK more secure, and provide automated protections for government online services to the citizen.		None
			5.1.4. Where possible, these initiatives will be delivered with or through partnerships with industry. For many, industry will be designing and leading implementation, with the Government's critical contribution being expert support, advice and thought-leadership.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			5.1.5. The Government will also undertake specific actions to implement these measures, which will include:		None
			• working with CSPs to block malware attacks. We will do this by restricting access to specific domains or web sites that are known sources of malware. This is known as Domain Name System (DNS) blocking / filtering;	5105-1	Blocking known malware sources
			• preventing phishing activity that relies on domain 'spoofing' (where an email appears to be from a specific sender, such as a bank or government department, but is actually fraudulent) by deploying an email verification system on government networks as standard and encouraging industry to do likewise;	5105-2	Promoting email verification systems
			• promoting security best practice through multi-stakeholder internet governance organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) which coordinates the domain name system), the Internet Engineering Task Force (IETF) and the European Regional Internet Registry (RIPE) and engagement with stakeholders in the UN Internet Governance Forum (IGF);	5105-3	Promoting security best practices
			• working with law enforcement channels in order to protect UK citizens from being targeted in cyber attacks from unprotected infrastructure overseas;		None
			• working towards the implementation of controls to secure the routing of internet traffic for government departments to ensure that it cannot be illegitimately re-routed by malicious actors; and	5105-4	Implementing secure routing
			• investing in programmes in the Ministry of Defence, the NCA and GCHQ that will enhance the capabilities of these organisations to respond to, and disrupt, serious state-sponsored and criminal cyber activity targeting UK networks.	5105-5	Enhancing capabilities against state-sponsored cyber activities
			We will develop these technical interventions as threats evolve to ensure that UK citizens and businesses are protected by default from the majority of large-scale commodity cyber attacks.	5105-6	Promoting technical development
		Measuring success	5.1.6. The Government will measure its success in establishing effective ACD by assessing progress towards the following outcomes:	5106-1	Metrics
			• the UK is harder to 'phish', because we have large-scale defences against the use of malicious domains, more active anti-phishing protection at scale and it is much harder to use other forms of communication, such as 'vishing' and SMS spoofing, to conduct social engineering attacks;		None
			• a far larger proportion of malware communications and technical artefacts associated with cyber attacks and exploitation are being blocked;		None
			• the UK's internet and telecommunications traffic is significantly less vulnerable to rerouting by malicious actors;		None
			• GCHQ, the Armed Forces' and NCA capabilities to respond to serious statesponsored and criminal threats have significantly increased.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
	5.2. BUILDING A MORE SECURE INTERNET		5.2.1. Changing technology provides us with the opportunity to significantly reduce the ability of our adversaries to conduct cyber crime in the UK by ensuring that future online products and services coming into use are 'secure by default'. That means ensuring that the security controls built into the software and hardware we use are activated as a default setting by the manufacturer so that the user experiences the maximum security offered to them, unless they actively choose to turn it off.		None
			The challenge is to effect transformative change in a way that supports the end user and offers a commercially viable, but secure, product or service – all within the context of maintaining the free and open nature of the Internet.		None
			5.2.2. The Government is well-placed to take a lead role in exploring those new technologies that will better protect our own systems, help industry build greater security into the supply chain, secure the software ecosystem and provide automated protections to citizens accessing government services online.		None
			The Government must test and implement new technologies that provide automated protection for government online products and services. Where possible, similar technologies should be offered to the private sector and the citizen.		None
		Objective	5.2.3. The majority of online products and services coming into use become 'secure by default' by 2021. Consumers will be empowered to choose products and services that have built-in security as a default setting. Individuals can switch off these settings if they choose to do so but those consumers who wish to engage in cyberspace in the most secure way will be automatically protected.		None
		Our approach	5.2.4. We will pursue the following actions:		None
			• the Government will lead by example by running secure services on the Internet that do not rely on the Internet itself being secure;		None
			• the Government will explore options for collaboration with industry to develop cutting-edge ways to make hardware and software more 'secure by default'; and		None
			• we will adopt challenging new cyber security technologies in government, encouraging Devolved Administrations to do likewise, in order to reduce perceived risks of adoption. This will provide proof of concept and demonstrate the security benefits of new technologies and approaches.		None
			It will also put security at the heart of new product development, eliminate opportunities for criminal exploitation and thereby protect the end user.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			5.2.5. To do this we will:		None
			• continue to encourage hardware and software providers to sell products with security settings activated as default, requiring the user to actively disable these settings to make them insecure.	5205-1	Security settings by default
			Some vendors are already doing this, but some are not yet taking these necessary steps;		None
			• continue to develop an Internet Protocol (IP) reputation service to protect government digital services (this would allow online services to get information about an IP address connecting to them, helping the service make more informed risk management decisions in real time);	5205-2	Developing IP reputation informing service
			• seek to install products on government networks that will provide assurance that software is running correctly, and not being maliciously interfered with;	5205-3	Software integrity assuarance
			• look to expand beyond the GOV.UK domain into other digital services measures that notify users who are running out-of-date browsers; and	5205-4	Promoting out-of-date browsers filtering
			• invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast Identity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate. The Government will test innovative authentication mechanisms to demonstrate what they can offer, both in terms of security and overall user experience.	5205-5	Investing new technologies like TPM, FIDO
			5.2.6. The Government will also explore how to encourage the market by providing security ratings for new products, so that consumers have clear information on which products and services offer them the greatest security. The Government will also explore how to link these product ratings to new and existing regulators, and ways to warn consumers when they are about to take an action online that might compromise their security.	5206-1	Introducing security ratings for products
		Measuring success	5.2.7. The Government will measure its success in building a secure Internet by assessing progress towards the following outcomes:	5207-1	Metrics
			• the majority of commodity products and services available in the UK in 2021 are making the UK more secure because they have their default security settings enabled by default or have security integrated into their design; and		None
			• all government services provided at national, local and Devolved Administration level are trusted by the UK public because they have been implemented as securely as possible, and fraud levels are within acceptable risk parameters.		None
	5.3. PROTECTING GOVERNMENT		5.3.1. The UK Government, Devolved Administrations and the wider public sector hold large quantities of sensitive data. They deliver essential services to the public and operate networks that are critical to national security and resilience. The Government's systems underpin the functioning of our society. The modernisation of public sector services will continue to be the cornerstone of the UK's Digital Strategy – the Government's digital ambition is for the UK to be the world's leading digital nation.		None
			To retain the trust of citizens in online public sector services and systems, data held by government must be protected and all branches of government must implement appropriate levels of cyber security in the face of continuous attempts by hostile actors to gain access to government and public sector networks and data.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Objectives	5.3.2. We want to achieve the following outcomes:		None
			• citizens use government online services with confidence: they trust that their sensitive information is safe and, in turn, understand their responsibility to submit their sensitive information online in a secure manner;		None
			• the Government will set and adhere to the most appropriate cyber security standards, to ensure that all branches of government understand and meet their obligations to secure their networks, data and services; and		None
			• the Government's critical assets, including those at the highest classification, are protected from cyber attacks.		None
		Our approach	5.3.3. The UK Government will continue to move more of its services online so that the UK can become truly 'digital by default'.	5303-1	Promoting e-government
			The Government Digital Service (GDS), the Crown Commercial Service (CCS) and the NCSC will ensure that all new digital services built or procured by government are also 'secure by default'.	5303-2	'Security-by-default' in e-government
			5.3.4. The Government's networks are highly complex and in many cases still incorporate legacy systems, as well as some commercially available software which is no longer supported by the vendor. We will ensure that there are no unmanaged risks from legacy systems and unsupported software.	5304-1	Eliminating unsupported softwares in public sector
			5.3.5. We will improve government and wider public sector resilience to cyber attack. This means ensuring an accurate and up to date knowledge of all systems, data, and those who have access to them.	5305-1	Comprehensive knowledge about all public sector systems
			The likelihood and impact of a cyber incident will be minimised by implementing best practice as set out by the NCSC.	5305-2	Promoting best practices in public sector
			The Government will also ensure that it is able to respond effectively to cyber incidents through a programme of incident exercises and regular testing of government networks.	5305-3	Cyber exercise
			We will invite Devolved Administrations and local authorities to participate in these exercises, as appropriate.	5305-4	Participation of lower levels of public sector
			Through automated scanning, we will ensure that we have a better knowledge of government's online security status.	5305-5	Automated vulnerability scan on e-government
			5.3.6. Cyber security is not just about technology. Almost all successful cyber attacks have a contributing human factor.		None
			We will therefore continue to invest in our people, to ensure that everyone who works in government has a sound awareness of cyber risk.	5306-1	Awarenes raising in public sector
			We will develop specific cyber expertise in areas where the risks are heightened and ensure that we have the right processes in place to manage these risks effectively.	5306-2	Development of cyber expertise
			5.3.7. The NCSC will develop worldleading cyber security guidance which will keep pace with the threat and development of new technologies.	5307-1	Developing new guidance
			We will take steps to make sure government organisations have easy access to threat information to inform their understanding of their own cyber risks and take appropriate action.	5307-2	Making cyber threat infomation easily available
			5.3.8. We will continue to improve our highest classification networks to safeguard the Government's most sensitive communications.	5308-1	Improving highest classification networks

National Cyber Security Strategy 2016 - 2023					Itemised	
Section	Subsection	Objective/Approach/Measuring			#	Action Item
			5.3.9.	Health and care systems pose unique challenges in the context of cyber security.		None
				The sector employs around 1.6 million people in over 40,000 organisations, each with vastly differing information security resources and capability. The National Data Guardian for Health and Care has set new data security standards for the health and social care systems in England, alongside a new data consent/opt-out model for patients. The Government will work with health and social care organisations to implement these standards.	5309-1	Promoting new standards in health & care industries
			5.3.10.	Cyber security is vital to our defence.		None
				Our Armed Forces depend on information and communications systems, both in the UK and on operations around the world. The infrastructure and personnel of the Ministry of Defence (MoD) are prominent targets.		None
				Defence systems are regularly targeted by criminals, foreign intelligence services and other malicious actors seeking to exploit personnel, disrupt business and operations, and corrupt and steal information. We will	5310-1	Awareness raising in Armed Forces
					5310-2	Enhancing detection & reaction functions
		Measuring success	5.3.11.	The Government will measure its success in protecting government networks, systems and data by assessing progress towards the following outcomes:	5311-1	Metrics
				• the Government has an in-depth understanding of the level of cyber security risk across the whole of government and the wider public sector;		None
				• individual government departments and other bodies protect themselves in proportion to their level of risk and to an agreed government minimum standard;		None
				• government departments and the wider public sector are resilient and can respond effectively to cyber incidents, maintaining functions and recovering quickly;		None
				• new technologies and digital services deployed by government will be cyber secure by default;		None
				• we are aware of, and actively mitigating, all known internet-facing vulnerabilities in government systems and services; and		None
				• all suppliers to the Government meet appropriate cyber security standards.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
	5.4. PROTECTING OUR CRITICAL NATIONAL INFRASTRUCTURE AND OTHER PRIORITY SECTORS	Context	5.4.1. The cyber security of certain UK organisations is of particular importance because a successful cyber attack on them would have the severest impact on the country's national security. This impact could have a bearing on the lives of UK citizens, the stability and strength of the UK economy, or the UK's international standing and reputation. This premium group of companies and organisations within the public and private sector includes the critical national infrastructure (CNI), which provides essential services to the nation. Ensuring the CNI is secure and resilient against cyber attack will be a priority for the Government. This premium group also includes other companies and organisations, beyond the CNI, that require a greater level of support. They include:		None
			• the jewels in our economic crown – the UK's most successful companies and also those that hold our future economic strength in the value of their research and intellectual property;		None
			• data holders – not just organisations that hold large amounts of personal data, but also those that hold data on vulnerable citizens here and abroad, such as charities;		None
			• high-threat targets – such as media organisations, where an attack could harm the UK's reputation, damage public confidence in the Government, or endanger freedom of expression;		None
			• the touchstones of our digital economy – digital service providers that enable e-commerce and our digital economy, and who depend on consumer trust in their services; and		None
			• those organisations that, through market forces and authority, can exert influence on the whole economy to improve their cyber security, such as insurers, investors, regulators and professional advisors.		None
			5.4.2. More needs to be done to protect these vital parts of our economy and support the organisations that heavily influence others. Our CNI – in both the private and public sector – continues to be a target for attack. Across these and many other priority sectors cyber risk is still not properly understood or managed, even as the threat continues to diversify and increase.		None
		Objective	5.4.3. the UK Government, working with the Devolved Administrations and other responsible authorities where appropriate, will ensure that the UK's most important organisations and companies, including the CNI, are sufficiently secure and resilient in the face of cyber attack. Neither the Government nor other public bodies will take on the responsibility to manage this risk for the private sector, which rightly sits with boards, owners and operators.		None
			But the Government will provide support and assurance proportionate both to the threat these companies and organisations face, and to the consequences of their being attacked.		None

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Our approach	5.4.4. Organisations and company boards are responsible for ensuring their networks are secure. They must identify critical systems and regularly assess their vulnerability against an evolving technological landscape and threat.	5404-1	Awareness raising of board members
			They must invest in technology and their staff to reduce vulnerabilities in current and future systems, and in their supply chain, to maintain a level of cyber security proportionate to the risk.	5404-2	Urging organisations & companies to invest in security
			They must also have tested capabilities in place to respond if an attack happens.	5404-3	Urging organisations & companies to excercise incident response
			For the CNI, they must do this with government bodies and regulators so we can be confident that cyber risk is being properly managed and – if it is not – intervene in the interests of national security.	5404-4	Cybersecurity in CNI
			5.4.5. The Government will, therefore, understand the level of cyber security across our CNI and have measures in place to intervene where necessary to drive improvements that are in the national interest.	5405-1	Government to understand cybersecurity levels in CNI
			5.4.6. The Government will:		None
			• share threat information with industry that only the Government can obtain so they know what they must protect themselves against;	5406-1	Sharing information with CNI
			• produce advice and guidance on how to manage cyber risk and, working collaboratively with industry and academia, define what good cyber security looks like;	5406-2	Setting a new standard by collaborating with industries & academia
			• stimulate the introduction of the highend security needed to protect the CNI, such as training facilities, testing labs, security standards and consultancy services; and	5406-3	Encouraging investment in the latest technologies
			• conduct exercises with CNI companies to assist them in managing their cyber risks and vulnerabilities.	5406-4	Exercising with CNI
			5.4.7. The NCSC will provide these services for the UK's most important companies and organisations, including the CNI. It will do so in partnership with departments and regulators, who will assure whether cyber risk is being managed in their sectors to the level demanded by the national interest.		None
			5.4.8. The Government will also make sure that the right regulatory framework for cyber security is in place, one that:		None
			• ensures industry acts to protect itself from the threat;	5408-1	Private sector mind-set
			• is outcome focused and sufficiently flexible so that it will not fall behind the threat, or lead to compliance rather than sound risk management;	5408-2	Flexible policies for private sector cybersecurity
			• is agile enough to foster growth and innovation, rather than lead it;	5408-3	Promoting growth of cybersecurity industries
			• is harmonised with regimes in other jurisdictions so that UK companies do not suffer from a fragmented and burdensome approach; and	5408-4	Coordinating international legal framework
			• delivers, when combined with effective support from the Government, a competitive advantage for the UK.		None
			5.4.9. Many of our industry sectors are already regulated for cyber security.		None
			Nonetheless, we must ensure the right steps are taken across the whole economy, including the CNI, to manage cyber security risks.	5409-1	Cybersecurity as a regulation

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Measuring success	5.4.10. The Government will measure its success in protecting our CNI and other priority sectors by assessing progress towards the following outcomes:	5410-1	Metrics
			• we understand the level of cyber security across the CNI, and have measures in place to intervene, where necessary, to drive improvements in the national interest; and		None
			• our most important companies and organisations understand the level of threat and implement proportionate cyber security practices.		None
	5.5. CHANGING PUBLIC AND BUSINESS BEHAVIOURS		5.5.1. A successful UK digital economy relies upon the confidence of businesses and the public in online services. The UK The Government has worked with industry and other parts of the public sector to increase awareness and understanding of the threat. The Government has also provided the public and business with access to some of the tools that they need to protect themselves. While there are many organisations that are doing an excellent job – in places, world-leading – of protecting themselves, and in providing services to others online, the majority of businesses and individuals are still not properly managing cyber risk.		None
		Objective	5.5.2. Our objective is to ensure that individuals and organisations, regardless of size or sector, are taking appropriate steps to protect themselves, and their customers, from the harm caused by cyber attacks.		None
		Our approach	5.5.3. The Government will provide the advice that the economy needs to protect itself. We will improve how this advice is delivered to maximise its effect. For the public, the Government will harness 'trusted voices' to increase the reach, credibility and relevance of our message. We will provide advice that is easy to act upon and relevant to individuals, at the point they are accessing services and exposing themselves to risk.	5503-1	Public awareness raising
			We will involve the Devolved Administrations and other authorities as appropriate.		None
			5.5.4. For businesses, we will work through organisations such as insurers, regulators and investors which can exert influence over companies to ensure they manage cyber risk. In doing so, we will highlight the clear business benefits and the pricing of cyber risk by market influencers. We will seek to understand better why many organisations still fail to protect themselves adequately and then work in partnership with organisations such as professional standards bodies, to move beyond raising awareness to persuade companies to take action. We will also make sure we have the right regulatory framework in place to manage those cyber risks the market fails to address. As part of this, we will seek to use levers, such as the GDPR, to drive up standards of cyber security and protect citizens.	5504-1	Using cybersecurity insurance for corporate awareness raising
			5.5.5. Individuals and organisations and organisations in the UK will have access to the information, education, and tools they need to protect themselves. To ensure we deliver a step-change in public behaviour, we will maintain a coherent and consistent set of messages on cyber security guidance from both the Government and our partners.	5505-1	Making information, education, tools easily available to public & corporates
			The NCSC will provide technical advice to underpin this guidance. It will reflect business and public priorities and practices, and be clear, easily accessible and consistent, while keeping pace with the threat.		None
			Law enforcement will work closely with industry and the NCSC to share the latest criminal threat intelligence, to support industry to defend itself against threats, and to mitigate the impact of attacks on UK victims.	5505-2	Intelligence sharing between government & law enforcement

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Measuring success	5.5.6. The Government will measure its success in protecting our CNI and other priority sectors by assessing progress towards the following outcomes:		(same as 5.4.10)
			• the UK economy's level of cyber security is as high as, or higher than, comparative advanced economies;		None
			• the number, severity and impact of successful cyber attacks against businesses in the UK has reduced, because cyber hygiene standards have improved; and		None
			• there is an improving cyber security culture across the UK because organisations and the public understand their cyber risk levels and understand the cyber hygiene steps they need to take to manage those risks.		None
	5.6. MANAGING INCIDENTS AND UNDERSTANDING THE THREAT		5.6.1. The number and severity of cyber incidents affecting organisations across the public and private sector are likely to increase. We therefore need to define how both the private sector and the public engage with the Government during a cyber incident. We will ensure that the UK Government's level of support for each sector – taking into account its cyber maturity – is clearly defined and understood. The Government's collection and dissemination of information about the threat must be delivered in a manner and at a speed suitable for all types of organisation. The private sector, government and the public can currently access multiple sources of information, guidance and assistance on cyber security.		None
			This must be simplified.		None
			5.6.2. We must ensure that the Government offering, both in response to incidents, and in the provision of guidance, does not exist in isolation, but in partnership with the private sector. Our incident management processes should reflect a holistic approach to incidents, whereby we learn from partners and share mitigation techniques. We will also continue to use our relationships with other Computer Emergency Response Teams (CERTs) and our allies as an integrated part of our incident management function.		None
			5.6.3. Current incident management remains somewhat fragmented across government departments and this strategy will create a unified approach. The NCSC will deliver a streamlined and effective government-led incident response function.		None
			In the event of a serious cyber incident, we will ensure that the Armed Forces are able to provide assistance, whether in a conventional form addressing the physical impact of an incident, or in the form of specialist support from regular or reserve cyber personnel. While we will provide all the support our resources will allow, the Government continues to stress the importance of industry, society and the public acting to safeguard their basic cyber security.		None
		Objectives	5.6.4. Our objectives are as follows:		None
			• the Government will provide a single, joined-up approach to incident management, based on an improved understanding and awareness of the threat and actions being taken against us. The NCSC will be a key enabler, as will partnership with the private sector, law enforcement and other government departments, authorities and agencies;		None
			• the NCSC defines clear processes for reporting incidents, tailored to the profile of the victim; and		None
			• we will prevent the most common cyber incidents, and we will have effective information-sharing structures in place to inform 'pre-incident' planning.		None
		Our approach	5.6.5. It is the responsibility of organisation and company management, in both the public and private sector, to ensure their networks are secure and to exercise incident response plans. In the event of a significant incident, the Government incident management process will reflect the three distinct elements of a cyber incident: the precursor causes, the incident itself and the post-incident response.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			5.6.6. To deliver incident management that is effective for both government and the private sector, we will work closely to review and define the scope of the Government response to ensure it reinforces cooperation.	5606-1	Enhancing cooperation in incident response between government & private sector
			We will build on our national cyber exercise plan, using our improved understanding and awareness of the threat, to improve our offer of support to public and private sector partners.	5606-2	Performing inter-sectoral exercise
			5.6.7. We will create a trusted and credible government identity for incident advice, assistance and assurance. This will increase the cyber security awareness across the UK digital community and will enable us the better to identify trends, take pro-active measures and, ultimately, prevent incidents.	5607-1	Trust between government & private sector
			5.6.8. In moving towards automated information sharing (i.e. cyber security systems automatically alerting each other to incidents or attacks), we will deliver a more effective service. This will allow organisations to act swiftly on relevant threat information.	5608-1	Automated information sharing system
		Measuring success	5.6.9. The Government will measure its success in managing incidents by assessing progress towards the following outcomes:	5609-1	Metrics
			• a higher proportion of incidents are reported to the authorities, leading to a better understanding of the size and scale of the threat;		None
			• cyber incidents are managed more effectively, efficiently and comprehensively, as a result of the creation of the NCSC as a centralised incident reporting and response mechanism; and		None
			• we will address the root causes of attacks at a national level, reducing the occurrence of repeated exploitation across multiple victims and sectors.		None
6. DETER			6.0.1. The National Security Strategy states that defence and protection start with deterrence. This is as true in cyberspace as any other sphere. To realise our vision of a nation that is secure and resilient to cyber threats, and prosperous and confident in the digital world, we have to dissuade and deter those who would harm us and our interests. To achieve this we all need to continue to raise levels of cyber security so that attacking us in cyberspace – whether to steal from us or harm us – is neither cheap nor easy. Our adversaries must know that they cannot act with impunity: that we can and will identify them, and that we can act against them, using the most appropriate response from amongst all the tools at our disposal. We will continue to build global alliances and promote the application of international law in cyberspace. We will also more actively disrupt the activity of all those who threaten us in cyberspace and the infrastructure on which they rely. Delivering this ambition requires world-class sovereign capabilities.		None
	6.1. CYBER'S ROLE IN DETERRENCE		6.1.1. Cyberspace is only one sphere in which we must defend our interests and sovereignty. Just as our actions in the physical sphere are relevant to our cyber security and deterrence, so our actions and posture in cyberspace must contribute to our wider national security.		None
			6.1.2. The principles of deterrence are as applicable in cyberspace as they are in the physical sphere. The UK makes clear that the full spectrum of our capabilities will be used to deter adversaries and to deny them opportunities to attack us. However, we recognise that cyber security and resilience are in themselves a means of deterring attacks that rely on the exploitation of vulnerabilities.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			6.1.3. We will pursue a comprehensive national approach to cyber security and deterrence that will make the UK a harder target, reducing the benefits and raising the costs to an adversary – be they political, diplomatic, economic or strategic. We must ensure our capability and intent to respond are understood by potential adversaries in order to influence their decision-making.		None
			We shall have the tools and capabilities we need: to deny our adversaries easy opportunities to compromise our networks and systems; to understand their intent and capabilities; to defeat commodity malware threats at scale; and to respond and protect the nation in cyberspace.		None
	6.2. REDUCING CYBER CRIME		6.2.1. We need to raise the cost, raise the risk, and reduce the reward of cyber criminals' activity. While we must harden the UK against cyber attacks and reduce vulnerabilities, we must also focus relentlessly on pursuing criminals who continue to target the UK.		None
			6.2.2. Law enforcement agencies will focus their efforts on pursuing the criminals who persist in attacking UK citizens and businesses. We will work with domestic and international partners to target criminals wherever they are located, and to dismantle their infrastructure and facilitation networks. Law enforcement agencies will also continue to help raise awareness and standards of cyber security, in collaboration with the NCSC.		None
			6.2.3. This strategy complements the 2013 Serious and Organised Crime Strategy, which set out the UK Government's strategic response to cyber crime, alongside other types of serious and organised crime. The National Cyber Crime Unit (NCCU) that sits within the National Crime Agency (NCA) was established to lead and coordinate the national response to cyber crime. Action Fraud provides a national reporting centre for fraud and cyber crime. A network of cyber crime units within Regional Organised Crime Units (ROCUs) provide access to specialist cyber capabilities at a regional level, supporting the NCCU and local forces.		None
		Objective	6.2.4. We will reduce the impact of cyber crime on the UK and its interests by deterring cyber criminals from targeting the UK and relentlessly pursuing those who persist in attacking us.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Our approach	6.2.5. To reduce the impact of cyber crime, we will:		None
			• enhance the UK's law enforcement capabilities and skills at national, regional and local level to identify, pursue, prosecute and deter cyber criminals within the UK and overseas;	6205-1	Enhancing law enforcement capability in national, regional & local levels
			• build a better understanding of the cyber crime business model, so we know where to target interventions in order to have the most disruptive effect on criminal activity. We will use this knowledge to: - make the UK a high-cost, high-risk environment in which to operate by targeting the UK nexus of criminality, and by working with industry to reduce the ability of criminals to exploit UK infrastructure; and - tackle cyber crime upstream, adding friction to the criminal business model by dismantling their infrastructure and financial networks, and wherever possible, bringing offenders to justice.	6205-2	Making UK inefficient cybercrime target based on understanding of cybercrime business model
			• build international partnerships to end the perceived impunity of cyber criminals acting against the UK, by bringing criminals in overseas jurisdictions to justice;	6205-3	International juridical partnership
			• deter individuals from being attracted to, or becoming involved in, cyber crime by building on our early intervention measures;	6205-4	Discouraging individuals being involved in cybercrime
			• enhance collaborations with industry to provide them with proactive intelligence on the threat, and to provide us with the upstream intelligence that they possess, in order to assist with our upstream disruption efforts;	6205-5	Exchanging intelligence with industry
			• develop a new 24/7 reporting and triage capability in Action Fraud, linked to the NCSC, the NCA's National Cyber Crime Unit and the wider law enforcement community, to improve support to victims of cyber crime, to provide a faster response to reported crimes and enhanced protective security advice. A new reporting system will be established to share information in real time across law enforcement on cyber crime and threats;	6205-6	New 24/7 reporting system
			• work with the NCSC and the private sector to reduce vulnerabilities in UK infrastructure that could be exploited at scale by cyber criminals; and	6205-7	Reducing vulnerabilities in infrastructures
			• work with the finance sector to make the UK a more hostile environment for those seeking to monetise stolen credentials, including by disrupting their networks.	6205-8	Making use of stolen credentials difficult in UK
		Measuring success	6.2.6. The Government will measure its success in reducing cyber crime by assessing progress towards the following outcomes:	6206-1	Metrics
			• we have a greater disruptive effect on cyber criminals attacking the UK, with higher numbers of arrests and convictions, and larger numbers of criminal networks dismantled as a result of law enforcement intervention;		None
			• there is improved law enforcement capability, including greater capacity and skills of dedicated specialists and mainstream officers and enhanced law enforcement capability amongst overseas partners;		None
			• there is improved effectiveness and increased scale of early intervention measures dissuades and reforms offenders; and		None
			• there are fewer low-level cyber offences as a result of cyber criminal services being harder to access and less effective.		None
	6.3. COUNTERING HOSTILE FOREIGN ACTORS		6.3.1. We need to bring to bear the full range of government capabilities to counter the threat posed by hostile foreign actors that increasingly threaten our political, economic and military security. Working with international partners will be key to our success, and greater emphasis will be placed on engaging them and working with them to counter the threat. Much of this action will not be in the public domain.		None
			Our investment in sovereign capabilities and partnerships with industry and the private sector will continue to underpin our ability to detect, observe and identify this constantly evolving activity against us.		None

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Objective	6.3.2. We will have strategies, policies and priorities in place for each adversary, to ensure a proactive, well-calibrated and effective approach is taken to counter the threat and in order to drive down the number and severity of cyber incidents in the future.		None
		Our approach	6.3.3. To reduce the cyber threat from hostile foreign actors, we will:		None
			• reinforce the application of international law in cyberspace in addition to promoting the agreement of voluntary, non-binding norms of responsible state behaviour	6303-1	Applying international law in cyberspace
			and the development and implementation of confidence building measures;	6303-2	Confidence building
			• work with international partners, particularly through collective defence, cooperative security, and enhanced deterrence that our membership of NATO affords;	6303-3	Enhancing NATO cooperation
			• identify both the unique and generic aspects of our adversaries' cyber activity;	6303-4	Understanding cyber activity of adversaries
			• generate and explore all available options for deterring and countering this threat, drawing on the full range of government capabilities. We will take full account of other related factors, including country-specific strategies, international cyber priorities, and cyber crime and prosperity objectives;	6303-5	Generating all available options
			• use existing networks and relationships with our key international partners to share information about current and nascent threats, adding value to existing thought and expertise; and	6303-6	Intenational information sharing
			• attribute specific cyber identities publicly when we judge it in the national interest to do so.	6303-7	Attributing specific identities
		Measuring success	6.3.4. The Government will measure its success in countering the actions of hostile foreign actors by assessing progress towards the following outcomes:	6304-1	Metrics
			• the stronger information-sharing networks that we have established with our international partners, and wider multilateral agreements in support of lawful and responsible behaviour by states, are substantially contributing to our ability to understand and respond to the threat, resulting in a better defended UK; and		None
			• our defence and deterrence measures, alongside our country-specific strategies, are making the UK a harder target for hostile foreign actors to act against.		None
	6.4. PREVENTING TERRORISM		6.4.1. The technical capability of terrorists currently remains limited but they continue to aspire to conduct damaging computer network operations against the UK, with publicity and disruption as the primary objective of their cyber activity. The Government will identify and disrupt terrorists using and intending to use cyber for this purpose. In doing so, we will minimise their impact and prevent an uplift in terrorist cyber capability that would further threaten UK networks and national security.		None
		Objective	6.4.2. To mitigate the threat of terrorist use of cyber, through the identification and disruption of terrorist cyber actors who currently hold, and aspire to build, capability that could threaten UK national security.		None
		Our approach	6.4.3. To ensure the threat posed by cyber terrorism remains low, we will:		None
			• detect cyber terrorism threats, identifying actors who are seeking to conduct damaging network operations against the UK and our allies;	6403-1	Enhancing detection of cyber terrorism
			• investigate and disrupt these cyber terrorism actors to prevent them from using cyber capability against the UK and its allies; and	6403-2	Enhancing investigation of cyber terrorism
			• work closely with international partners to enable us to better tackle the threat from cyber terrorism.	6403-3	International cooperation

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Measuring success	6.4.4. The Government will measure its success in preventing terrorism by assessing progress towards the following outcomes:	6404-1	Metrics
			• a full understanding of risk posed by cyber terrorism, through identification and investigation of cyber terrorism threats to the UK; and		None
			• close monitoring, and disruption of terrorist cyber capability at the earliest opportunity, with the aim of preventing an increase in such terrorist capability in the long term.		None
	6.5. ENHANCING SOVEREIGN CAPABILITIES – OFFENSIVE CYBER		6.5.1. Offensive cyber capabilities involve deliberate intrusions into opponents' systems or networks, with the intention of causing damage, disruption or destruction. Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere.		None
			Through our National Offensive Cyber Programme (NOCP), we have a dedicated capability to act in cyberspace and we will commit the resources to develop and improve this capability.		None
		Objective	6.5.2. We will ensure that we have at our disposal appropriate offensive cyber capabilities that can be deployed at a time and place of our choosing, for both deterrence and operational purposes, in accordance with national and international law.		None
		Our approach	6.5.3. To do this, we will:		None
			• invest in our NOCP – the partnership between the Ministry of Defence and GCHQ that is harnessing the skills and talents of both organisations to deliver the tools, techniques and tradecraft required;	6503-1	Enhancing development of cyber HR
			• develop our ability to use offensive cyber tools; and	6503-2	Developing offensive cyber capability
			• develop the ability of our Armed Forces to deploy offensive cyber capabilities as an integrated part of operations, thereby enhancing the overall impact we can achieve through military action.	6503-3	Integrating offensive cyber capability to armed forces
		Measuring success	6.5.4. The Government will measure our success in establishing offensive cyber capabilities by assessing progress towards the following outcomes:	6504-1	Metrics
			• the UK is a world leader in offensive cyber capability; and		None
			• the UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities.		None
	6.6. ENHANCING SOVEREIGN CAPABILITIES – CRYPTOGRAPHY		6.6.1. Cryptographic capability is fundamental to protecting our most sensitive information and to choosing how we deploy our Armed Forces and national security capabilities. To maintain this capability, we will require private sector skills and technologies that are assured by GCHQ. This is likely to require work to be done in the UK, by British Nationals with the requisite security clearance, working for companies who are prepared to be completely open with GCHQ in discussing design and implementation details. The MOD and GCHQ are working to establish a sound understanding of the long-term cost implications of maintaining such sovereign cryptographic capabilities, based on prevailing market conditions and in cooperation with those companies currently able to provide such solutions.		None
		Objective	6.6.2. We have the confidence that the UK will always have political control over those cryptographic capabilities vital to our national security and, therefore, the means to protect UK secrets.		None

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Our approach	6.6.3. We will select the means that allow us to share information effectively with our allies, and ensure that trusted information and information systems are available, when and where required. Working closely with other government departments and agencies, GCHQ and MOD will together define sovereign requirements, and how best to meet those requirements when suppliers must be domestic. This will be delivered through a new joint framework for determining requirements for operational advantage and freedom of action.	6603-1	Creating new requirement of cryptography
		Measuring success	6.6.4. The Government will measure its success in maintaining our cryptographic capabilities by assessing progress towards the following outcome:	6604-1	Metrics
			• our sovereign cryptographic capabilities are effective in keeping our secrets and sensitive information safe from unauthorised disclosure.		None
7. DEVELOP			7.0.1. The DEVELOP strand of the strategy sets out how we will acquire and strengthen the tools and capabilities that the UK needs to protect itself from the cyber threat.		None
			7.0.2. The UK requires more talented and qualified cyber security professionals.		None
			The Government will act now to plug the growing gap between demand and supply for key cyber security roles, and inject renewed vigour into this area of education and training. This is a long-term, transformative objective, and this strategy will kick-start this important work, which will necessarily continue beyond 2021.		None
			A skilled workforce is the lifeblood of a vital and world leading cyber security commercial ecosystem. This ecosystem will ensure cyber start-ups prosper and receive the investment and support they need. This innovation and vigour can only be provided by the private sector; but the Government will act to support its development, and actively promote the wider cyber security sector to the world market. A dynamic and thriving scientific research sector is required to support both the development of highly skilled people, and to ensure that new ideas translate into cutting-edge products.		None
	7.1. STRENGTHENING CYBER SECURITY SKILLS		7.1.1. The UK needs to tackle the systemic issues at the heart of the cyber skills shortage: the lack of young people entering the profession; the shortage of current cyber security specialists; insufficient exposure to cyber and information security concepts in computing courses; a shortage of suitably qualified teachers; and the absence of established career and training pathways into the profession.		None
			7.1.2. This calls for swift intervention by the Government to help address the current shortage and develop a coherent long-term strategy that can build on these interventions to close the skills gap. However, it must be recognised that to have any profound impact, this effort must be collaborative, with input from a range of participants and influencers across the Devolved Administrations, public sector, education providers, academia bodies and industry.		None
		Objective	7.1.3. The Government's ambition is to ensure the sustained supply of the best possible home-grown cyber security talent, whilst funding specific interventions in the short term to help meet known skills gaps.		None
			We will also define and develop the cyber security skills needed across the population and workforce to operate safely and securely online.		None
			7.1.4. This requires action over the next twenty years, not just the next five. We will define the long-term, coordinated set of actions needed by government, industry, education providers and academia to establish a sustained supply of competent cyber security professionals, who meet the requisite standards and certification to practise confidently and securely.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			7.1.5. We will close the skills gap in Defence. We will attract cyber specialists to government who are not only effectively trained but also ready to maintain our national security. This includes an understanding of the impact of cyberspace on military operations.		None
		Our approach	7.1.6. We will develop and implement a self-standing skills strategy that builds on existing work to integrate cyber security into the education system. This will continue to improve the state of computer science teaching overall and embed cyber security into the curriculum. Everyone studying computer science, technology or digital skills will learn the fundamentals of cyber security and will be able to bring those skills into the workforce. As part of this effort, we will address the gender imbalance in cyber-focused professions, and reach people from more diverse backgrounds, to make sure we are drawing from the widest available talent pool. We will work closely with the Devolved Administrations to encourage a consistent approach across the UK.	7106-1	Including cybersecurity into computer science education
			7.1.7. We will set out more clearly the respective roles of government and industry, including how these might evolve over time. The UK Government and Devolved Administrations have a key role in creating the right environment for cyber security skills to be developed and to update the education system to reflect the changing needs of industry and government.	7107-1	Making clear rolls of government & private sector in cybersecurity training
			But employers also have a significant responsibility to clearly articulate their needs, as well as train and develop employees and young people entering the profession.	7107-2	Urging corporate management to train employees
			Industry has an important role in building diverse and attractive career and training pathways in partnership with academia, professional bodies and trade associations.	7107-3	More attractive careers of cybersecurity professionals
			7.1.8. In recognition of the collective challenge we face in closing the skills gap, we will establish a skills advisory group formed of government, employers, professional bodies, skills bodies, education providers and academia, which will strengthen the coherence between these key sectors. This group will support the development of a long-term strategy which will take account of developments in the broad field of digital skills, ensuring that cyber security considerations are aligned and incorporated throughout. This group will work with similar bodies across the UK.	7108-1	Inter-sectoral coordination of education/training

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			7.1.9. Alongside this work, the Government will invest in a range of initiatives to bring about immediate improvements and inform the development of the long-term skills strategy. These include:		None
			• establishing a schools programme to create a step change in specialist cyber security education and training for talented 14-18 year olds (involving classroom-based activities, after-school sessions with expert mentors, challenging projects and summer schools);	7109-1	Specialist education targeting 14-18 years
			• creating higher and degree-level apprenticeships within the energy, finance and transport sectors to address skills gaps in essential areas;	7109-2	Degree-level apprenticeship in energy, finance & transport
			• establishing a fund to retrain candidates already in the workforce who show a high potential for the cyber security profession;	7109-3	Retraining funds
			• identifying and supporting quality cyber graduate and post graduate education, and identifying and filling any specialist skills gaps – acknowledging the key role that universities play in skills development;	7109-4	Supporting high quality post graduate education
			• supporting the accreditation of teacher professional development in cyber security. This work will help teachers, and others supporting learning, to understand cyber security education and provide a method of externally accrediting such individuals;	7109-5	Accredition of teachers
			• developing the cyber security profession, including through achieving Royal Chartered status by 2020, reinforcing the recognised body of cyber security excellence within the industry and providing a focal point which can advise, shape and inform national policy;	7109-6	Identifying excellent organisation
			• developing a Defence Cyber Academy as a centre of excellence for cyber training and exercise across the Ministry of Defence and wider Government, addressing specialist skills and wider education;	7109-7	Defence cyber academy to CoE
			• developing opportunities for collaboration in training and education between government, the Armed Forces, industry and academia, together with facilities to maintain and exercise skills; and	7109-8	Collaborating between government, forces, industry & academia
			• we will work with industry to expand the CyberFirst programme to identify and nurture the diverse young talent pool to defend our national security; and	7109-9	CyberFirst: nurturing young talent programme
			• embedding cyber security and digital skills as an integral an integral part of relevant courses within the education system, from primary to postgraduate levels, setting standards, improving quality and providing a firm foundation for onwards progression into the field.	7109-10	Cybersecurity education from primary to postgraduate
			As education is a devolved matter, some of these initiatives will apply mainly in England. We will however work with the Devolved Administrations to encourage a consistent approach across the UK education systems.		None
		Measuring success	7.1.10. The Government will measure our success in strengthening cyber security skills by assessing progress towards the following outcomes:	7110-1	Metrics
			• there are effective and clear entry routes into the cyber-security profession, which are attractive to a diverse range of people;		None
			• by 2021 cyber security is taught effectively as an integral part of relevant courses from primary to post-graduate level;		None
			• cyber security is widely acknowledged as an established profession with clear career pathways, and has achieved Royal Chartered Status;		None
			• appropriate cyber security knowledge is an integral part of the continual professional development for relevant non-cyber security professionals, across the economy; and		None
			• the Government and the Armed Forces and the Armed Forces have access to cyber specialists able to maintain the security and resilience of the UK.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
	7.2. STIMULATING GROWTH IN THE CYBER SECURITY SECTOR		7.2.1. A burgeoning and innovative cyber security sector is a necessity for our modern, digital economy. UK cyber security firms provide world-leading technologies, training and advice to industry and governments.		None
			But whilst the UK is a leading player, it faces fierce competition to stay ahead. There are also barriers that the Government needs to address. UK companies and academics develop cutting-edge technology, but some require support to develop the commercial and entrepreneurial skills required to thrive.		None
			There are funding gaps that prevent SMEs from growing and expanding into new markets and territories. The most groundbreaking products and services, that offer the potential to keep us ahead of the threat, struggle to find customers who are willing to act as early adopters.		None
			Overcoming these challenges requires government, industry and academia to work effectively together.		None
		Objective	7.2.2. The Government will support the creation of a growing, innovative and thriving cyber security sector in the UK in order to create an ecosystem where:		None
			• security companies prosper, and get the investment they need to grow;		None
			• the best minds from government, academia and the private sector collaborate closely to spur innovation; and		None
			• customers of the Government and industry are sufficiently confident and prepared to adopt cutting-edge services.		None
		Our approach	7.2.3. To create this ecosystem, we will:		None
			• commercialise innovation in academia, providing training and mentoring to academics;	7203-1	Supporting commercialisation of academic innovation
			• establish two innovation centres, to drive the development of cutting-edge cyber products and dynamic new cyber security companies, which will sit at the heart of a programme of initiatives to give start-ups the support they need to get their first customers and attract further investment;	7203-2	Establishing innovation centres
			• allocate a proportion of the £165m Defence and Cyber Innovation Fund to support innovative procurement in defence and security;	7203-3	Allocating funds
			• provide testing facilities for companies to develop their products, together with a fast-track form of assessment for the next generation of cyber security products and services as they emerge, enabling customers to be confident in their use;	7203-4	Providing testing facilities
			• draw on the collective expertise of the industry-government Cyber Growth Partnership to help shape and focus further growth and innovation interventions;	7203-5	Enhancing cooperation between industry & government
			• help companies of all sizes scale-up and access international markets; and	7203-6	Supporting scaling-up
			• promote agreed international standards that support access to the UK market.	7203-7	Promoting international standards for easier market access
			7.2.4. We will also use the weight of government procurement to spur innovation. The Government faces some of the hardest challenges in cyber security, and some of the biggest threats. We can, and must, pursue the most effective solutions to these problems. That means making it easier for smaller companies to do business with government. It also means the Government must be less risk averse in testing and using new products.	7204-1	Easier access to government procurement for start-ups
			This is a win-win solution: the Government will get the best services, and innovative technology will get an early adopter, making it easier to attract investment and a larger customer base. We will encourage all parts of government, including the Devolved Administrations, to take a similar approach.		None

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Measuring success	7.2.5. The Government will measure its success in stimulating growth in the cyber security sector by assessing progress towards the following outcomes:	7205-1	Metrics
			• greater than average global growth in the size of the UK cyber sector year on year;		None
			• a significant increase in investment in early stage companies;		None
			• adoption of more innovative and effective cyber security technologies in government.		None
	7.3. PROMOTING CYBER SECURITY SCIENCE AND TECHNOLOGY		7.3.1. The UK's thriving science and technology sector and its cutting-edge research, underpins our world-leading cyber security capabilities. To maintain and enhance the UK's reputation as a global leader in cutting-edge research, we need our academic research establishments to continue to attract the best and the brightest minds in the field of cyber security. This will require us to foster centres of excellence that attract the most able and dynamic scientists and researchers, and deepen the active partnership between academia, the Government and industry. This will involve a match-making role for the Government, where we incentivise such collaborations.		None
			Success would see us establish a selfsustaining ecosystem that allows ideas – and people – to circulate between the three sectors in a mutually beneficial way.		None
		Objective	7.3.2. By 2021, the UK will have strengthened its position as a world leader in cyber science and technology.		None
			Flexible partnerships between universities and industry will translate research into commercially successful products and services. The UK will maintain its reputation for innovative excellence, including in those areas of exceptional national strength, such as the financial sector.		None
		Our approach	7.3.3. To achieve this, the Government will encourage collaboration, innovative and flexible funding models for research, and the commercialisation of research.	7303-1	Making research funding more effective
			Government will ensure that the human and behavioural aspects of cyber are given sufficient attention, and that systems beyond the technical, such as business processes and organisational structures, are included within cyber science and technology.	7303-2	Human & behavioural aspects of cyber science
			7.3.4. This will underpin the creation of products, systems and services that are 'secure by default', with appropriate security considered from the outset and where security becomes a conscious 'opt-out' for users.	7304-1	Enhancing 'secure-by-default'
			7.3.5. We will publish a detailed Cyber Science and Technology Strategy after a thorough consultation with partners and stakeholders. This will include identifying areas of science and technology that the Government, industry and academia consider to be important and identifying gaps in the UK's current capacity to address them.	7305-1	Establishing Cyber Science and Technology Strategy
			7.3.6. The Government will continue to provide funding and support for the Academic Centres of Excellence, Research Institutes and Centres for Doctoral Training.	7306-1	Supporting academic CoE, research institutes & doctral training
			In addition, we will create a new Research Institute in a strategically important subject area. We will also fund further research in those areas where the upcoming Cyber Science and Technology Strategy identifies capability gaps. Important areas that will be given consideration include: big data analytics; autonomous systems; trustworthy industrial control systems; cyber-physical systems and the Internet of Things; smart cities; automated system verification; and the science of cyber security.	7306-2	Establishing new research institute
			7.3.7. We will continue to sponsor UK national PhD students at the Academic Centres of Excellence to increase the number of UK nationals with cyber expertise.	7307-1	Supporting PhD

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			7.3.8. The Government will work with bodies, including Innovate UK and the Research Councils to encourage collaboration between industry, the Government and academia. To support this collaboration we will review best practice concerning security classifications and identify security-cleared experts, including academics. This will ensure that work from the unclassified space to beyond secret can be as collaborative as possible.	7308-1	Encouraging collaboration between government, industry & academia
			7.3.9. The Government will fund a 'grand challenge' to identify and provide innovative solutions to some of the most pressing problems in cyber security. CyberInvest, a new industry and Government partnership to support cutting-edge cyber security research and protect the UK in cyberspace, will be part of our approach to building the academic-government-industry partnership.	7309-1	Funding 'grand challenge'
		Measuring success	7.3.10. The Government will measure its success in promoting cyber security science and technology by assessing progress towards the following outcomes:	7310-1	Metrics
			• significantly increased numbers of UK companies successfully commercialising academic cyber research and fewer agreed and identified gaps in the UK's cyber security research capability with effective action to close them; and		None
			• the UK is regarded as a global leader in cyber security research and innovation.		None
	7.4. EFFECTIVE HORIZON SCANNING		7.4.1. The Government must ensure that policy-making takes account of the changing cyber, geopolitical and technology landscape. To do this, we need to make effective use of broad horizon scanning and assessment work. We need to invest in proofing ourselves against future threats and anticipate market changes that might affect our cyber resilience in five to ten years' time.		None
			We need horizon scanning programmes that generate recommendations to inform current and future government policy and programme planning.		None
		Objective	7.4.2. The Government will ensure that our horizon scanning programmes include a rigorous assessment of cyber risk, and that this is integrated into cyber security and other technology policy development areas, along with all-source assessment and other available evidence. We will join up horizon scanning between national security and other policy areas to ensure a holistic assessment of emerging challenges and opportunities.		None
		Our approach	7.4.3. We will:		None
			• identify gaps in current work, and coordinate work across disciplinary boundaries to develop a holistic approach to horizon scanning for cyber security;	7403-1	Promoting inter-disciplinary research for development of horizon scanning
			• promote better integration of technical aspects of cyber security with behavioural science;	7403-2	Integration of cybersecurity & behavioural science
			• support rigorous monitoring of the cyber criminal market place to spot new tools and services that might enable technology transfer to hostile states, terrorists or criminals;	7403-3	Monitoring cyber criminal market
			• analyse emergent internet-connected process control technologies;	7403-4	Investigating new technologies
			• anticipate vulnerabilities around digital currencies; and	7403-5	-do-
			• monitor market trends in telecommunications technologies to develop early defences against anticipated future attacks.	7403-6	Early defence technology
			7.4.4. We recognise that horizon scanning goes beyond the technical, to include political, economic, legislative, social and environmental dimensions. Cyber security is just one aspect of the issues that effective horizon scanning can help to address. Therefore, we will ensure that where we conduct horizon scanning of these other policy areas, we will take into account any cyber security implications.	7404-1	Including cybersecurity into any other research areas for horizon scanning

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
			7.4.5. We will also ensure that cyber policy-making follows an evidence-based approach, taking into account assessments from all available sources. This will include, for example:		None
			• specific technical evidence, for example on the Internet of Things, or the future role of advanced materials; and		None
			• international strategic and societal trends and their impact on cyber.		None
			7.4.6. We will ensure that cyber security is considered within the remit of the cross- Government Emerging Technology and Innovation Analysis Cell (ETIAC), which will be established to identify technology threats and opportunities relevant to national security and that cyber is considered by existing horizon-scanning structures, including the Government Futures Group (GFG), and the Cabinet Secretary's Advisory Group on horizon scanning (CSAG).		None
		Measuring success	7.4.7. The Government will measure our success in establishing an effective horizon scanning capability by assessing progress towards the following outcomes:	7407-1	Metrics
			• cross-government horizon scanning and all-source assessment are integrated into cyber policy making; and		None
			• the impact of cyber security is factored into all cross-government horizon scanning.		None
8. INTERNATIONAL ACTION			8.1. Our economic prosperity and social wellbeing increasingly depend on the openness and security of networks that extend beyond our own borders.		None
			It is essential that we work closely with international partners to ensure the continuation of a free, open, peaceful and secure cyberspace that delivers these benefits. This will only become more important as the next billion users come online across the globe.		None
			8.2. International cooperation on cyber issues has become an essential part of wider global economic and security debates. It is a rapidly evolving area of policy, without a single agreed international vision. The UK and its allies have been successful in ensuring some elements of the rules-based international system are in place: there has been agreement that international law applies in cyberspace; that human rights apply online as they do offline; and a broad consensus that the multi-stakeholder approach is the best way to manage the complexities of governing the Internet.		None
			However, with a growing divide over how to address the common challenge of reconciling national security with individual rights and freedoms, any global consensus remains fragile.		None
		Objectives	8.3. The UK aims to safeguard the long-term future of a free, open, peaceful and secure cyberspace, driving economic growth and underpinning the UK's national security. On this basis, the UK will continue to: champion the multi-stakeholder model of internet governance; oppose data localisation; and work to build the capacity of our partners to improve their own cyber security. In order to reduce the threat to the UK and our interests, much of which originates overseas, we will seek to influence the decision-making of those engaging in cyber crime, cyber espionage, and disruptive or destructive cyber activity and continue to build frameworks to support international cooperation.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Our Approach	8.4. To do this we will:		None
			• strengthen and embed a common understanding of responsible state behaviour in cyberspace;	84---1	Contributing to international debate of international law in cyber space
			• build on agreement that international law applies in cyberspace;	84---2	-do-
			• continue to promote the agreement of voluntary, non-binding, norms of responsible state behaviour;	84---3	-do-
			• support the development and implementation of confidence-building measures;	84---4	Confidence building measures
			• increase our ability to disrupt and prosecute cyber criminals based abroad, especially in hard-to-reach jurisdictions;	84---5	Cross-border prosecution
			• help foster an environment which allows our law enforcement agencies to work together to ensure fewer places exist where cyber criminals can act without fear of investigation and prosecution;	84---6	Enhancing law enforcement
			• promote the resilience of cyberspace by shaping the technical standards governing emerging technologies internationally (including encryption), making cyberspace more 'secure by design' and promoting best practice;	84---7	Promoting international standards & best practices in emerging technologies
			• work to build common approaches amongst like-minded countries for capabilities such as strong encryption, which have cross-border implications;	84---8	Cross-border cooperation in capabilities & new technologies
			• build the capacity of others to tackle threats to the UK, and our interests overseas;	84---9	Assist other countries to build capabilities
			• continue to help our partners develop their own cyber security – since we share a single cyberspace, we collectively become stronger when each country improves its own defences;	84---10	Assist other countries to enhance cybersecurity
			• ensure that NATO is prepared for the conflicts of the 21st century, which will play out in cyberspace as well as on the battlefield;	84---11	Enhancing NATO's capability in cyber space
			• work with our allies to enable NATO to operate as effectively in cyberspace as it does on land, air and sea; and	84---12	-do-
			• ensure that the 'London Process' of Global Conferences on Cyberspace continues to promote global consensus towards a free, open, peaceful and secure cyberspace.	84---13	Contributing international norm development in cyber space
			8.5. There are a range of relationships and tools we will continue to invest in to deliver and underpin all our international cyber objectives; we cannot achieve our objectives in isolation. These include:		None
			• working in concert with traditional allies and new partners to establish and maintain strong active political and operational relationships; creating the political conditions to build strong global alliances;	85---1	Enhancing cooperation with allies
			• using our influence with multilateral organisations such as the United Nations, G20, European Union, NATO, OSCE, Council of Europe, the Commonwealth and within the global development community; and	85---2	Contributing to international oganisations
			• building stronger relationships with non-government actors – industry, civil society, academia and the technical community. These actors are crucial in informing and challenging international policy formulation, and strengthening political messages on a wide range of cyber issues. Our world-class academic links provide a neutral, collaborative platform with international partners.	85---3	Cooperating international non-government actors

Appendix D

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection	Objective/Approach/Measuring		#	Action Item
		Measuring Success	8.6. The Government will measure its success in advancing our international interests in cyber by assessing progress towards the following outcomes:	86---1	Metrics
			• enhanced international collaboration reduces cyber threat to the UK and our interest overseas;		None
			• a common understanding of responsible state behaviour in cyberspace;		None
			• international partners have increased their cyber security capability; and		None
			• strengthened international consensus on the benefits of a free, open, peaceful and secure cyberspace.		None
9. METRICS			9.1. Cyber security remains an area of relative immaturity when it comes to the measurement of outcomes and impacts – normally referred to as metrics. Already the science of cyber security has been obscured by hyperbole and obstructed by an absence of calibrated data. This is a source of frustration for policy-makers and businesses alike, who have struggled to measure investment against outcomes.		None
			The Government assesses that the effective use of metrics is essential for delivering this strategy and focussing the resources that underpin it.		None
			9.2. We will ensure that this strategy is founded upon a rigorous and comprehensive set of metrics against which we measure progress towards the outcomes we need to achieve. As well as being a major deliverable under the Strategy in its own right, the NCSC will play a crucial role in enabling other parts of Government, industry and society to deliver all of these strategic outcomes within this strategy.		None

National Cyber Security Strategy 2016 - 2023				Itemised	
Section	Subsection		Objective/Approach/Measuring	#	Action Item
			9.3. Annex 3 sets out how the success measures set out in the strategy will contribute to the strategic outcomes, which will be reviewed annually to ensure they accurately reflect our national goals and requirements. The headline, strategic outcomes are as follows:		None
			1. The UK has the capability effectively to detect investigate and counter the threat from the cyber activities of our adversaries.		None
			2. The impact of cybercrime on the UK and its interests is significantly reduced and cyber criminals are deterred from targeting the UK.		None
			3. The UK has the capability to manage and respond effectively to cyber incidents to reduce the harm they cause to the UK and counter cyber adversaries.		None
			4. Our partnerships with industry on active cyber defence mean that large scale phishing and malware attacks are no longer effective.		None
			5. The UK is more secure as a result of technology products and services having cyber security designed into them and activated by default.		None
			6. Government networks and services will be as secure as possible from the moment of their first implementation. The public will be able to use government digital services with confidence and trust that their information is safe.		None
			7. All organisations in the UK, large and small, are effectively managing their cyber risk and are supported by high quality advice designed by the NCSC, underpinned by the right mix of regulation and incentives.		None
			8. There is the right ecosystem in the UK to develop and sustain a cyber security sector that can meet our national security demands.		None
			9. The UK has a sustainable supply of home grown cyber skilled professionals to meet the growing demands of an increasingly digital economy, in both the public and private sectors, and defence.		None
			10. The UK is universally acknowledged as a global leader in cyber security research and development, underpinned by high levels of expertise in UK industry and academia.		None
			11. The UK government is already planning and preparing for policy implementation in advance of future technologies and threats and is ‘future proofed’.		None
			12. The threat to the UK and our interests overseas is reduced due to increased international consensus and capability towards responsible state behaviour in a free, open, peaceful and secure cyberspace.		None
			13. UK Government policies, organisations and structures are simplified to maximise the coherence and effectiveness of the UK’s response to the cyber threat.		None
			9.4. We recognise that some of our ambitions for this strategy go beyond its five year timescale. In order that any future investment in cyber beyond 2021 can continue to deliver the maximum transformative effect, we intend that these longer term outcomes are allocated beyond 2021 to industry, regulators, auditors, insurers and other parts of the public and private sector, as the effective management of cyber security risks is integrated into standard management activity for all.		None

Appendix E Japanese Action Items Allocated to Tentative ANC3T

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-111a	Promoting 'Security-by-Design' in new business harnessing IoT systems.	511L2-4	512L1-2	513L3-1			Promotion of use of standards & best practices
7-112a	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.	511L2-4	512L1-2	513L3-1			Promotion of use of standards & best practices
7-112a2	Promoting secure IoT systems based on "General Framework for Secure IoT Systems".	511L2-4					Promotion of use of standards & best practices
7-112b	Considering measures to exterminate 'bot-net'.	221L2-2	521L2-1	541L2-1			Promotion of online trust established
7-113a	Promoting "IoT Security Guidelines".	511L2-4					Promotion of use of standards & best practices
7-113a2	Promoting "IoT Security Guidelines" as international standard.	511L3-3					Contributing to international standards
7-113b	Promoting "EDSA certification" (security certification for control systems).	133L3-1	511L2-4				Cybersecurity oriented risk management in CI
7-113c	Analysing open source information & warning organisations of vulnerable systems.	122L4-2	131L3-2	132L2-1			Early warning capability
7-113d	Continuing operation of reporting & dissemination system for vulnerability information.	571L3-1	571L3-2				Established responsible disclosure processes
7-114a	Researching innovative & advanced technologies.	321L2-5	322L2-2				Research & development in cybersecurity promoted
7-114b	Researching technologies for security countermeasures for IoTs.	541L3-2					Regular review of technical security controls
7-114c	Developing technologies of threat analysis & risk evaluation for control systems.	133L3-1	511L2-1				Cybersecurity oriented risk management in CI
7-114d	Researching & developing technologies for automotive security in "SIP: Cross-ministerial Strategic Innovation Promotion Program".	133L3-1	511L2-1	541L3-2			Cybersecurity oriented risk management in CI
7-114e	Promoting countermeasures against vulnerable IoT products in the market based on "Policy for IoT Security Countermeasures ver.1.0".	213L3-1	221L2-2	221L3-1			Most users have mind-set
7-121a	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of Cybersecurity for Corporate Management".	311L3-2	312L3-1	511L2-3	511L2-4	511L2-5	Metrics for effectiveness of awareness raising programmes
7-121b	Promoting "Cybersecurity Management Guidelines".	212L3-1	312L3-1	511L2-1			Mind-set spread in private sector
7-121c	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring them in national tenders.	312L3-1	511L2-1	512L3-1	562L2-1		Executives' understandings of cybersecurity measures
7-122a	Promoting human resources development for each category - board members, bridge personnel & working-level - based on "Cybersecurity Human Resources Development Program".	312L3-1	312L3-3	331L2-4	331L3-2	331L3-3	Executives' understandings of cybersecurity measures
7-123a	Promoting 'Security-by-Design'.	511L2-4	512L1-2	513L3-1			Promotion of use of standards & best practices
7-123b	same as 7-121c2						
7-123b2	Promoting "Cybersecurity Management Guidelines" to SMEs (small-to medium-sized enterprises).	212L4-1	312L3-1	511L2-2			Mind-set commonplace in private sector
7-123c	Reviewing rules & regulations so as to improve security of whole supply chains of IT development & operation.	513L3-1	513L4-2				Security consideration in all stages
7-123d	Encouraging corporates to establish CSIRT.	212L3-2	312L3-3				Mind-set based strategy in private sector
7-123e	Performing practical cyber defence exercise "CYDER" at "National Cyber Training Center".	124L4-1	141L3-1				Scenario testing of incident response processes
7-123e2	Performing cyber exercises assuming attacks against Tokyo Olympics/Paralympics in 2020, employing large scale exercise environment "Cyber Colosseo".	124L4-1	141L3-1				Scenario testing of incident response processes
7-123f	Performing practical APT exercises.	141L3-1					High-level scenario of national incident exercise
7-123g	Enhancing "J-CRAT: Cyber Rescue Team" (activity to assist organisational incident responses).	123L3-1					Subnational / sectorial incident response organisations
7-123h	Performing financial industry-wide cyber exercises.	141L3-1					High-level scenario of national incident exercise
7-123i	Promoting "iLogScanner: Attack Indication Detecting Tool for Websites".	221L2-2	521L2-1				Promotion of online trust established
7-123j	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".	132L2-1	132L2-2	132L2-3	132L2-4	153L2-2	Information sharing established between CI & government
7-123k	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-ISAC).	132L2-1	132L2-2	132L2-3	431L3-3		Information sharing established between CI & government
7-123l	Enhancing "Financial ISAC Japan".	132L2-1	132L2-2	132L2-3	431L3-3		Information sharing established between CI & government

Allocation (Requirement Keyword)			
2	3	4	5
Promotion of use of standards & best practices for procurement	Security consideration in all stages		
Promotion of use of standards & best practices for procurement	Security consideration in all stages		
Reliable internet infrastructures	Latest technical controls & patch managements widely implemented		
Promotion of use of standards & best practices			
Vulnerability & asset management of CI assets	Information sharing established between CI & government		
Analysis & dissemination processes			
Budget for research & education for cybersecurity			
Established standards & best practices			
Established standards & best practices	Regular review of technical security controls		
Promotion of online trust established	Most users can use internet securely		
Executives' understandings of cybersecurity measures	Metrics of adoption of standards & best practices	Promotion of use of standards & best practices	Metrics of compliance of standards & best practices
Executives' understandings of cybersecurity measures	Established standards & best practices		
Established standards & best practices	Standards & best practices for procurement widely used & complied	Established cybersecurity insurance market	
Executives' understanding of crisis management plans	Cybersecurity training programmes for non-professionals	Cybersecurity training aligned with national strategy	Communication skills in cybersecurity training
Promotion of use of standards & best practices for procurement	Security consideration in all stages		
Executives' understandings of cybersecurity measures	Standards & best practices widely used		
Adopting standards throughout life-time			
Executives' understanding of crisis management plans			
High-level scenario of national incident exercise			
High-level scenario of national incident exercise			
Reliable internet infrastructures			
Formal & consistent information sharing between CI & government	Point of contact	Government engagement in CI protection	Intelligence sharing between CI & defence
Formal & consistent information sharing between CI & government	Point of contact	Resources for information exchange between public & private sectors	
Formal & consistent information sharing between CI & government	Point of contact	Resources for information exchange between public & private sectors	

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-131a	Cultivating cybersecurity-related business to a growth industry by establishing certification for security services.	561L2-1	561L2-2				Domestic providers of security products
7-131b	Promoting "Cloud Security Guidelines" & "Cloud Audit System".	511L2-1	561L3-1				Established standards & best practices
7-131c	Promoting security investment of SMEs (small-to medium-sized enterprises).	312L3-1	511L2-2	511L2-4	541L2-1	541L2-2	Executives' understandings of cybersecurity measures
7-131d	Reconsidering "Copyright Act" about reverse engineering for security purposes.	121L4-1	124L3-2				Adapted analysis of incidents
7-132a	Continuing "Public & Private Sectors Forum for Trade Secret" to share information about information exfiltration.	311L2-1	431L1-2				National programme of awareness raising
7-132b	Promoting "Handbook for Confidential Information Protection" & "Guide for Handbook for Confidential Information Protection".	511L2-1	511L2-4				Established standards & best practices
7-132c	Promoting guidelines for deterrence/prevention of internal misconduct within organisations.	511L2-1	511L2-4				Established standards & best practices
7-132d	Communicating & negotiating with countries who apply 'Forced Localization Measures'.	521L4-2					Optimised cost for internet infrastructures
7-133a	Supporting international standardization in security through participation to ISO/IEC JTC1/SC27, ITU-T SG17 etc.	511L3-3					Contributing to international standards
7-133b	Supporting international standardization in cryptography, certification for cryptograph & security products.	412L4-4	511L3-3	551L4-1	551L4-2		Contributing to international privacy protection online
7-133c	Supporting international standardization in vulnerability management like SCAP, CVSS etc.	511L3-3	571L4-2				Contributing to international standards
7-133d	Supporting international standardization in security evaluation like PP (Protection Profile) etc.	511L3-3					Contributing to international standards
7-133e	Assisting ITPEC (IT Professionals Examination Council: organisation for a common IT examination in Asian countries) by 'exporting' "Japan Information-Technology Engineers Examination".	311L3-4	322L3-3	332L4-1			Contribution to international awareness raising
7-133f	Assisting security management in ASEAN countries.	311L3-4					Contribution to international awareness raising
7-133g	Assisting establishment of 'secure development' in countries where Japanese corporates outsource software development.	311L3-4	513L1-3	513L2-2	513L3-1	541L2-5	Contribution to international awareness raising
7-133h	Researching international standards & evaluation system for IoT systems.	133L3-1	511L3-3				Cybersecurity oriented risk management in CI
7-211a	Same as 7-123b						
7-211b	Promoting 'Security-by-Design' in IoT & embedded systems.	511L2-4	512L1-2	513L3-1			Promotion of use of standards & best practices
7-211c	Promoting "How to Secure Your Web Site".	223L2-4	223L2-4	513L1-3	513L2-2	541L2-5	Promotion of trust of e-commerce
7-211c2	Promoting "AppGoat" (training tool for secure development).	513L1-3	513L2-2	541L2-5			Coding standards
7-211d	Researching technologies for securer development & more sophisticated evaluation.	513L2-2	541L2-5	541L3-2			Education & training for development
7-211d2	Same as 7-113a3						
7-211d3	Same as 7-113a4						
7-211e	Same as 7-113h						
7-211f	Supporting vulnerability management in organisations, by promoting structured languages for vulnerability information.	541L2-1					Latest technical controls & patch managements widely implemented
7-211g	Promoting 'fuzz testing' for pro-active vulnerability detection.	571L2-1					Established vulnerability disclosure framework
7-211h	Upgrading "NICTER: Network Incident Analysis Center for Tactical Emergency Response".	122L4-2					Early warning capability
7-211i	Continuing operation of "ACTIVE: Advanced Cyber Threat Response Initiative" (assistance for users to disinfect malwares from compromised PCs).	221L2-2	221L2-3				Promotion of online trust established
7-211j	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point observation system).	122L4-2	123L4-2	124L4-4	431L2-1		Early warning capability
7-211k	Continuing operation of "Council of Anti-Phishing Japan".	221L2-2	431L3-3				Promotion of online trust established
7-211l	Promoting "icat: IPA Cyber Security Alert Service".	221L2-2	541L2-1				Promotion of online trust established
7-211m	Urging public Wi-Fi service providers to prevent cybercrime & to enable effective tracking back.	221L2-2	432L2-2	541L2-4			Promotion of online trust established
7-211n	Initiating Wi-Fi service providers & users to safer communication.	213L2-1	221L2-1	221L2-2	541L2-4		Growing number of users have mind-set
7-211o	Considering development of intelligence sharing platform for government & private sectors.	132L2-1	132L2-2	153L2-2	431L3-3		Information sharing established between CI & government

Allocation (Requirement Keyword)			
2	3	4	5
Lowering dependency on foreign cybersecurity technologies			
Security products complied to International standards			
Standards & best practices widely used	Promotion of use of standards & best practices	Latest technical controls & patch managements widely implemented	Anti-malware softwares & network firewalls
Sophisticated incident analysis			
Exchange of information between public & private sectors about cybercrimes			
Promotion of use of standards & best practices			
Promotion of use of standards & best practices			
Contributing to international standards	Regular review of relevance of cryptographic controls	Revision of cryptographic control policies	
Internationally contributing to responsible disclosure			
International cooperation in cybersecurity education	Cybersecurity trained professionals internationally contributing		
Coding standards	Education & training for development	Security consideration in all stages	Technical security controls based on international frameworks
Contributing to international standards			
Promotion of use of standards & best practices for procurement	Security consideration in all stages		
Promotion of trust of e-commerce	Coding standards	Education & training for development	Technical security controls based on international frameworks
Education & training for development	Technical security controls based on international frameworks		
Technical security controls based on international frameworks	Regular review of technical security controls		
User assistance available			
Regional coordination	Regional coordination	Established formal international cooperation	
Resources for information exchange between public & private sectors			
Latest technical controls & patch managements widely implemented			
Established informal cooperation between ISPs & law enforcement	Established ISPs' policies of technical security control		
Growing number of users can use internet securely	Promotion of online trust established	Established ISPs' policies of technical security control	
Formal & consistent information sharing between CI & government	Intelligence sharing between CI & defence	Resources for information exchange between public & private sectors	

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-212a	Initiating users to security in cyber space.	213L2-1	221L2-1				Growing number of users have mind-set
7-212b	Initiating users to secure use of internet, protection from cybercrimes, latest criminal techniques & safety on smartphones.	213L2-1	221L2-1	221L3-2	231L2-1		Growing number of users have mind-set
7-212b2	Initiating educators & staff of local public entities to elimination of cyber environment that is harmful to youth.	213L3-1	221L3-1	251L3-2			Most users have mind-set
7-212c	Promoting use of electronic signature.	221L2-2	551L2-1	551L2-2			Promotion of online trust established
7-212d	Initiating youth to secure use of internet & smartphones.	213L3-1	221L3-1	221L3-2	251L3-2		Most users have mind-set
7-212e	Continuing moral education for information usage at school.	213L3-1	221L3-1				Most users have mind-set
7-212f	Continuing promotion of moral education for internet usage.	221L3-2	251L3-2				Users' ability to control providing personal information
7-212g	Promoting "Information Leakage Prevention Tool" (tool to prevent data exfiltration through file sharing softwares).	231L2-1					Growing number of users can secure personal information online
7-212h	Arousing security awareness of youth.	213L3-1					Most users have mind-set
7-212i	Assisting local public entities to raise public awareness of security.	213L2-1	221L2-1				Growing number of users have mind-set
7-212j	Continuing "Safety Class" to raise public awareness of secure internet usage.	213L3-1	221L3-1	221L3-2	231L2-1		Most users have mind-set
7-212k	Assisting local public entities to raise public awareness of security.	213L2-1	221L2-1				Growing number of users have mind-set
7-212l	Supporting SMEs (small-to medium-sized enterprises) to enhance security by training security personnel in SMEs & counsellors for SMEs.	212L3-1					Mind-set spread in private sector
7-212m	Providing public & SMEs (small-to medium-sized enterprises) with intelligence of security incidents & countermeasures.	123L3-3	541L2-1				Information sharing across sectors
7-212n	Supporting incident response of public & SMEs (small-to medium-sized enterprises) through "Information Security Consultation Counter" & "APT Special Consultation Counter".	123L3-1	241L2-2				Subnational / sectorial incident response organisations
7-212o	Collecting, analysing & reporting cybersecurity information.	123L3-3					Information sharing across sectors
7-212p	Urging universities to enhance information security.	212L3-1					Mind-set spread in private sector
7-212q	Taking course of action to implement newly effected "Amended Act on the Protection of Personal Information".	412L3-1					Cybersecurity legal framework aligned with international best practices
7-213a	Strengthening capability of investigation of cybercrime.	421L3-2	421L3-3				Advanced investigative capabilities for cybercrimes
7-213b	Enhancing cooperation between public, private & academic sectors, with "JC3: Japan Cybercrime Control Center" (Japanese version of NCFTA (National Cyber-Forensics & Training Alliance) playing the central role.	421L3-5	431L3-3				Statistics & analysis of cybercrime investigations
7-213c	Strengthening capability of investigation of unauthorized access, phishing & illegal acquisition/retention of third party IDs.	421L3-2	431L2-3	431L3-3			Advanced investigative capabilities for cybercrimes
7-213c2	Providing corporates with intelligence of latest criminal techniques, etc.	431L3-3					Resources for information exchange between public & private sectors
7-213d	Supporting establishment of anti-cybercrime voluntary corps.	213L2-1	221L2-1	221L2-2			Growing number of users have mind-set
7-213e	Strengthening capability of investigation of crimes targeting smartphone users.	421L3-2	431L1-2				Advanced investigative capabilities for cybercrimes
7-213f	Training investigators specialized in cybercrime.	421L4-1					Specialised and continuous training for law enforcement officers
7-213g	Collecting & disseminating information about phishing through operation of "Council of Anti-Phishing Japan".	221L2-2	431L3-3				Promotion of online trust established
7-213h	Making the most of High-Tech Crime Technology Division to tackle complicated & diversified cybercrimes.	421L4-2					Sophisticated digital forensic tools
7-213i	Training prosecutors for cybercrimes.	422L4-3					Specialised and continuous training for prosecutors
7-213j	Taking a course of action against cybercrimes upon effectuation of "Cyber Criminal Law".	417L3-1	418L3-2				Exceeding minimum requirement in international agreements on cybercrime
7-213k	Promoting "Guidelines Regarding the Protection of Personal Information in the Telecommunications Business".	432L2-2					Established informal cooperation between ISPs & law enforcement
7-213k2	Enhancing capabilities to analyse IoTs.	421L3-2	421L4-2				Advanced investigative capabilities for cybercrimes

Allocation (Requirement Keyword)			
2	3	4	5
Growing number of users can use internet securely			
Growing number of users can use internet securely	Users' ability to control providing personal information	Growing number of users can secure personal information online	
Most users can use internet securely	Frequent discussion on social media security		
Cryptographic controls widely used	Secure communication services		
Most users can use internet securely	Users' ability to control providing personal information	Frequent discussion on social media security	
Most users can use internet securely			
Frequent discussion on social media security			
Growing number of users can use internet securely			
Most users can use internet securely	Users' ability to control providing personal information	Growing number of users can secure personal information online	
Growing number of users can use internet securely			
Latest technical controls & patch managements widely implemented			
Promotion of incident reporting channels			
Regular training for law enforcement officers			
Resources for information exchange between public & private sectors			
Legislative requirements on information exchange between public & private sectors	Resources for information exchange between public & private sectors		
Growing number of users can use internet securely	Promotion of online trust established		
Exchange of information between public & private sectors about cybercrimes			
Resources for information exchange between public & private sectors			
Exceeding minimum requirement in international agreements on cybercrime			
Sophisticated digital forensic tools			

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-220a	N/A Promoting 5 action plans (specified below) based on "The Basic Policy of Critical Information Infrastructure Protection (3rd Edition)".						
7-220b	Considering & preparing for legislation of security countermeasures for CIIs.	133L3-1	411L3-1				Cybersecurity oriented risk management in CI
7-220b2	Monitoring & publishing improvement of security standards annually.	131L4-1	133L4-1	511L4-1			Regular review of CI risk priorities
7-220c	Improving security standards for CIIs including risk assessment, functionality assurance, BCPs & internal audit.	131L3-2	131L4-1	132L4-1	133L4-1		Vulnerability & asset management of CI assets
7-220c2	Researching for development of information sharing platform for CIIs.	132L2-2					Formal & consistent information sharing between CI & government
7-220d	Improving countermeasures against interference in critical wireless communication.	133L2-2					Risk management processes in CI
7-220e	Improving stability of telecommunication by analysing incidents in telecommunication.	133L2-2					Risk management processes in CI
7-220f	Improving incident response ability of CII operators by performing cross-sectional exercises.	133L2-3	141L2-1	141L2-2	141L2-3		National CI incident response plan
7-220f2	Performing practical cyber defence exercise "CYDER" for CIIs at "National Cyber Training Center".	133L3-1	141L3-1				Cybersecurity oriented risk management in CI
7-220f3	Performing practical cyber defence exercises with CII operators.	133L3-1	141L3-1				Cybersecurity oriented risk management in CI
7-220f4	Performing cyber defence exercises in financial services sector.	133L3-1	141L3-1				Cybersecurity oriented risk management in CI
7-220g	Establishing "ICSCoE: Industrial Cyber Security Center of Excellence".	133L3-1	322L3-4				Cybersecurity oriented risk management in CI
7-221a	Extending action plans based on "The Basic Policy of Critical Information Infrastructure Protection (4th Edition)" to SMEs (small-to medium-sized enterprises).	132L3-3	511L2-6				Supply chain management of CI
7-222a	Enhancing information sharing mechanism for CIIs specifically; Considering introduction of severity grades for service failure. Diversifying communication method. Establishing information sharing platform.	132L2-1	133L3-2	161L3-1			Information sharing established between CI & government
7-222b	Increasing participants & enhancing shared information of "J-CSIP: Cyber Intelligence Sharing Initiative".	132L2-2					Formal & consistent information sharing between CI & government
7-222c	Assisting CII operators to respond cyber attacks from abroad.	132L2-2	132L2-4				Formal & consistent information sharing between CI & government
7-222d	N/A Intra-government cooperation.						
7-222e	Enhancing analysis of targeted attacks by using proving environment simulating large scale LAN.	121L3-2					Incident analysis
7-222f	Enhancing information gathering & analysis on cyber attacks & malwares.	431L3-3					Resources for information exchange between public & private sectors
7-222f2	Enhancing information gathering on cyber attacks.	431L3-3					Resources for information exchange between public & private sectors
7-222f3	Enhancing information sharing & cooperation with CII operators.	132L2-1					Information sharing established between CI & government
7-222f4	Enhancing information sharing with CII operators through "Cyber Terrorism Council".	132L2-1					Information sharing established between CI & government
7-222g	Enhancing security countermeasures of credit card settlement system.	133L3-1	541L3-2				Cybersecurity oriented risk management in CI
7-223a	Supporting local public entities for their cybersecurity.	211L3-1	211L3-2				Mind-set spread in public sector
7-223b	Supporting local public entities to educate & train their personnel for security by holding seminars & e-learning.	211L3-1					Mind-set spread in public sector
7-223b2	Supporting local public entities to revise security policies.	211L3-2					Mind-set based strategy in public sector
7-223c	Providing local public entities with intelligence of security incidents & countermeasures through "LGWAN: Local Government Wide Area Network".	123L3-1	123L3-3				Subnational / sectorial incident response organisations
7-223d	Providing local public entities with services of vulnerability scanning & malware detection.	541L2-1					Latest technical controls & patch managements widely implemented
7-223d2	Providing local public entities with tools for incident response exercises.	141L2-1					National incident exercise done
7-223e	Establishing integrated cybersecurity network monitoring for government & local public entities.	123L3-1	541L2-1				Subnational / sectorial incident response organisations
7-223e2	Supporting local public entities to enhance cybersecurity of their ICTs & to establish cloud network with FY2017 budget.	123L3-1	541L2-1				Subnational / sectorial incident response organisations

Allocation (Requirement Keyword)			
2	3	4	5
Regular review of cybersecurity legal framework			
Regular audit of CI	Regular review of adoption of standards & best practices		
Regular review of CI risk priorities	Ability to adjust of CI protection	Regular audit of CI	
National incident exercise done	Appropriate resources for national incident exercise	Roles in national incident exercise defined	
High-level scenario of national incident exercise			
High-level scenario of national incident exercise			
High-level scenario of national incident exercise			
CoE in cybersecurity			
Standards & best practices used by CI supply chains			
Regular review of impact analysis of CI	Redundant communications for key stakeholders		
Government engagement in CI protection			
Regular review of technical security controls			
Mind-set based strategy in public sector			
Information sharing across sectors			
Latest technical controls & patch managements widely implemented			
Latest technical controls & patch managements widely implemented			

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-223e3	Urging local public entities to isolate "My Number" (Japanese version of Social Security Number) related systems/networks from internet.	222L3-2	541L2-1				Privacy-by-default in e-gov
7-223e4	Urging local public entities to comply with "Guidelines for Proper Handling of Specific Personal Information".	222L3-2					Privacy-by-default in e-gov
7-223f	Promoting collaboration of public & private sectors on authentication using "My Number Portal".	222L3-2					Privacy-by-default in e-gov
7-223g	Incorporating vulnerability information for control systems into existing operation of reporting & dissemination system for vulnerability information.	133L3-1	571L2-1	571L2-2			Cybersecurity oriented risk management in CI
7-223h	Performing practical exercises for control systems of CIIs.	133L3-1	141L3-1				Cybersecurity oriented risk management in CI
7-223i	Promoting security assessment & certification for control systems.	133L3-1	511L2-4	511L2-5			Cybersecurity oriented risk management in CI
7-230a	Preparing for next revision of "Common Standards Group for Information Security Measures for Government Agencies and Related Agencies".	111L4-1	113L4-1	511L4-1			Continual revision of strategy
7-231a	Monitoring & analysing ICT networks of government agencies @24/7.	541L2-1					Latest technical controls & patch managements widely implemented
7-231b	Strengthening incident response capabilities of government agencies by enhancing cooperation between CSIRT of public organisations.	122L3-2	123L3-1	123L3-3			Adequate resources for incident response
7-231c	Urging government agencies to adopt 'security by design' in procurement.	511L2-4	512L1-2	513L3-1			Promotion of use of standards & best practices
7-231c2	Urging government agencies to consider security upon utilisation of cloud network.	513L3-1					Security consideration in all stages
7-231d	Reviewing "List of Requirements for Ensuring Security in Procurement of IT Products".	512L3-2					Regular review of procurement
7-231d2	Disseminating information including PP (protection profiles) to procurement professionals of government agencies.	512L3-1	512L3-2				Standards & best practices for procurement widely used & complied
7-231e	Reviewing & promoting "JISEC: Japan Information Technology Security and Certification Scheme".	512L3-1	512L3-2				Standards & best practices for procurement widely used & complied
7-231f	Promoting "JCMVP: Japan Cryptographic Module Validation Program".	512L3-1	512L3-2	551L3-2			Standards & best practices for procurement widely used & complied
7-231g	Performing penetration testing to ICT systems of government agencies.	541L2-1	541L3-1				Latest technical controls & patch managements widely implemented
7-231h	Performing vulnerability scanning & examining cybersecurity measures of government agencies.	541L2-1	541L3-1				Latest technical controls & patch managements widely implemented
7-231i	Speeding up detecting & informing incidents to government agencies by enhancing GSOC censors/systems. Considering next generation system of GSOC.	124L3-2					Sophisticated incident analysis
7-231j	Reviewing policies for obtaining & storing ICT systems logs to enhance incident response capabilities.	124L3-2	124L3-4				Sophisticated incident analysis
7-231k	Examining CSIRT of government agencies & urging them to enhance incident response capabilities.	123L3-1	124L2-2	124L3-3			Subnational / sectorial incident response organisations
7-231l	Performing cybersecurity exercises for incident response personnel of government agencies.	123L3-1	124L2-2	124L3-3			Subnational / sectorial incident response organisations
7-231l2	Performing cybersecurity exercises for CYMAT members.	123L3-1	124L2-2	124L3-3			Subnational / sectorial incident response organisations
7-231l3	Performing practical cyber defence exercise "CYDER" for government agencies with "National Cyber Training Center".	141L3-1					High-level scenario of national incident exercise
7-231l4	Performing "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).	124L3-1	331L3-2				Training & accreditation for CSIRT members established
7-231m	Sharing cybersecurity intelligence with national universities.	431L1-2					Exchange of information between public & private sectors about cybercrimes
7-231m2	Supporting national universities to enhance cybersecurity by training security personnel.	311L3-1	331L2-4				Sector specific programmes of awareness raising
7-231n	Considering to enhance "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).	124L3-1	331L3-2				Training & accreditation for CSIRT members established
7-231o	Training digital forensics professionals.	124L3-2	124L3-4	331L3-2			Sophisticated incident analysis
7-231p	Promoting "Guidelines for Risk Assessment of Advanced Cyber Attacks Measurements".	511L2-4	541L3-2				Promotion of use of standards & best practices
7-232a	Performing audit of all government agencies & related agencies during 2 years based on "Common Standards Group for Information Security Measures for Government Agencies and Related Agencies".	123L3-1	511L2-5	541L3-2			Subnational / sectorial incident response organisations

Allocation (Requirement Keyword)			
2	3	4	5
Latest technical controls & patch managements widely implemented			
Established vulnerability disclosure framework	Established processes against vulnerability information		
High-level scenario of national incident exercise			
Promotion of use of standards & best practices	Metrics of compliance of standards & best practices		
Continual revision of strategy	Regular review of adoption of standards & best practices		
Subnational / sectorial incident response organisations	Information sharing across sectors		
Promotion of use of standards & best practices for procurement	Security consideration in all stages		
Regular review of procurement			
Regular review of procurement			
Regular review of procurement	Regular review of cryptographic control policies		
User side security controls			
User side security controls			
Forensics			
Regular training for CSIRT members	Regular review of incident response processes		
Regular training for CSIRT members	Regular review of incident response processes		
Regular training for CSIRT members	Regular review of incident response processes		
Cybersecurity training aligned with national strategy			
Cybersecurity training programmes for non-professionals			
Cybersecurity training aligned with national strategy			
Forensics	Cybersecurity training aligned with national strategy		
Regular review of technical security controls			
Metrics of compliance of standards & best practices	Regular review of technical security controls		

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-232b	Training cybersecurity personnel & experts based on "General Policy for Cybersecurity Human Resources Development". Each government agency establishes own plan for build security & IT human resources.	123L3-1	124L2-2	331L3-2			Subnational / sectorial incident response organisations
7-232c	Continuing information sharing in cybersecurity community across government.	123L3-1					Subnational / sectorial incident response organisations
7-232d	Supporting government agencies to develop cybersecurity human resources by training non-security personnel & providing with educational materials.	123L3-1	211L2-1	331L2-4			Subnational / sectorial incident response organisations
7-232e	Reviewing & reconstructing education & training systems for IT human resources.	124L4-2	331L3-4	332L3-1			Evaluating effectiveness of CSIRT members training
7-233a	Researching & developing security measures for cloud services, standardising if necessary.	511L2-1	541L2-1				Established standards & best practices
7-233b	Promoting 'security-by-design' in obtainment of new ICT systems for administrative operation.	512L1-2	513L1-2	513L3-1			Promotion of use of standards & best practices for procurement
7-234a	Performing audit of related agencies (besides government agencies) on cybersecurity.	511L2-5	541L1-2	541L3-2			Metrics of compliance of standards & best practices
7-310a	Performing initial response exercises in preparation for potential large-scale cyber attack.	141L2-1					National incident exercise done
7-310b	Enhancing resources for collection & analysis of cyber attack intelligence from homeland & abroad.	153L3-1					Analytical capability in cyber defence
7-311a	Enhancing counter-intelligence capabilities.				**Not allocated**		
7-311b	N/A Not referring to specific action plans.						
7-311c	Enhancing capability of Cyber Force Center by performing exercises & upgrading monitoring equipment.	124L3-2	421L3-2				Sophisticated incident analysis
7-311c2	Performing cybersecurity exercises for large-scale industrial control systems.	133L3-1	141L3-1				Cybersecurity oriented risk management in CI
7-311c3	Enhancing analytic capabilities of malwares.	421L3-2					Advanced investigative capabilities for cybercrimes
7-311d	Considering education & training of highly professional human resources.	331L3-2					Cybersecurity training aligned with national strategy
7-311e	Enhancing protection & analysis equipment & cyber intelligence collection equipment.	153L3-1					Analytical capability in cyber defence
7-311e2	Enhancing security of "DII: Defense Information Infrastructure".	161L3-1					Redundant communications for key stakeholders
7-311f	Performing practical exercises on environment simulating defence information systems.	141L3-1	161L3-1				High-level scenario of national incident exercise
7-311g	Training CSIRT members for response against highly advanced attacks.	124L3-1	331L3-2				Training & accreditation for CSIRT members established
7-311h	Preparing for penetration testing of defence information network.	161L3-1					Redundant communications for key stakeholders
7-311i	Researching contingency operation of defence information infrastructures.	161L3-1	161L4-1				Redundant communications for key stakeholders
7-312a	Implementing cybersecurity measures of supply chains of defence equipment.	132L3-3	511L2-6				Supply chain management of CI
7-312b	Backing-up National Research and Development Agencies with leading technologies especially in information security area.	321L2-5	322L3-4				Research & development in cybersecurity promoted
7-312b2	Supporting universities with leading technologies to enhance countermeasures against information exfiltration by cyber attacks.	321L2-5	322L3-4	541L3-2			Research & development in cybersecurity promoted
7-313a	Enhancing cooperation between MOD & defence industry.	132L3-3	511L2-6				Supply chain management of CI
7-320a	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point observation system). Extending observation points to other regions.	122L4-2	123L4-2	124L4-4	431L2-1		Early warning capability
7-321a	Positively contributing to international debate of international laws, rules & codes for cyberspace.	151L4-1	152L4-1	153L4-1	417L4-1	418L4-1	Rules of engagement in cyberspace
7-321b	Speeding up international assistance in investigation of cybercrimes under treaty for mutual legal assistance. Considering further conclusion of treaty.	431L2-2	431L3-2	431L4-1			Mutual legal assistance & extradition
7-321c	Exchanging information with law enforcement of those countries who are related to Japanese cybercrime circumstances.	431L2-1	432L1-3				Established formal international cooperation
7-321c2	Positively contributing to international framework for cooperation of anti-cybercrime.	417L4-1	418L4-1				Contributing to international cybercrime treaties
7-321c3	Enhancing relationship with neighbouring countries by holding Asian Pacific Regional Cyber Crime Investigation Technical Conferences.	431L2-1	432L1-3				Established formal international cooperation

Allocation (Requirement Keyword)			
2	3	4	5
Regular training for CSIRT members	Cybersecurity training aligned with national strategy		
Most officials have mind-set	Cybersecurity training programmes for non-professionals		
Metrics of effectiveness of cybersecurity training	Review of cybersecurity training programmes		
Latest technical controls & patch managements widely implemented			
Promotion of use of standards & best practices for development	Security consideration in all stages		
Latest technical security controls promoted	Regular review of technical security controls		
Advanced investigative capabilities for cybercrimes			
High-level scenario of national incident exercise			
Redundant communications for key stakeholders			
Cybersecurity training aligned with national strategy			
Optimised for extended outages			
Standards & best practices used by CI supply chains			
CoE in cybersecurity			
CoE in cybersecurity	Regular review of technical security controls		
Standards & best practices used by CI supply chains			
Regional coordination	Regional coordination	Established formal international cooperation	
Cross-border response ability	Leading international debate about cyber defence	Contributing to international cybercrime treaties	Contributing to international cybercrime treaties
Strategically expanding international cooperation	Regular review of international cooperation		
Informal international cooperation in law enforcement			
Contributing to international cybercrime treaties			
Informal international cooperation in law enforcement			

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-321d	Positively contributing to promotion of "Budapest Convention on Cybercrime" (the first international treaty seeking to address Internet and computer crime by harmonizing national laws), improving investigative techniques, & increasing cooperation among nations.	417L2-2	418L2-2	431L2-1			Participation to international agreements on cybercrime
7-322a	Contributing to UN effort to establish international rules to prevent contingencies from arising out of cyber attacks.	151L4-1	152L4-1	153L4-1			Rules of engagement in cyberspace
7-322a2	Sharing information about cyber threat & cybersecurity strategies through bilateral meetings.	153L4-2					Intelligence shared with allies
7-322b	Enhancing international relationship & cooperation through participating international conferences like "IWWN: International Watch and Warning Network" (established in 2004 to foster international collaboration on addressing cyber threats, attacks, and vulnerabilities).	123L2-3	123L3-2	124L3-5	153L4-2		International cooperation in incident response
7-322c	Continuing & enhancing international coordination & cooperation in incident responses,	123L2-3	123L3-2	124L3-5			International cooperation in incident response
7-323a	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace under direction of Director of Cabinet Intelligence.	151L3-2	152L3-1	153L3-1			Capturing landscape of national-level threat
7-323b	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace.	153L3-1					Analytical capability in cyber defence
7-324a	Government agencies positively support other nations based on "Basic Policy for Assistance of Cybersecurity Capacity Building in Developing Counties". Supporting ASEAN countries to build cybersecurity capabilities through "ASEAN-Japan Information Security Policy Meeting".	123L4-2	124L4-4				Regional coordination
7-324a2	Supporting countries in Asian Pacific region to build cybersecurity capabilities through "Asian Pacific Regional Cyber Crime Investigation Technical Conferences" & JICA's technical training programs.	411L4-2	417L4-1	418L4-1			Participation to international cooperation agreements
7-324a3	Contributing to regional cybersecurity awareness raising through "APT: Asia-Pacific Telecommunity", "ITU-D: ITU Telecommunication Development Sector" & "Ministerial Meeting on Telecommunications and Information Industry of APEC: Asia Pacific Economic Cooperation".	311L3-4					Contribution to international awareness raising
7-324a4	Supporting ASEAN countries to build cybersecurity capabilities through "Asian Pacific Regional Cyber Crime Investigation Technical Conferences" & "UNODC: United Nations Office on Drugs and Crime".	123L4-2	124L4-4				Regional coordination
7-324a5	Supporting ASEAN countries to build cybersecurity capabilities by holding seminars of ISMS & CSMS.	123L4-2	124L4-4				Regional coordination
7-324a6	Supporting countries in Asian Pacific & Africa to build & operate national CSIRTs.	123L4-2	124L4-4				Regional coordination
7-324a7	Holding seminars for 'secure development' for foreign software suppliers.	332L4-1	511L2-6				Cybersecurity trained professionals internationally contributing
7-325a	Encouraging personnel of government agencies & related agencies to attend international conferences, international CTFs & foreign schools.	123L3-2	124L3-5	331L3-1			International coordination
7-330a	N/A Not a specific action.						
7-330b	Enhancing coordination & cooperation of G7 through "Ise-Shima Cyber Group".	123L2-3	123L3-2	124L3-5			International cooperation in incident response
7-330c	Continuing & extending international cooperation through bilateral meetings.	123L2-3	123L3-2	124L3-5			International cooperation in incident response
7-330d	Enhancing intelligence sharing with foreign governments.	153L4-2					Intelligence shared with allies
7-330e	Contributing to international effort to raise cybersecurity awareness.	311L3-4					Contribution to international awareness raising
7-330f	Enhancing intelligence sharing with foreign law enforcement & legal communities.	431L2-1	431L3-2	432L1-3			Established formal international cooperation
7-330g	Researching technologies for measuring cyber health of countries/regions ("Cyber Green Project").	511L3-3					Contributing to international standards
7-330h	Enhancing information sharing with foreign agencies for information security like NIST.	511L3-3					Contributing to international standards
7-330i	Same as 7-324a, 7-324b						
7-330j	Considering possible cooperation in cyberspace between MOD/JSDF & foreign forces.	123L3-2	124L3-5	152L4-1			International coordination
7-331a	Same as 7-324c						
7-331a2	Building regional confidence measures through "ARF: ASEAN Regional Forum".	123L4-2	124L4-4				Regional coordination

Allocation (Requirement Keyword)			
2	3	4	5
Participation to international agreements on cybercrime	Established formal international cooperation		
Cross-border response ability	Leading international debate about cyber defence		
International coordination	International coordination	Intelligence shared with allies	
International coordination	International coordination		
Advanced capabilities & situational awareness	Analytical capability in cyber defence		
Regional coordination			
Contributing to international cybercrime treaties	Contributing to international cybercrime treaties		
Regional coordination			
Regional coordination			
Regional coordination			
Standards & best practices used by CI supply chains			
International coordination	Cybersecurity training aligned with international best practices		
International coordination	International coordination		
International coordination	International coordination		
Strategically expanding international cooperation	Informal international cooperation in law enforcement		
International coordination	Cross-border response ability		
Regional coordination			

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-331b	Supporting countries in Asian Pacific region to establish cybercrime jurisdiction.			Not allocated			
7-331c	Establishing cooperation with South-East Asian countries & Australia in cybersecurity.	123L4-2	124L4-4				Regional coordination
7-332a	Enhancing coordination & cooperation with US through "Japan-U.S. Cyber Dialogues".	123L2-3	123L3-2	124L3-5			International cooperation in incident response
7-332a2	Enhancing cyber defence cooperation with European countries through "Japan-UK Bilateral Consultations on Cyberspace", "Japan-NATO Staff Talks on Cyber defence" & participation in exercises held by NATO.	152L4-1	153L4-2				Cross-border response ability
7-332b	Enhancing information sharing with US based on "U.S.-Japan Policy Cooperation Dialogue on the Internet Economy".	153L4-2					Intelligence shared with allies
7-332b2	Promoting cooperation between Japan's ICT-ISAC & US IT-ISAC.	431L2-1	432L3-2				Established formal international cooperation
7-332c	Enhancing cyber defence cooperation with US through "U.S.-Japan Cyber defence Policy Working Group".	152L4-1	153L4-2				Cross-border response ability
7-333a	Enhancing cooperation through bilateral meetings.	152L4-1					Cross-border response ability
7-333b	Gathering information on latest technologies through consultation with "JIWG: Joint Industry Working Group".	541L3-2					Regular review of technical security controls
7-334a	Enhancing cooperation through bilateral meetings.	123L2-3					International cooperation in incident response
7-410a	Establishing "Strategy for Research & Development of Cybersecurity".	321L2-5					Research & development in cybersecurity promoted
7-410b	Researching security assessment of cryptographic algorisms & protocols.	551L4-1					Regular review of relevance of cryptographic controls
7-411a	Researching technologies for countermeasures against cyber attacks.	541L3-2					Regular review of technical security controls
7-411a2	Building up large scale reservoir of cybersecurity related information.	321L2-5					Research & development in cybersecurity promoted
7-411a3	Improving R&D environment by establishing security validation platform.	321L2-5					Research & development in cybersecurity promoted
7-411b	Researching technologies for detection & prediction of cyber attacks on control systems.	133L3-1	541L3-2				Cybersecurity oriented risk management in CI
7-411b2	Researching technologies for vulnerability management on control systems without interruption of services.	133L3-1	541L2-1	541L3-2			Cybersecurity oriented risk management in CI
7-411c	Providing with "NONSTOP" (R&D platform for secure handling of malware samples).	321L2-5					Research & development in cybersecurity promoted
7-411d	Researching technologies for data analysis & resilience against cyber attacks.	321L2-5	541L3-2				Research & development in cybersecurity promoted
7-412a	Same as 7-410a2	321L2-5	321L4-1	322L4-1			Research & development in cybersecurity promoted
7-412b	Researching technologies for creation of cyber-physical system.	321L2-5	321L4-1	322L4-1			Research & development in cybersecurity promoted
7-412c	Promoting researching of advanced AI infrastructure & its practical research for cybersecurity area.	321L2-5	321L4-1	322L4-1			Research & development in cybersecurity promoted
7-413a	Researching for quantum cryptography communication.	551L4-1					Regular review of relevance of cryptographic controls
7-413b	Promoting "The List of Ciphers that should be Referred to in the Procurement for the e-Government System" by "CRYPTREC: Cryptography Research and Evaluation Committees".	551L4-2					Revision of cryptographic control policies
7-413b2	Researching technologies for secure cryptography.	551L4-1					Regular review of relevance of cryptographic controls
7-413b3	Promoting use of secure cryptography.	551L2-1					Cryptographic controls widely used
7-413c	Researching innovative & advanced technologies for balancing security & efficiency of IoTs.	133L3-1	541L4-1				Cybersecurity oriented risk management in CI
7-414a	Positively contributing to international debate of standards for information security by participating ITU-T SG17.	511L3-3					Contributing to international standards
7-415a	Researching technologies for monitoring & analysis of control & communication systems through "Cyber-Security for Critical Infrastructure" of "SIP: Cross-ministerial Strategic Innovation Promotion Program".	133L3-1	521L4-3	521L4-4	541L4-1		Cybersecurity oriented risk management in CI
7-420a	Promoting human resources development based on "Cybersecurity Human Resources Development Program".	331L3-2	332L3-1				Cybersecurity training aligned with national strategy
7-421a	Promoting practical exercise & PBL (problem based learning) on cybersecurity by collaboration of multiple universities and/or academia-industry.	321L4-3	322L4-2	322L4-3			Cybersecurity education adapting to changing needs
7-421b	Promoting collaboration of industry, government & academia on practical cyber exercises.	322L4-2	331L4-1	331L4-2	332L3-2		Cooperation between all stakeholders in cybersecurity education
7-421c	Developing human resources with hybrid careers.	322L4-3	331L3-3	331L4-3			Cybersecurity education aligned with practical problems

Allocation (Requirement Keyword)			
2	3	4	5
Regional coordination			
International coordination	International coordination		
Intelligence shared with allies			
Cooperation between foreign ISPs & law enforcement			
Intelligence shared with allies			
Regular review of technical security controls			
Latest technical controls & patch managements widely implemented	Regular review of technical security controls		
Regular review of technical security controls			
Internationally forerunning in cybersecurity education	International CoE in cybersecurity		
Internationally forerunning in cybersecurity education	International CoE in cybersecurity		
Internationally forerunning in cybersecurity education	International CoE in cybersecurity		
Continuous assess of technical security controls			
Controlled acquisition of critical technologies	Independency & persistence of internet infrastructure technologies	Continuous assess of technical security controls	
Review of cybersecurity training programmes			
Cooperation between all stakeholders in cybersecurity education	Cybersecurity education aligned with practical problems		
Collaboration between public & private in cybersecurity training	Coordination between cybersecurity training & education	Coordination of cybersecurity training across sectors	
Communication skills in cybersecurity training	Incentives for cybersecurity trained workforce		

Appendix E

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7-421d	Enhancing cybersecurity education at colleges of technology ("Kosen") based on needs from industry. Providing with cyber ranges	321L3-5	321L4-3	322L4-3			Cybersecurity education from primary to post-graduate
7-421e	Promoting cybersecurity education for working adults at universities.	322L4-2	322L4-3				Cooperation between all stakeholders in cybersecurity education
7-421f	Incorporating cybersecurity education into public vocational training.	331L2-4	331L4-1				Cybersecurity training programmes for non-professionals
7-422a	Promoting education at elementary, middle & high schools about IT, information security & information moral based on individual ability of use of IT.	213L3-1	213L4-1	311L4-3	321L3-5		Most users have mind-set
7-422b	Training teachers for IT skills & information moral	213L3-1	213L4-1	311L4-3	321L3-5		Most users have mind-set
7-423a	Continuing to hold "Security Camp" to raise awareness of youth & to discover prominent human resources.	213L3-1	321L3-5				Most users have mind-set
7-423b	Jointly promoting CTFs with "JNSA: Japan Network Security Association".	332L3-2					Coordination of cybersecurity training across sectors
7-423c	Conducting "MITOU Program: Exploratory IT Human Resources Project" to discover innovative talents.	321L3-3	321L4-1				Cybersecurity specific degree
7-424a	Promoting "Information Technology Engineers Examination" to develop highly skilled IT human resources.	331L2-1	331L2-2	332L2-1			Structured cybersecurity training programmes
7-424b	Promoting "Information Security Management Examination" (a subject of "Information Technology Engineers Examination").	331L1-2					Cybersecurity training for general IT staff
7-424c	Supporting young engineers & student to design their career pass in IT industry.	322L2-3					Attractiveness of cybersecurity career
7-424d	Promoting new national qualification "Registered Information Security Specialist".	331L2-2	331L3-2	332L2-3			Security professional certification
7-424e	Training youth to cybersecurity expert at "National Cyber Training Center".	321L3-5	331L4-2				Cybersecurity education from primary to post-graduate
7-425a	Sending officials to study at graduate schools.	124L3-1	322L4-3	331L4-1			Training & accreditation for CSIRT members established
7-425b	Performing upgraded practical cyber defence exercise "(New) CYDER" at "National Cyber Training Center".	141L3-1					High-level scenario of national incident exercise
7-425c	Establishing practical exercise environment of communication system of JSDF.	161L3-1					Redundant communications for key stakeholders
7-425d	Enhancing cooperation between MOD/JSDF & defence industry.	132L3-3					Supply chain management of CI
7-425d2	Enhancing cooperation between MOD/JSDF & operators of infrastructures affecting operation.	153L2-1	153L2-2				Coordination between CI & defence

Allocation (Requirement Keyword)			
2	3	4	5
Cybersecurity education adapting to changing needs	Cybersecurity education aligned with practical problems		
Cybersecurity education aligned with practical problems			
Collaboration between public & private in cybersecurity training			
Users' mind-set reducing threat	Entire society involved in awareness raising	Cybersecurity education from primary to post-graduate	
Users' mind-set reducing threat	Entire society involved in awareness raising	Cybersecurity education from primary to post-graduate	
Cybersecurity education from primary to post-graduate			
Internationally forerunning in cybersecurity education			
Security professional certification	Cybersecurity trained & certified employees		
Cybersecurity training aligned with national strategy	Job creation in cybersecurity		
Coordination between cybersecurity training & education			
Cybersecurity education aligned with practical problems	Collaboration between public & private in cybersecurity training		
Intelligence sharing between CI & defence			

Appendix F Japanese Action Items Mapping Result by Requirement

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	111L1-1	Outline of strategy	0	111L2-1
				111L1-2	Development process of strategy	0	111L2-2
				111L1-3	Stakeholders involved in strategy development	0	111L2-3
112	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Organisation	112L1-1	Cybersecurity programme under development	0	112L2-1
							112L2-2
							112L2-3
							112L2-4
113	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Content	113L1-1	Risk priorities of cybersecurity defined in strategy	0	113L2-1
							113L2-2
121	Cybersecurity Policy and Strategy	Incident Response	Identification of Incidents	121L1-1	Recording incidents	0	121L2-1
122	Cybersecurity Policy and Strategy	Incident Response	Organisation	122L1-1	Key incident response organisations in private sector identified	0	122L2-1
				122L1-2	N/A	0	122L2-2
				122L1-3	Ad-hoc responses	0	
123	Cybersecurity Policy and Strategy	Incident Response	Coordination	123L1-1	Leading incident response organisation designated	0	123L2-1
							123L2-2
							123L2-3
124	Cybersecurity Policy and Strategy	Incident Response	Mode of Operation	124L1-1	Key incident response processes	0	124L2-1
				124L1-2	CSIRT member training	0	124L2-2
							124L2-3
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	131L1-1	List of CI assets	0	131L2-1
							131L2-2
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	132L1-1	Informal information sharing between CI & government	0	132L2-1
							132L2-2
							132L2-3
							132L2-4
133	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Risk Management and Response	133L1-1	Access control implemented in CI	0	133L2-1
				133L1-2	Basic capacity against cyber threat in CI	0	133L2-2
				133L1-3	Data security policy in CI	0	133L2-3
141	Cybersecurity Policy and Strategy	Crisis Management	Crisis Management	141L1-1	Assessment of exercise of national incident	0	141L2-1
				141L1-2	Exercise planning organisation designated for national incident	0	141L2-2
				141L1-3	Stakeholders' participation in national incident exercise	0	141L2-3
							141L2-4
							141L2-5
							141L2-6

Nb. = Number of Related Action Items

Level 2		Level 3			Level 4		
Keywords	**Nb.**	ID	Keywords	**Nb.**	ID	Keywords	**Nb.**
Strategy established	0	111L3-1	Reviewing process of strategy	0	111L4-1	Continual revision of strategy	1
Stakeholders' consultation in strategy	0	111L3-2	Cyber exercises considered in strategy	0	111L4-2	Contributing to international debate of strategy	0
Implementation of strategy	0	111L3-3	Measurement of cybersecurity defined in strategy	0			
		111L3-4	Capacity building & investment considered in strategy	0			
Cybersecurity programme agreed	0	112L3-1	PDCA processes of cybersecurity programme	0	112L4-1	Reassignment & reallocation of resources for cybersecurity programme	0
Coordinating body of cybersecurity programme	0	112L3-2	Consolidated budget for cybersecurity	0	112L4-2	Dissemination & feedbacks about cybersecurity programme	0
Goals & measurement of cybersecurity programme	0						
Discrete budget for cybersecurity	0						
National objectives of cybersecurity defined in strategy	0	113L3-1	Measurement of cybersecurity defined in strategy	0	113L4-1	Continual revision of strategy	1
Minimum coverage of strategy contents	0	113L3-2	Protection of critical infrastructures defined in strategy	0	113L4-2	Contributing to international cooperation	0
Central registry of incidents	0	121L3-1	Regular revision of incident registry	0	121L4-1	Adapted analysis of incidents	1
		121L3-2	Incident analysis	1			
National CSIRT	0	122L3-1	Formal roles & responsibilities allocated	0	122L4-1	Sustainability of incident response capability	0
Roles & responsibilities of national CSIRT	0	122L3-2	Adequate resources for incident response	1	122L4-2	Early warning capability	4
					122L4-3	Capability to manage threat landscape	0
Coordination established	0	123L3-1	Subnational / sectorial incident response organisations	13	123L4-1	Coordinating all levels / sectors	0
Communication lines for crisis	0	123L3-2	International coordination	7	123L4-2	Regional coordination	8
International cooperation in incident response	6	123L3-3	Information sharing across sectors	4			
Incident response processes & tools established	0	124L3-1	Training & accreditation for CSIRT members established	4	124L4-1	Scenario testing of incident response processes	2
Regular training for CSIRT members	4	124L3-2	Sophisticated incident analysis	5	124L4-2	Evaluating effectiveness of CSIRT members training	1
Limited response to national level incidents	0	124L3-3	Regular review of incident response processes	3	124L4-3	Tools against zero-day vulnerabilities	0
		124L3-4	Forensics	2	124L4-4	Regional coordination	8
		124L3-5	International coordination	7			
Audit of CI assets	0	131L3-1	Priority of CI risks	0	131L4-1	Regular review of CI risk priorities	2
CI assets audit list	0	131L3-2	Vulnerability & asset management of CI assets	2			
Information sharing established between CI & government	8	132L3-1	Centralised management of CI protection	0	132L4-1	Ability to adjust of CI protection	1
Formal & consistent information sharing between CI & government	7	132L3-2	Public awareness campaign of CI protection	0	132L4-2	Trust between CI & government	0
Point of contact	3	132L3-3	Supply chain management of CI	4			
Government engagement in CI protection	2						
Standards & best practices in CI	0	133L3-1	Cybersecurity oriented risk management in CI	18	133L4-1	Regular audit of CI	2
Risk management processes in CI	2	133L3-2	Regular review of impact analysis of CI	1	133L4-2	Indirect costs inclusive in impact analysis of CI incidents	0
National CI incident response plan	1	133L3-3	Regular review of CI incident response plans	0			
		133L3-4	Regular review of resource allocation for CI protection	0			
		133L3-5	Insider threat detection in CI	0			
National incident exercise done	3	141L3-1	High-level scenario of national incident exercise	12	141L4-1	Peer observance of national incident exercise	0
Appropriate resources for national incident exercise	1	141L3-2	Trust between participants of national incident exercise	0	141L4-2	National incident exercise contributing to international challenges	0
Roles in national incident exercise defined	1	141L3-3	SMART objectives & KPI of national incident exercise	0	141L4-3	Internationally shared result of national incident exercise	0
Incentives to participate in national incident exercise	0	141L3-4	Evaluation of national incident exercise informing investment	0	141L4-4	National crisis management established	0
Trained monitors of national incident exercise	0	141L3-5	National crisis management aligned with international best practices	0			
Evaluation of national incident exercise	0	141L3-6	Tailored reports of national incident exercise	0			

Appendix F

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
151	Cybersecurity Policy and Strategy	Cyber Defence	Strategy	151L1-1	National-level threats identified	0	151L2-1
152	Cybersecurity Policy and Strategy	Cyber Defence	Organisation	152L1-1	Dispersed cyber operations	0	152L2-1
153	Cybersecurity Policy and Strategy	Cyber Defence	Coordination	153L1-1	Cyber defence capability requirements agreed	0	153L2-1
							153L2-2
161	Cybersecurity Policy and Strategy	Communications Redundancy	Communications Redundancy	161L1-1	Gaps in emergency communication identified	0	161L2-1
				161L1-2	Emergency procedures established	0	161L2-2
							161L2-3
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	211L1-1	Leading agencies only have mind-set	0	211L2-1
212	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	212L1-1	Leading firms only have mind-set	0	212L2-1
				212L1-2	Materials for best practices available	0	
213	Cyber Culture and Society	Cybersecurity Mind-set	Users	213L1-1	Limited users only have mind-set	0	213L2-1
221	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	221L1-1	A few users can use internet securely	0	221L2-1
				221L1-2	Promotion of online trust exists	0	221L2-2
							221L2-3
222	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-government Services	222L1-1	Government's recognition of needs for security in e-gov	0	222L2-1
				222L1-2	Stakeholders' recognition of needs for security in e-gov	0	222L2-2
				222L1-3	A few users can use e-gov securely	0	222L2-3
				222L1-4	Security measures in e-gov	0	222L2-4
							222L2-5
223	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-commerce Services	223L1-1	Limited e-commerce provided	0	223L2-1
				223L1-2	Private sectors' recognition of need for security in e-commerce	0	223L2-2
				223L1-3	A few users can use e-commerce securely	0	223L2-3
				223L1-4	Security measures in e-commerce	0	223L2-4
							223L2-5
231	Cyber Culture and Society	User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	231L1-1	Users have only general knowledge about personal information protection	0	231L2-1
				231L1-2	Discussions on protecting personal information	0	231L2-2
241	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	241L1-1	Reporting channels of incidents	0	241L2-1
							241L2-2
251	Cyber Culture and Society	Media and Social Media	Media and Social Media	251L1-1	Media coverage of cybersecurity	0	251L2-1
				251L1-2	Discussion on social media security	0	251L2-2
							251L2-3

Level 2		Level 3			Level 4		
Keywords	**Nb.**	ID	Keywords	**Nb.**	ID	Keywords	**Nb.**
Cyber defence strategy exists	0	151L3-1	Dedicated resources for cyber defence	0	151L4-1	Rules of engagement in cyberspace	2
		151L3-2	Capturing landscape of national-level threat	1	151L4-2	Military doctrine in cyberspace	0
		151L3-3	Cyber defence strategy meets objectives	0			
Defined responsibility of cyber defence organisation	0	152L3-1	Advanced capabilities & situational awareness	1	152L4-1	Cross-border response ability	6
Coordination between CI & defence	1	153L3-1	Analytical capability in cyber defence	4	153L4-1	Leading international debate about cyber defence	2
Intelligence sharing between CI & defence	3	153L3-2	Strengths & weaknesses of cyber defence understood	0	153L4-2	Intelligence shared with allies	6
Emergency response assets hardwired	0	161L3-1	Redundant communications for key stakeholders	6	161L4-1	Optimised for extended outages	1
Communication between emergency response functions distributed	0	161L3-2	Interoperability & functionality under compromised situation	0	161L4-2	Assisting neighbours	0
Testing, training, drills of emergency response	0	161L3-3	Evaluation of national incident exercise informing investment	0			
		161L3-4	Contribution to international communications' redundancy	0			
Most officials have mind-set	1	211L3-1	Mind-set spread in public sector	2	211L4-1	Mind-set commonplace in public sector	0
		211L3-2	Mind-set based strategy in public sector	2			
Most private sector actors have mind-set	0	212L3-1	Mind-set spread in private sector	3	212L4-1	Mind-set commonplace in private sector	1
		212L3-2	Mind-set based strategy in private sector	1			
Growing number of users have mind-set	6	213L3-1	Most users have mind-set	9	213L4-1	Users' mind-set reducing threat	2
Growing number of users can use internet securely	6	221L3-1	Most users can use internet securely	5	221L4-1	Users can evaluate risk & adjust behaviour	0
Promotion of online trust established	11	221L3-2	Users' ability to control providing personal information	4	221L4-2	Promotion of online trust revised	0
User assistance available	1	221L3-3	Promotion of online trust evaluated	0			
E-gov established	0	222L3-1	Disclosures of activities of government agencies	0	222L4-1	Promotion of e-gov revised	0
Risk reduction in e-gov	0	222L3-2	Privacy-by-default in e-gov	3	222L4-2	Data protection measures of e-gov	0
Promotion of e-gov	0	222L3-3	Most users can use e-gov securely	0			
Growing number of users can use e-gov securely	0	222L3-4	User feedbacks for e-gov	0			
Incident disclosure in e-gov	0						
E-commerce established	0	223L3-1	Resource allocation for e-commerce	0	223L4-1	Continuous improvement of e-commerce	0
Secure payment	0	223L3-2	Most users can use e-commerce securely	0	223L4-2	Clear terms & conditions of e-commerce	0
Growing number of users can use e-commerce securely	0	223L3-3	Investment for e-commerce	0	223L4-3	User feedbacks for e-commerce	0
Promotion of trust of e-commerce	2						
Terms & conditions of e-commerce accessible	0						
Growing number of users can secure personal information online	3	231L3-1	Measures to protect personal information online	0	231L4-1	Users can adapt to changing environments	0
Discussions on balance between security & privacy	0	231L3-2	Privacy rights	0	231L4-2	Wide recognition about personal information protection	0
		231L3-3	Security & privacy balanced	0	231L4-3	Security & privacy balanced in changing environment	0
		231L3-4	Privacy-by-default	0	231L4-4	Regular assessment of privacy protection	0
Incident reporting mechanisms established	0	241L3-1	Coordination of incident reporting channels	0	241L4-1	Regular enhancement of incident reporting	0
Promotion of incident reporting channels	1	241L3-2	Promotion of incident reporting channels prioritised	0	241L4-2	Coordination of response to reported incidents	0
		241L3-3	Metrics of incident reporting	0			
Cybersecurity as common subject in media	0	251L3-1	Media coverage of information about cybersecurity measures	0	251L4-1	Discussion changing policy & society	0
Wide range of issues of cybersecurity in media	0	251L3-2	Frequent discussion on social media security	3			
Broad discussion on social media security	0						

Appendix F

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	311L1-1	Awareness raising programmes	0	311L2-1
				311L1-2	Awareness raising programmes affected by international initiatives	0	311L2-2
							311L2-3
312	Cybersecurity Education, Training and Skills	Awareness Raising	Executive Awareness Raising	312L1-1	Executives' awareness about general cybersecurity issues	0	312L2-1
				312L1-2	Executives of particular sectors have awareness	0	312L2-2
							312L2-3
321	Cybersecurity Education, Training and Skills	Framework for Education	Provision	321L1-1	Qualification programme for cybersecurity educators	0	321L2-1
				321L1-2	Professional cybersecurity educators	0	321L2-2
				321L1-3	Educational courses for cybersecurity	0	321L2-3
				321L1-4	Demand exists for cybersecurity education	0	321L2-4
							321L2-5
322	Cybersecurity Education, Training and Skills	Framework for Education	Administration	322L1-1	Cybersecurity education needs recognised	0	322L2-1
				322L1-2	Ad-hoc supply of resources for cybersecurity education	0	322L2-2
							322L2-3
331	Cybersecurity Education, Training and Skills	Framework for Professional Training	Provision	331L1-1	Cybersecurity training needs recognised	0	331L2-1
				331L1-2	Cybersecurity training for general IT staff	1	331L2-2
				331L1-3	ICT certification with some cybersecurity issues	0	331L2-3
				331L1-4	Training courses for cybersecurity	0	331L2-4
332	Cybersecurity Education, Training and Skills	Framework for Professional Training	Uptake	332L1-1	Metrics of uptake of cybersecurity trainings	0	332L2-1
							332L2-2
							332L2-3
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	411L1-1	Discussion of establishing cybersecurity legal framework	0	411L2-1
				411L1-2	Priorities identified in cybersecurity legal framework	0	411L2-2
412	Legal and Regulatory Frameworks	Legal Framework	Privacy, Freedom of Speech & Other Human Rights Online	412L1-1	Partial privacy protection legislation	0	412L2-1
				412L1-2	Freedom of expression	0	412L2-2
				412L1-3	Discussion of establishing digital human rights legislation	0	412L2-3
							412L2-4
							412L2-5
413	Legal and Regulatory Frameworks	Legal Framework	Data Protection Legislation	413L1-1	Partial data protection legislation	0	413L2-1
				413L1-2	Stakeholders' participation in data protection legislation	0	413L2-2
414	Legal and Regulatory Frameworks	Legal Framework	Child Protection Online	414L1-1	Partial online child protection legislation	0	414L2-1
				414L1-2	Stakeholders' participation in online child protection legislation	0	414L2-2

Level 2		Level 3			Level 4		
Keywords	Nb.	ID	Keywords	Nb.	ID	Keywords	Nb.
National programme of awareness raising	1	311L3-1	Sector specific programmes of awareness raising	1	311L4-1	Awareness raising programmes adapted according to effectiveness	0
Consultation with stakeholders in national programme of awareness raising	0	311L3-2	Metrics for effectiveness of awareness raising programmes	1	311L4-2	Revision of national awareness raising programme	0
Cybersecurity information portal	0	311L3-3	Evolution of awareness raising programmes	0	311L4-3	Entire society involved in awareness raising	2
		311L3-4	Contribution to international awareness raising	5	311L4-4	Overall threat reduced by awareness raising	0
Executives' basic understandings of cybersecurity	0	312L3-1	Executives' understandings of cybersecurity measures	6	312L4-1	Cybersecurity as common agenda in board meetings	0
Limited executives' understandings of cybersecurity's affect	0	312L3-2	Executives' ability to reallocate resources	0	312L4-2	Executives' attitude as international role model	0
Raising programmes for awareness of crisis management	0	312L3-3	Executives' understanding of crisis management plans	2			
		312L3-4	Mandatory cybersecurity education for executives	0			
Qualification for cybersecurity educators established	0	321L3-1	Business experts' participation in cybersecurity education	0	321L4-1	Internationally forerunning in cybersecurity education	4
University level courses for cybersecurity	0	321L3-2	Mandatory cybersecutity courses for computer science degrees	0	321L4-2	Balance between core components & adaptive processes	0
Degrees in cybersecurity	0	321L3-3	Cybersecurity specific degree	1	321L4-3	Cybersecurity education adapting to changing needs	2
Seminars for non-specialist	0	321L3-4	Cybersecurity as focusing area	0			
Research & development in cybersecurity promoted	11	321L3-5	Cybersecurity education from primary to post-graduate	5			
Broad discussion for enhancing cybersecurity education	0	322L3-1	Cybersecurity education demand/supply monitored	0	322L4-1	International CoE in cybersecurity	3
Budget for research & education for cybersecurity	1	322L3-2	Adapted budget for cybersecurity education	0	322L4-2	Cooperation between all stakeholders in cybersecurity education	3
Attractiveness of cybersecurity career	1	322L3-3	International cooperation in cybersecurity education	1	322L4-3	Cybersecurity education aligned with practical problems	5
		322L3-4	CoE in cybersecurity	3			
Structured cybersecurity training programmes	1	331L3-1	Cybersecurity training aligned with international best practices	1	331L4-1	Collaboration between public & private in cybersecurity training	3
Security professional certification	2	331L3-2	Cybersecurity training aligned with national strategy	9	331L4-2	Coordination between cybersecurity training & education	2
Cybersecurity training requirements listed	0	331L3-3	Communication skills in cybersecurity training	2	331L4-3	Incentives for cybersecurity trained workforce	1
Cybersecurity training programmes for non-professionals	4	331L3-4	Metrics of effectiveness of cybersecurity training	1			
Cybersecurity trained & certified employees	1	332L3-1	Review of cybersecurity training programmes	2	332L4-1	Cybersecurity trained professionals internationally contributing	2
Knowledge transfer in cybersecurity	0	332L3-2	Coordination of cybersecurity training across sectors	2			
Job creation in cybersecurity	1						
Cybersecurity legal framework established	0	411L3-1	Regular review of cybersecurity legal framework	1	411L4-1	Balance between cybersecurity legal framework & best practices	0
Coverages of cybersecurity legal framework	0				411L4-2	Participation to international cooperation agreements	1
					411L4-3	Exceeding minimum requirement of international cooperation agreement	0
Online privacy protected	0	412L3-1	Cybersecurity legal framework aligned with international best practices	1	412L4-1	Amendment procedures for cybersecurity legal framework	0
Freedom of expression protected	0	412L3-2	Exceeding minimum requirement of international agreement	0	412L4-2	Internet access as human right	0
Privacy protected during investigation	0				412L4-3	Contributing to international digital human rights	0
Stakeholders' participation to discuss digital human rights legislation	0				412L4-4	Contributing to international privacy protection online	1
Participation to international agreements	0						
Data protection legislation established	0	413L3-1	Timeframe of storing personal data during investigation	0	413L4-1	Amendment procedures for data protection legislation	0
Personal data protected	0	413L3-2	Data protection legislation aligned with international best practices	0			
Online child protection legislation established	0	414L3-1	Online child protection legislation aligned with international best practices	0	414L4-1	Amendment procedures for online child protection legislation	0
Legal minors protected	0						

Appendix F

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
415	Legal and Regulatory Frameworks	Legal Framework	Consumer Protection Legislation	415L1-1	Partial consumer protection legislation	0	415L2-1
				415L1-2	Stakeholders' participation in consumer protection legislation	0	415L2-2
416	Legal and Regulatory Frameworks	Legal Framework	Intellectual Property Legislation	416L1-1	Partial intellectual property legislation	0	416L2-1
				416L1-2	Stakeholders' participation in intellectual property legislation	0	
417	Legal and Regulatory Frameworks	Legal Framework	Substantive Cybercrime Legislation	417L1-1	Partial substantive cybercrime legislation	0	417L2-1
							417L2-2
418	Legal and Regulatory Frameworks	Legal Framework	Procedural Cybercrime Legislation	418L1-1	Partial procedural cybercrime legislation	0	418L2-1
							418L2-2
421	Legal and Regulatory Frameworks	Criminal Justice System	Law Enforcement	421L1-1	Limited digital forensics capabilities in law enforcement	0	421L2-1
				421L1-2	Training for law enforcement officers	0	421L2-2
							421L2-3
422	Legal and Regulatory Frameworks	Criminal Justice System	Prosecution	422L1-1	Limited capabilities to prosecute cybercrimes	0	422L2-1
				422L1-2	Training for prosecutors	0	
423	Legal and Regulatory Frameworks	Criminal Justice System	Courts	423L1-1	Limited capabilities to judge cybercrimes	0	423L2-1
				423L1-2	Training for judges	0	423L2-2
431	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	431L1-1	Formal international cooperation against cybercrimes	0	431L2-1
				431L1-2	Exchange of information between public & private sectors about cybercrimes	3	431L2-2
							431L2-3
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Informal Cooperation	432L1-1	Exchange of information between government & justice about cybercrimes	0	432L2-1
				432L1-2	Cooperation between ISPs & law enforcement	0	432L2-2
				432L1-3	Informal international cooperation in law enforcement	3	432L2-3
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	511L1-1	Standards for information risk management	0	511L2-1
				511L1-2	Standards for information risk management partly used	0	511L2-2
				511L1-3	International standards & best practices implemented	0	511L2-3
							511L2-4
							511L2-5
							511L2-6

Level 2		Level 3			Level 4		
Keywords	Nb.	ID	Keywords	Nb.	ID	Keywords	Nb.
Consumer protection legislation established	0	415L3-1	Consumer protection legislation aligned with international best practices	0	415L4-1	Amendment procedures for consumer protection legislation	0
Responsible agency designated for consumer protection	0						
Intellectual property legislation established	0	416L3-1	Intellectual property legislation aligned with international best practices	0	416L4-1	Balance between intellectual property & open access policy	0
		416L3-2	Stakeholders' participation in amendment of intellectual property legislation	0			
Substantive cybercrime legislation exists	0	417L3-1	Exceeding minimum requirement in international agreements on cybercrime	1	417L4-1	Contributing to international cybercrime treaties	3
Participation to international agreements on cybercrime	1	417L3-2	Amendment procedures for substantive cybercrime legislation	0	417L4-2	Regular review of substantive cybercrime legislation	0
Procedural cybercrime legislation exists	0	418L3-1	Procedural cybercrime legislation enables cross-border investigation	0	418L4-1	Contributing to international cybercrime treaties	3
Participation to international agreements on cybercrime	1	418L3-2	Exceeding minimum requirement in international agreements on cybercrime	1	418L4-2	Regular review of procedural cybercrime legislation	0
		418L3-3	Amendment procedures for procedural cybercrime legislation	0			
Comprehensive investigative capabilities for cybercrimes	0	421L3-1	Dedicated investigative resources for cybercrimes	0	421L4-1	Specialised and continuous training for law enforcement officers	1
Established chain of custody of digital evidence	0	421L3-2	Advanced investigative capabilities for cybercrimes	6	421L4-2	Sophisticated digital forensic tools	2
Standards for training for law enforcement officers	0	421L3-3	Regular training for law enforcement officers	1	421L4-3	Regular review of investigative capabilities for cybercrimes	0
		421L3-4	Cross-border investigation of cybercrimes	0			
		421L3-5	Statistics & analysis of cybercrime investigations	1			
Comprehensive prosecutorial capabilities for cybercrimes	0	422L3-1	Institutional structures in prosecution services	0	422L4-1	Prosecution of cross-border cybercrimes	0
		422L3-2	Statistics & analysis of cybercrime prosecutions	0	422L4-2	Dedicated prosecutorial resources for cybercrimes	0
		422L3-3	Exchange of best practices between prosecutors & judges	0	422L4-3	Specialised and continuous training for prosecutors	1
Sufficient jurisdictional capabilities for cybercrimes	0	423L3-1	Centralised judges for cybercrimes	0	423L4-1	Specialised and continuous training for judges	0
Specialised training for judges	0	423L3-2	Institutional structures of courts	0	423L4-2	Regular review of court system capabilities to judge cybercrimes	0
		423L3-3	Statistics & analysis of cybercrime convictions	0			
Established formal international cooperation	7	431L3-1	Communication channels for international cooperation	0	431L4-1	Regular review of international cooperation	1
Mutual legal assistance & extradition	1	431L3-2	Strategically expanding international cooperation	2	431L4-2	Interoperability of formal & informal international cooperation	0
Legislative requirements on information exchange between public & private sectors	1	431L3-3	Resources for information exchange between public & private sectors	10	431L4-3	Regularly adjusted information exchange between public & private sectors	0
Established informal cooperation between government & justice	0	432L3-1	Established relationship among government, prosecutors, judges & law enforcement	0	432L4-1	Adapted cooperation & exchange of information	0
Established informal cooperation between ISPs & law enforcement	2	432L3-2	Cooperation between foreign ISPs & law enforcement	1	432L4-2	Adapted international cooperation	0
Informal international integration in law enforcement	0	432L3-3	Joint international investigation & prosecution	0	432L4-3	Interoperability of formal & informal international cooperation	0
Established standards & best practices	8	511L3-1	Risk-based adoption of standards & best practices	0	511L4-1	Regular review of adoption of standards & best practices	2
Standards & best practices widely used	2	511L3-2	Resource allocation based on standards	0	511L4-2	Decision making of non-compliance to standards & best practices	0
Metrics of adoption of standards & best practices	1	511L3-3	Contributing to international standards	9	511L4-3	Risk-based decision making of compliance	0
Promotion of use of standards & best practices	14						
Metrics of compliance of standards & best practices	4						
Standards & best practices used by CI supply chains	4						

Appendix F

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
512	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	512L1-1	Standards & best practices for procurement	0	512L2-1
				512L1-2	Promotion of use of standards & best practices for procurement	6	512L2-2
							512L2-3
513	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	513L1-1	Standards & best practices for development	0	513L2-1
				513L1-2	Promotion of use of standards & best practices for development	1	513L2-2
				513L1-3	Coding standards	3	
521	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	521L1-1	Limited internet infrastructures	0	521L2-1
				521L1-2	Discussion on resilience of internet infrastructures	0	521L2-2
							521L2-3
							521L2-4
531	Standards, Organisations, and Technologies	Software Quality	Software Quality	531L1-1	Quality & functional requirement of software	0	531L2-1
				531L1-2	Catalogue of secure softwares	0	531L2-2
				531L1-3	Software update policies under development	0	531L2-3
				531L1-4	Software deficiencies information	0	531L2-4
541	Standards, Organisations, and Technologies	Technical Security Controls	Technical Security Controls	541L1-1	Technical security controls deployed	0	541L2-1
				541L1-2	Latest technical security controls promoted	1	541L2-2
				541L1-3	Anti-malware services by ISPs	0	541L2-3
				541L1-4	ISPs' policies of technical security control	0	541L2-4
				541L1-5	IDS/IPS deployed	0	541L2-5
551	Standards, Organisations, and Technologies	Cryptographic Controls	Cryptographic Controls	551L1-1	Cryptographic controls deployed	0	551L2-1
				551L1-2	TLS deployed	0	551L2-2
							551L2-3
							551L2-4
561	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cybersecurity Technologies	561L1-1	Domestic security products market	0	561L2-1
				561L1-2	Cybersecurity consideration in development	0	561L2-2
562	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cyber Insurance	562L1-1	Needs for cybersecurity insurance understood	0	562L2-1
				562L1-2	Development of cybersecurity insurance	0	562L2-2
571	Standards, Organisations, and Technologies	Responsible Disclosure	Responsible Disclosure	571L1-1	Information sharing of vulnerabilities	0	571L2-1
				571L1-2	Ability to address vulnerability reports	0	571L2-2
							571L2-3

Level 2		Level 3			Level 4		
Keywords	**Nb.**	ID	Keywords	**Nb.**	ID	Keywords	**Nb.**
International standards & best practices for procurement implemented	0	512L3-1	Standards & best practices for procurement widely used & complied	4	512L4-1	Realtime monitoring of non-compliance to standards & best practices for procurement	0
Metrics of adoption of standards & best practices for procurement	0	512L3-2	Regular review of procurement	4	512L4-2	Risk-based decision making of non-compliance	0
Metrics of compliance of standards & best practices for procurement	0	512L3-3	Wider resource planning in procurement	0			
		512L3-4	Procurement skills benchmark	0			
		512L3-5	E-sourcing / e-tendering	0			
Metrics of adoption of standards & best practices for development	0	513L3-1	Security consideration in all stages	9	513L4-1	Risk-based decision making of non-compliance	0
Education & training for development	4	513L3-2	Core development activities	0	513L4-2	Adopting standards throughout life-time	1
		513L3-3	Risk-based adoption of standards	0	513L4-3	Explicit requirements by contract	0
Reliable internet infrastructures	2	521L3-1	Metrics of compliance to international standards of internet infrastructures	0	521L4-1	Controlled acquisition of infrastructures	0
Established e-commerce & electronic authentication	0	521L3-2	Investment to new technologies in internet infrastructures	0	521L4-2	Optimised cost for internet infrastructures	1
Internet infrastructures compliant to international standards & best practices	0				521L4-3	Controlled acquisition of critical technologies	1
Internet infrastructures formally managed	0				521L4-4	Independency & persistence of internet infrastructure technologies	1
Established quality & functional requirement of software	0	531L3-1	Monitoring software quality	0	531L4-1	High performance, reliability & usability softwares	0
Softwares complying with international standards	0	531L3-2	Review of software update policies & processes	0	531L4-2	Automated service continuity	0
Established software update processes	0	531L3-3	Business benefit from improving software quality	0	531L4-3	Regular review of quality requirement	0
Software classification	0	531L3-4	Software deficiency handling	0			
Latest technical controls & patch managements widely implemented	14	541L3-1	User side security controls	2	541L4-1	Continuous assess of technical security controls	2
Anti-malware softwares & network firewalls	1	541L3-2	Regular review of technical security controls	13	541L4-2	Business impact by technical security controls understood	0
Physical security controls	0				541L4-3	Supplemental security services by ISPs	0
Established ISPs' policies of technical security control	2						
Technical security controls based on international frameworks	4						
Cryptographic controls widely used	2	551L3-1	Risk-based use of cryptographic controls	0	551L4-1	Regular review of relevance of cryptographic controls	4
Secure communication services	1	551L3-2	Regular review of cryptographic control policies	1	551L4-2	Revision of cryptographic control policies	2
Cryptographic controls complied to international standards	0						
TLS widespread	0						
Domestic providers of security products	1	561L3-1	Security products complied to International standards	1	561L4-1	Automated security functions	0
Lowering dependency on foreign cybersecurity technologies	1	561L3-2	Risk-based product development	0	561L4-2	Exporting superior security products	0
Established cybersecurity insurance market	1	562L3-1	Covering various costs	0	562L4-1	Innovative cybersecurity insurance market	0
Covering additional costs (ex. Forensic investigation etc.)	0	562L3-2	Choice of coverages	0	562L4-2	Emerging risks & various cyber harm	0
		562L3-3	Cybersecurity insurance products for SMEs	0	562L4-3	Premium discount for secure behaviour	0
Established vulnerability disclosure framework	2	571L3-1	Established responsible disclosure processes	1	571L4-1	Regular review of vulnerability disclosure policies	0
Established processes against vulnerability information	1	571L3-2	Analysis & dissemination processes	1	571L4-2	Internationally contributing to responsible disclosure	1
Non legal action	0	571L3-3	Deadlines of update	0	571L4-3	Deadlines of update complied	0
					571L4-4	Reviewing process of deadlines	0

Appendix G U.K. Action Items Allocated to Tentative ANC3T

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
5105-1	Blocking known malware sources	521L3-2	541L4-1	541L4-3			Investment to new technologies in internet infrastructures
5105-2	Promoting email verification systems	541L3-1	541L3-2				User side security controls
5105-3	Promoting security best practices	511L2-4	511L3-3				Promotion of use of standards & best practices
5105-4	Implementing secure routing	521L3-2	541L4-1				Investment to new technologies in internet infrastructures
5105-5	Enhancing capabilities against state-sponsored cyber activities	152L3-1	152L4-1				Advanced capabilities & situational awareness
5105-6	Promoting technical development	541L4-1					Continuous assess of technical security controls
5106-1	Metrics	511L2-3	511L2-5				Metrics of adoption of standards & best practices
5205-1	Security settings by default	513L3-1	531L2-2	541L2-5			Security consideration in all stages
5205-2	Developing IP reputation informing service	222L2-2	222L4-2	521L3-2			Risk reduction in e-gov
5205-3	Software integrity assuarance	512L3-1	531L3-4				Standards & best practices for procurement widely used & complied
5205-4	Promoting out-of-date browsers filtering	222L2-2	222L4-2	511L2-4			Risk reduction in e-gov
5205-5	Investing new technologies like TPM, FIDO	222L2-2	222L4-2	521L3-2	541L4-1	551L4-2	Risk reduction in e-gov
5206-1	Introducing security ratings for products	531L2-4	561L3-1				Software classification
5207-1	Metrics	513L2-1					Metrics of adoption of standards & best practices for development
5303-1	Promoting e-government	222L2-3					Promotion of e-gov
5303-2	'Security-by-default' in e-government	222L4-2	513L3-1				Data protection measures of e-gov
5304-1	Eliminating unsupported softwares in public sector	512L3-1	541L2-1				Standards & best practices for procurement widely used & complied
5305-1	Comprehensive knowledge about all public sector systems	511L2-2					Standards & best practices widely used
5305-2	Promoting best practices in public sector	511L2-4					Promotion of use of standards & best practices
5305-3	Cyber exercise	111L3-2	124L2-1	141L2-1			Cyber exercises considered in strategy
5305-4	Participation of lower levels of public sector	123L3-1					Subnational / sectorial incident response organisations
5305-5	Automated vulnerability scan on e-government	222L4-2	541L2-1				Data protection measures of e-gov
5306-1	Awarenes raising in public sector	211L4-1	311L3-1				Mind-set commonplace in public sector
5306-2	Development of cyber expertise	311L3-1	331L3-2				Sector specific programmes of awareness raising
5307-1	Developing new guidance	511L3-3	541L4-1				Contributing to international standards
5307-2	Making cyber threat infomation easily available	121L2-1	311l2-3				Central registry of incidents
5308-1	Improving highest classification networks	161L3-1					Redundant communications for key stakeholders
5309-1	Promoting new standards in health & care industries	511L2-4					Promotion of use of standards & best practices
5310-1	Awareness raising in Armed Forces	311L3-1					Sector specific programmes of awareness raising
5310-2	Enhancing detection & reaction functions	152L3-1	152L4-1				Advanced capabilities & situational awareness
5311-1	Metrics	311L3-2	331L3-4	511L2-5	512L2-3		Metrics for effectiveness of awareness raising programmes
5404-1	Awareness raising of board members	212L3-1	312L4-1				Mind-set spread in private sector
5404-2	Urging organisations & companies to invest in security	312L3-1	312L3-2	541L2-1	541L3-2		Executives' understandings of cybersecurity measures
5404-3	Urging organisations & companies to excercise incident response	331L2-4	332L2-1				Cybersecurity training programmes for non-professionals
5404-4	Cybersecurity in CNI	131L3-2	132L3-3	133L3-1	133L3-2	133L3-3	Vulnerability & asset management of CI assets
5405-1	Government to understand cybersecurity levels in CNI	131L4-1	132L4-2				Regular review of CI risk priorities
5406-1	Sharing information with CNI	132L2-1					Information sharing established between CI & government

Allocation (Requirement Keyword)			
2	3	4	5
Continuous assess of technical security controls	Supplemental security services by ISPs		
Regular review of technical security controls			
Contributing to international standards			
Continuous assess of technical security controls			
Cross-border response ability			
Metrics of compliance of standards & best practices			
Softwares complying with international standards	Technical security controls based on international frameworks		
Data protection measures of e-gov	Investment to new technologies in internet infrastructures		
Software deficiency handling			
Data protection measures of e-gov	Promotion of use of standards & best practices		
Data protection measures of e-gov	Investment to new technologies in internet infrastructures	Continuous assess of technical security controls	Revision of cryptographic control policies
Security products complied to International standards			
Security consideration in all stages			
Latest technical controls & patch managements widely implemented			
Incident response processes & tools established	National incident exercise done		
Latest technical controls & patch managements widely implemented			
Sector specific programmes of awareness raising			
Cybersecurity training aligned with national strategy			
Continuous assess of technical security controls			
Cybersecurity information portal			
Cross-border response ability			
Metrics of effectiveness of cybersecurity training	Metrics of compliance of standards & best practices	Metrics of compliance of standards & best practices for procurement	
Cybersecurity as common agenda in board meetings			
Executives' ability to reallocate resources	Latest technical controls & patch managements widely implemented	Regular review of technical security controls	
Cybersecurity trained & certified employees			
Supply chain management of CI	Cybersecurity oriented risk management in CI	Regular review of impact analysis of CI	Regular review of CI incident response plans
Trust between CI & government			

Appendix G

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
5406-2	Setting a new standard by collaborating with industries & academia	132L4-1	511L3-3				Ability to adjust of CI protection
5406-3	Encouraging investment in the latest technologies	133L3-4	141L3-4	161L3-3			Regular review of resource allocation for CI protection
5406-4	Exercising with CNI	141L3-1					High-level scenario of national incident exercise
5408-1	Private sector mind-set	212L4-1					Mind-set commonplace in private sector
5408-2	Flexible policies for private sector cybersecurity	411L4-1					Balance between cybersecurity legal framework & best practices
5408-3	Promoting growth of cybersecurity industries	541L4-1	561L3-1	561L4-2			Continuous assess of technical security controls
5408-4	Coordinating international legal framework	411L4-1	411L4-2	412L4-3	412L4-4	416L4-1	Balance between cybersecurity legal framework & best practices
5409-1	Cybersecurity as a regulation	411L4-1					Balance between cybersecurity legal framework & best practices
5410-1	Metrics	112L4-1	131L4-1	132L4-1			Reassignment & reallocation of resources for cybersecurity programme
5503-1	Public awareness raising	213L3-1	222L3-3	223L3-2	311L4-3		Most users have mind-set
5504-1	Using cybersecurity insurance for corporate awareness raising	562L4-1	562L4-3				Innovative cybersecurity insurance market
5505-1	Making information, education, tools easily available to public & corporates	212L4-1	213L4-1	311L4-3	311L4-4		Mind-set commonplace in private sector
5505-2	Intelligence sharing between government & law enforcement	432L3-1					Established relationship among government, prosecutors, judges & law enforcement
5606-1	Enhancing cooperation in incident response between government & private sector	123L3-3	123L4-1				Information sharing across sectors
5606-2	Performing inter-sectoral exercise	141L2-1					National incident exercise done
5607-1	Trust between government & private sector	141L3-2					Trust between participants of national incident exercise
5608-1	Automated information sharing system	123L3-3					Information sharing across sectors
5609-1	Metrics	141L3-4	141L4-4	161L3-3			Evaluation of national incident exercise informing investment
6205-1	Enhancing law enforcement capability in national, regional & local levels	421L3-1	422L4-2				Dedicated investigative resources for cybercrimes
6205-2	Making UK inefficient cybercrime target based on understanding of cybercrime business model	421L3-2	421L3-5				Advanced investigative capabilities for cybercrimes
6205-3	International juridical partnership	417L4-1	418L4-1	421L3-4	422L4-1	432L3-3	Contributing to international cybercrime treaties
6205-4	Discouraging individuals being involved in cybercrime	311L4-3	311L4-4				Entire society involved in awareness raising
6205-5	Exchanging intelligence with industry	123L3-3	431L2-1				Information sharing across sectors
6205-6	New 24/7 reporting system	121L2-1	241L2-1	241L2-2			Central registry of incidents
6205-7	Reducing vulnerabilities in infrastructures	131L3-2	521L2-3	541L2-1			Vulnerability & asset management of CI assets
6205-8	Making use of stolen credentials difficult in UK	411L3-1	415L4-1				Regular review of cybersecurity legal framework
6206-1	Metrics	417L4-2	418L4-2	421L4-3	423L4-2		Regular review of substantive cybercrime legislation
6303-1	Applying international law in cyberspace	152L4-1	153L4-1				Cross-border response ability
6303-2	Confidence building	111L4-2					Contributing to international debate of strategy
6303-3	Enhancing NATO cooperation	141L4-2	153L4-2				National incident exercise contributing to international challenges
6303-4	Understanding cyber activity of adversaries	151L3-2	152L3-1	153L3-1			Capturing landscape of national-level threat
6303-5	Generating all available options	152L3-1	153L3-1	153L3-2			Advanced capabilities & situational awareness
6303-6	Intenational information sharing	153L4-2					Intelligence shared with allies
6303-7	Attributing specific identities	153L4-1					Leading international debate about cyber defence
6304-1	Metrics	151L3-3					Cyber defence strategy meets objectives
6403-1	Enhancing detection of cyber terrorism	151L3-2	152L3-1	153L2-1	421L3-2		Capturing landscape of national-level threat

Allocation (Requirement Keyword)			
2	3	4	5
Contributing to international standards			
Evaluation of national incident exercise informing investment	Evaluation of national incident exercise informing investment		
Security products complied to International standards	Exporting superior security products		
Participation to international cooperation agreements	Contributing to international digital human rights	Contributing to international privacy protection online	Balance between intellectual property & open access policy
Regular review of CI risk priorities	Ability to adjust of CI protection		
Most users can use e-gov securely	Most users can use e-commerce securely	Entire society involved in awareness raising	
Premium discount for secure behaviour			
Users' mind-set reducing threat	Entire society involved in awareness raising	Overall threat reduced by awareness raising	
Coordinating all levels / sectors			
National crisis management established	Evaluation of national incident exercise informing investment		
Dedicated prosecutorial resources for cybercrimes			
Statistics & analysis of cybercrime investigations			
Contributing to international cybercrime treaties	Cross-border investigation of cybercrimes	Prosecution of cross-border cybercrimes	Joint international investigation & prosecution
Overall threat reduced by awareness raising			
Established formal international cooperation			
Incident reporting mechanisms established	Promotion of incident reporting channels		
Internet infrastructures compliant to international standards & best practices	Latest technical controls & patch managements widely implemented		
Amendment procedures for consumer protection legislation			
Regular review of procedural cybercrime legislation	Regular review of investigative capabilities for cybercrimes	Regular review of court system capabilities to judge cybercrimes	
Leading international debate about cyber defence			
Intelligence shared with allies			
Advanced capabilities & situational awareness	Analytical capability in cyber defence		
Analytical capability in cyber defence	Strengths & weaknesses of cyber defence understood		
Advanced capabilities & situational awareness	Coordination between CI & defence	Advanced investigative capabilities for cybercrimes	

Appendix G

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
6403-2	Enhancing investigation of cyber terrorism	421L3-2	421L3-4				Advanced investigative capabilities for cybercrimes
6403-3	International cooperation	153L4-2	431L3-1	432L3-3			Intelligence shared with allies
6404-1	Metrics	421L4-3	431L4-1	432L4-2			Regular review of investigative capabilities for cybercrimes
6503-1	Enhancing development of cyber HR	321L3-4	322L3-2	322L4-2	322L4-3		Cybersecurity as focusing area
6503-2	Developing offensive cyber capability	152L3-1	321L4-3	541L4-1	561L4-2		Advanced capabilities & situational awareness
6503-3	Integrating offensive cyber capability to armed forces	152L3-1	152L4-1				Advanced capabilities & situational awareness
6504-1	Metrics	151L3-3	541L4-1				Cyber defence strategy meets objectives
6603-1	Creating new requirement of cryptography	551L4-1	551L4-2				Regular review of relevance of cryptographic controls
6604-1	Metrics	551L4-1					Regular review of relevance of cryptographic controls
7106-1	Including cybersecurity into computer science education	321L3-2	321L3-4				Mandatory cybersecutity courses for computer science degrees
7107-1	Making clear rolls of government & private sector in cybersecurity training	331L3-2	331L4-1	332L3-2			Cybersecurity training aligned with national strategy
7107-2	Urging corporate management to train employees	331L3-2	332L3-2				Cybersecurity training aligned with national strategy
7107-3	More attractive careers of cybersecurity professionals	331L4-3					Incentives for cybersecurity trained workforce
7108-1	Inter-sectoral coordination of education/training	322L4-2	331L4-1	331L4-2			Cooperation between all stakeholders in cybersecurity education
7109-1	Specialist education targeting 14-18 years	321L3-3	321L4-1				Cybersecurity specific degree
7109-2	Degree-level apprenticeship in energy, finance & transport	322L4-3	332L3-2				Cybersecurity education aligned with practical problems
7109-3	Retraining funds	332L3-1					Review of cybersecurity training programmes
7109-4	Supporting high quality post graduate education	321L3-3					Cybersecurity specific degree
7109-5	Accredition of teachers	321L2-1					Qualification for cybersecurity educators established
7109-6	Identifying excellent organisation	331L3-2	331L4-3				Cybersecurity training aligned with national strategy
7109-7	Defence cyber academy to CoE	322L3-4	322L4-1	331L3-2			CoE in cybersecurity
7109-8	Collaborating between government, forces, industry & academia	322L4-2	331L4-1				Cooperation between all stakeholders in cybersecurity education
7109-9	CyberFirst: nurturing young talent programme	321L3-5					Cybersecurity education from primary to post-graduate
7109-10	Cybersecurity education from primary to postgraduate	321L3-5					Cybersecurity education from primary to post-graduate
7110-1	Metrics	321L4-3	331L3-4				Cybersecurity education adapting to changing needs
7203-1	Supporting commercialisation of academic innovation	321L4-2	322L4-1	322L4-3	561L4-2		Balance between core components & adaptive processes
7203-2	Establishing innovation centres	321L4-2	322L4-1	322L4-3	561L4-2		Balance between core components & adaptive processes
7203-3	Allocating funds	322L4-2	561L4-2				Cooperation between all stakeholders in cybersecurity education
7203-4	Providing testing facilities	561L4-2					Exporting superior security products
7203-5	Enhancing cooperation between industry & government	322L4-2					Cooperation between all stakeholders in cybersecurity education
7203-6	Supporting scaling-up	561L4-2					Exporting superior security products
7203-7	Promoting international standards for easier market access	561L3-1	561L4-2				Security products complied to International standards
7204-1	Easier access to government procurement for start-ups	561L3-1	561L4-2				Security products complied to International standards
7205-1	Metrics	321L4-3					Cybersecurity education adapting to changing needs
7303-1	Making research funding more effective	321L2-5	322L2-2	322L3-2	322L4-1		Research & development in cybersecurity promoted
7303-2	Human & behavioural aspects of cyber science	321L2-5	322L2-2	322L3-2	322L4-1		Research & development in cybersecurity promoted
7304-1	Enhancing 'secure-by-default'	513L3-1	561L3-1				Security consideration in all stages
7305-1	Establishing Cyber Science and Technology Strategy	321L2-5	322L2-2	322L3-2	322L4-1		Research & development in cybersecurity promoted

Allocation (Requirement Keyword)			
2	3	4	5
Cross-border investigation of cybercrimes			
Communication channels for international cooperation	Joint international investigation & prosecution		
Regular review of international cooperation	Adapted international cooperation		
Adapted budget for cybersecurity education	Cooperation between all stakeholders in cybersecurity education	Cybersecurity education aligned with practical problems	
Cybersecurity education adapting to changing needs	Continuous assess of technical security controls	Exporting superior security products	
Cross-border response ability			
Continuous assess of technical security controls			
Revision of cryptographic control policies			
Cybersecurity as focusing area			
Collaboration between public & private in cybersecurity training	Coordination of cybersecurity training across sectors		
Coordination of cybersecurity training across sectors			
Collaboration between public & private in cybersecurity training	Coordination between cybersecurity training & education		
Internationally forerunning in cybersecurity education			
Coordination of cybersecurity training across sectors			
Incentives for cybersecurity trained workforce			
International CoE in cybersecurity	Cybersecurity training aligned with national strategy		
Collaboration between public & private in cybersecurity training			
Metrics of effectiveness of cybersecurity training			
International CoE in cybersecurity	Cybersecurity education aligned with practical problems	Exporting superior security products	
International CoE in cybersecurity	Cybersecurity education aligned with practical problems	Exporting superior security products	
Exporting superior security products			
Exporting superior security products			
Exporting superior security products			
Budget for research & education for cybersecurity	Adapted budget for cybersecurity education	International CoE in cybersecurity	
Budget for research & education for cybersecurity	Adapted budget for cybersecurity education	International CoE in cybersecurity	
Security products complied to International standards			
Budget for research & education for cybersecurity	Adapted budget for cybersecurity education	International CoE in cybersecurity	

Appendix G

#	Action Item	Allocation (Requirement ID)					
		1	2	3	4	5	1
7306-1	Supporting academic CoE, research institutes & doctral training	322L3-4	322L4-1				CoE in cybersecurity
7306-2	Establishing new research institute	322L3-4	322L4-1				CoE in cybersecurity
7307-1	Supporting PhD	321L3-3	321L4-1				Cybersecurity specific degree
7308-1	Encouraging collaboration between government, industry & academia	322L4-2					Cooperation between all stakeholders in cybersecurity education
7309-1	Funding 'grand challenge'	321L2-5	322L2-2	322L3-2	322L4-1		Research & development in cybersecurity promoted
7310-1	Metrics	321L4-3					Cybersecurity education adapting to changing needs
7403-1	Promoting inter-disciplinary research for development of horizon scanning	321L4-1					Internationally forerunning in cybersecurity education
7403-2	Integration of cybersecurity & behavioural science	321L4-1					Internationally forerunning in cybersecurity education
7403-3	Monitoring cyber criminal market	421L3-2	421L4-3				Advanced investigative capabilities for cybercrimes
7403-4	Investigating new technologies	541L4-1					Continuous assess of technical security controls
7403-5	-do-	541L4-1					Continuous assess of technical security controls
7403-6	Early defence technology	122L4-2	541L4-1				Early warning capability
7404-1	Including cybersecurity into any other research areas for horizon scanning	321L4-1					Internationally forerunning in cybersecurity education
7407-1	Metrics	321L4-3					Cybersecurity education adapting to changing needs
84---1	Contributing to international debate of international law in cyber space	153L4-1					Leading international debate about cyber defence
84---2	-do-	153L4-1					Leading international debate about cyber defence
84---3	-do-	153L4-1					Leading international debate about cyber defence
84---4	Confidence building measures	111L4-2					Contributing to international debate of strategy
84---5	Cross-border prosecution	417L4-1	418L4-1	422L4-1			Contributing to international cybercrime treaties
84---6	Enhancing law enforcement	421L3-3	421L3-4	432L3-3			Regular training for law enforcement officers
84---7	Promoting international standards & best practices in emerging technologies	311L3-4	511L3-3				Contribution to international awareness raising
84---8	Cross-border cooperation in capabilities & new technologies	161L3-4	161L4-2	541L4-1			Contribution to international communications' redundancy
84---9	Assist other countries to build capabilities	123L3-2	123L4-2	124L3-5	124L4-4	161L4-2	International coordination
84---10	Assist other countries to enhance cybersecurity	123L3-2	123L4-2	124L3-5	124L4-4	161L4-2	International coordination
84---11	Enhancing NATO's capability in cyber space	141L4-2	153L4-2				National incident exercise contributing to international challenges
84---12	-do-	141L4-2	153L4-2				National incident exercise contributing to international challenges
84---13	Contributing international norm development in cyber space	111L4-2	153L4-1				Contributing to international debate of strategy
85---1	Enhancing cooperation with allies	141L4-2	153L4-2				National incident exercise contributing to international challenges
85---2	Contributing to international oganisations	123L3-2	124L3-5				International coordination
85---3	Cooperating international non-government actors	432L4-2					Adapted international cooperation
86---1	Metrics	111L4-1	113L4-1	431L4-1	432L4-2		Continual revision of strategy

Allocation (Requirement Keyword)			
2	3	4	5
International CoE in cybersecurity			
International CoE in cybersecurity			
Internationally forerunning in cybersecurity education			
Budget for research & education for cybersecurity	Adapted budget for cybersecurity education	International CoE in cybersecurity	
Regular review of investigative capabilities for cybercrimes			
Continuous assess of technical security controls			
Contributing to international cybercrime treaties	Prosecution of cross-border cybercrimes		
Cross-border investigation of cybercrimes	Joint international investigation & prosecution		
Contributing to international standards			
Assisting neighbours	Continuous assess of technical security controls		
Regional coordination	International coordination	Regional coordination	Assisting neighbours
Regional coordination	International coordination	Regional coordination	Assisting neighbours
Intelligence shared with allies			
Intelligence shared with allies			
Leading international debate about cyber defence			
Intelligence shared with allies			
International coordination			
Continual revision of strategy	Regular review of international cooperation	Adapted international cooperation	

Appendix H U.K. Action Items Mapping Result by Requirement

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	111L1-1	Outline of strategy	0	111L2-1
				111L1-2	Development process of strategy	0	111L2-2
				111L1-3	Stakeholders involved in strategy development	0	111L2-3
112	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Organisation	112L1-1	Cybersecurity programme under development	0	112L2-1
							112L2-2
							112L2-3
							112L2-4
113	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Content	113L1-1	Risk priorities of cybersecurity defined in strategy	0	113L2-1
							113L2-2
121	Cybersecurity Policy and Strategy	Incident Response	Identification of Incidents	121L1-1	Recording incidents	0	121L2-1
122	Cybersecurity Policy and Strategy	Incident Response	Organisation	122L1-1	Key incident response organisations in private sector identified	0	122L2-1
				122L1-2	N/A	0	122L2-2
				122L1-3	Ad-hoc responses	0	
123	Cybersecurity Policy and Strategy	Incident Response	Coordination	123L1-1	Leading incident response organisation designated	0	123L2-1
							123L2-2
							123L2-3
124	Cybersecurity Policy and Strategy	Incident Response	Mode of Operation	124L1-1	Key incident response processes	0	124L2-1
				124L1-2	CSIRT member training	0	124L2-2
							124L2-3
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	131L1-1	List of CI assets	0	131L2-1
							131L2-2
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	132L1-1	Informal information sharing between CI & government	0	132L2-1
							132L2-2
							132L2-3
							132L2-4
133	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Risk Management and Response	133L1-1	Access control implemented in CI	0	133L2-1
				133L1-2	Basic capacity against cyber threat in CI	0	133L2-2
				133L1-3	Data security policy in CI	0	133L2-3
141	Cybersecurity Policy and Strategy	Crisis Management	Crisis Management	141L1-1	Assessment of exercise of national incident	0	141L2-1
				141L1-2	Exercise planning organisation designated for national incident	0	141L2-2
				141L1-3	Stakeholders' participation in national incident exercise	0	141L2-3
							141L2-4
							141L2-5
							141L2-6

Nb. = Number of Related Action Items

Level 2		Level 3			Level 4		
Keywords	**Nb.**	ID	Keywords	**Nb.**	ID	Keywords	**Nb.**
Strategy established	0	111L3-1	Reviewing process of strategy	0	111L4-1	Continual revision of strategy	1
Stakeholders' consultation in strategy	0	111L3-2	Cyber exercises considered in strategy	1	111L4-2	Contributing to international debate of strategy	3
Implementation of strategy	0	111L3-3	Measurement of cybersecurity defined in strategy	0			
		111L3-4	Capacity building & investment considered in strategy	0			
Cybersecurity programme agreed	0	112L3-1	PDCA processes of cybersecurity programme	0	112L4-1	Reassignment & reallocation of resources for cybersecurity programme	1
Coordinating body of cybersecurity programme	0	112L3-2	Consolidated budget for cybersecurity	0	112L4-2	Dissemination & feedbacks about cybersecurity programme	0
Goals & measurement of cybersecurity programme	0						
Discrete budget for cybersecurity	0						
National objectives of cybersecurity defined in strategy	0	113L3-1	Measurement of cybersecurity defined in strategy	0	113L4-1	Continual revision of strategy	1
Minimum coverage of strategy contents	0	113L3-2	Protection of critical infrastructures defined in strategy	0	113L4-2	Contributing to international cooperation	0
Central registry of incidents	2	121L3-1	Regular revision of incident registry	0	121L4-1	Adapted analysis of incidents	0
		121L3-2	Incident analysis	0			
National CSIRT	0	122L3-1	Formal roles & responsibilities allocated	0	122L4-1	Sustainability of incident response capability	0
Roles & responsibilities of national CSIRT	0	122L3-2	Adequate resources for incident response	0	122L4-2	Early warning capability	1
					122L4-3	Capability to manage threat landscape	0
Coordination established	0	123L3-1	Subnational / sectorial incident response organisations	1	123L4-1	Coordinating all levels / sectors	1
Communication lines for crisis	0	123L3-2	International coordination	3	123L4-2	Regional coordination	2
International cooperation in incident response	0	123L3-3	Information sharing across sectors	3			
Incident response processes & tools established	1	124L3-1	Training & accreditation for CSIRT members established	0	124L4-1	Scenario testing of incident response processes	0
Regular training for CSIRT members	0	124L3-2	Sophisticated incident analysis	0	124L4-2	Evaluating effectiveness of CSIRT members training	0
Limited response to national level incidents	0	124L3-3	Regular review of incident response processes	0	124L4-3	Tools against zero-day vulnerabilities	0
		124L3-4	Forensics	0	124L4-4	Regional coordination	2
		124L3-5	International coordination	3			
Audit of CI assets	0	131L3-1	Priority of CI risks	0	131L4-1	Regular review of CI risk priorities	2
CI assets audit list	0	131L3-2	Vulnerability & asset management of CI assets	2			
Information sharing established between CI & government	1	132L3-1	Centralised management of CI protection	0	132L4-1	Ability to adjust of CI protection	2
Formal & consistent information sharing between CI & government	0	132L3-2	Public awareness campaign of CI protection	0	132L4-2	Trust between CI & government	1
Point of contact	0	132L3-3	Supply chain management of CI	1			
Government engagement in CI protection	0						
Standards & best practices in CI	0	133L3-1	Cybersecurity oriented risk management in CI	1	133L4-1	Regular audit of CI	0
Risk management processes in CI	0	133L3-2	Regular review of impact analysis of CI	1	133L4-2	Indirect costs inclusive in impact analysis of CI incidents	0
National CI incident response plan	0	133L3-3	Regular review of CI incident response plans	1			
		133L3-4	Regular review of resource allocation for CI protection	1			
		133L3-5	Insider threat detection in CI	0			
National incident exercise done	2	141L3-1	High-level scenario of national incident exercise	1	141L4-1	Peer observance of national incident exercise	0
Appropriate resources for national incident exercise	0	141L3-2	Trust between participants of national incident exercise	1	141L4-2	National incident exercise contributing to international challenges	4
Roles in national incident exercise defined	0	141L3-3	SMART objectives & KPI of national incident exercise	0	141L4-3	Internationally shared result of national incident exercise	0
Incentives to participate in national incident exercise	0	141L3-4	Evaluation of national incident exercise informing investment	2	141L4-4	National crisis management established	1
Trained monitors of national incident exercise	0	141L3-5	National crisis management aligned with international best practices	0			
Evaluation of national incident exercise	0	141L3-6	Tailored reports of national incident exercise	0			

Appendix H

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
151	Cybersecurity Policy and Strategy	Cyber Defence	Strategy	151L1-1	National-level threats identified	0	151L2-1
152	Cybersecurity Policy and Strategy	Cyber Defence	Organisation	152L1-1	Dispersed cyber operations	0	152L2-1
153	Cybersecurity Policy and Strategy	Cyber Defence	Coordination	153L1-1	Cyber defence capability requirements agreed	0	153L2-1
							153L2-2
161	Cybersecurity Policy and Strategy	Communications Redundancy	Communications Redundancy	161L1-1	Gaps in emergency communication identified	0	161L2-1
				161L1-2	Emergency procedures established	0	161L2-2
							161L2-3
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	211L1-1	Leading agencies only have mind-set	0	211L2-1
212	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	212L1-1	Leading firms only have mind-set	0	212L2-1
				212L1-2	Materials for best practices available	0	
213	Cyber Culture and Society	Cybersecurity Mind-set	Users	213L1-1	Limited users only have mind-set	0	213L2-1
221	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	221L1-1	A few users can use internet securely	0	221L2-1
				221L1-2	Promotion of online trust exists	0	221L2-2
							221L2-3
222	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-government Services	222L1-1	Government's recognition of needs for security in e-gov	0	222L2-1
				222L1-2	Stakeholders' recognition of needs for security in e-gov	0	222L2-2
				222L1-3	A few users can use e-gov securely	0	222L2-3
				222L1-4	Security measures in e-gov	0	222L2-4
							222L2-5
223	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-commerce Services	223L1-1	Limited e-commerce provided	0	223L2-1
				223L1-2	Private sectors' recognition of need for security in e-commerce	0	223L2-2
				223L1-3	A few users can use e-commerce securely	0	223L2-3
				223L1-4	Security measures in e-commerce	0	223L2-4
							223L2-5
231	Cyber Culture and Society	User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	231L1-1	Users have only general knowledge about personal information protection	0	231L2-1
				231L1-2	Discussions on protecting personal information	0	231L2-2
241	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	241L1-1	Reporting channels of incidents	0	241L2-1
							241L2-2
251	Cyber Culture and Society	Media and Social Media	Media and Social Media	251L1-1	Media coverage of cybersecurity	0	251L2-1
				251L1-2	Discussion on social media security	0	251L2-2
							251L2-3

Level 2		Level 3			Level 4		
Keywords	Nb.	ID	Keywords	Nb.	ID	Keywords	Nb.
Cyber defence strategy exists	0	151L3-1	Dedicated resources for cyber defence	0	151L4-1	Rules of engagement in cyberspace	0
		151L3-2	Capturing landscape of national-level threat	2	151L4-2	Military doctrine in cyberspace	0
		151L3-3	Cyber defence strategy meets objectives	2			
Defined responsibility of cyber defence organisation	0	152L3-1	Advanced capabilities & situational awareness	7	152L4-1	Cross-border response ability	4
Coordination between CI & defence	1	153L3-1	Analytical capability in cyber defence	2	153L4-1	Leading international debate about cyber defence	6
Intelligence sharing between CI & defence	0	153L3-2	Strengths & weaknesses of cyber defence understood	1	153L4-2	Intelligence shared with allies	6
Emergency response assets hardwired	0	161L3-1	Redundant communications for key stakeholders	1	161L4-1	Optimised for extended outages	0
Communication between emergency response functions distributed	0	161L3-2	Interoperability & functionality under compromised situation	0	161L4-2	Assisting neighbours	3
Testing, training, drills of emergency response	0	161L3-3	Evaluation of national incident exercise informing investment	2			
		161L3-4	Contribution to international communications' redundancy	1			
Most officials have mind-set	0	211L3-1	Mind-set spread in public sector	0	211L4-1	Mind-set commonplace in public sector	1
		211L3-2	Mind-set based strategy in public sector	0			
Most private sector actors have mind-set	0	212L3-1	Mind-set spread in private sector	1	212L4-1	Mind-set commonplace in private sector	2
		212L3-2	Mind-set based strategy in private sector	0			
Growing number of users have mind-set	0	213L3-1	Most users have mind-set	1	213L4-1	Users' mind-set reducing threat	1
Growing number of users can use internet securely	0	221L3-1	Most users can use internet securely	0	221L4-1	Users can evaluate risk & adjust behaviour	0
Promotion of online trust established	0	221L3-2	Users' ability to control providing personal information	0	221L4-2	Promotion of online trust revised	0
User assistance available	0	221L3-3	Promotion of online trust evaluated	0			
E-gov established	0	222L3-1	Disclosures of activities of government agencies	0	222L4-1	Promotion of e-gov revised	0
Risk reduction in e-gov	3	222L3-2	Privacy-by-default in e-gov	0	222L4-2	Data protection measures of e-gov	5
Promotion of e-gov	1	222L3-3	Most users can use e-gov securely	1			
Growing number of users can use e-gov securely	0	222L3-4	User feedbacks for e-gov	0			
Incident disclosure in e-gov	0						
E-commerce established	0	223L3-1	Resource allocation for e-commerce	0	223L4-1	Continuous improvement of e-commerce	0
Secure payment	0	223L3-2	Most users can use e-commerce securely	1	223L4-2	Clear terms & conditions of e-commerce	0
Growing number of users can use e-commerce securely	0	223L3-3	Investment for e-commerce	0	223L4-3	User feedbacks for e-commerce	0
Promotion of trust of e-commerce	0						
Terms & conditions of e-commerce accessible	0						
Growing number of users can secure personal information online	0	231L3-1	Measures to protect personal information online	0	231L4-1	Users can adapt to changing environments	0
Discussions on balance between security & privacy	0	231L3-2	Privacy rights	0	231L4-2	Wide recognition about personal information protection	0
		231L3-3	Security & privacy balanced	0	231L4-3	Security & privacy balanced in changing environment	0
		231L3-4	Privacy-by-default	0	231L4-4	Regular assessment of privacy protection	0
Incident reporting mechanisms established	1	241L3-1	Coordination of incident reporting channels	0	241L4-1	Regular enhancement of incident reporting	0
Promotion of incident reporting channels	1	241L3-2	Promotion of incident reporting channels prioritised	0	241L4-2	Coordination of response to reported incidents	0
		241L3-3	Metrics of incident reporting	0			
Cybersecurity as common subject in media	0	251L3-1	Media coverage of information about cybersecurity measures	0	251L4-1	Discussion changing policy & society	0
Wide range of issues of cybersecurity in media	0	251L3-2	Frequent discussion on social media security	0			
Broad discussion on social media security	0						

Appendix H

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	311L1-1	Awareness raising programmes	0	311L2-1
				311L1-2	Awareness raising programmes affected by international initiatives	0	311L2-2
							311L2-3
312	Cybersecurity Education, Training and Skills	Awareness Raising	Executive Awareness Raising	312L1-1	Executives' awareness about general cybersecurity issues	0	312L2-1
				312L1-2	Executives of particular sectors have awareness	0	312L2-2
							312L2-3
321	Cybersecurity Education, Training and Skills	Framework for Education	Provision	321L1-1	Qualification programme for cybersecurity educators	0	321L2-1
				321L1-2	Professional cybersecurity educators	0	321L2-2
				321L1-3	Educational courses for cybersecurity	0	321L2-3
				321L1-4	Demand exists for cybersecurity education	0	321L2-4
							321L2-5
322	Cybersecurity Education, Training and Skills	Framework for Education	Administration	322L1-1	Cybersecurity education needs recognised	0	322L2-1
				322L1-2	Ad-hoc supply of resources for cybersecurity education	0	322L2-2
							322L2-3
331	Cybersecurity Education, Training and Skills	Framework for Professional Training	Provision	331L1-1	Cybersecurity training needs recognised	0	331L2-1
				331L1-2	Cybersecurity training for general IT staff	0	331L2-2
				331L1-3	ICT certification with some cybersecurity issues	0	331L2-3
				331L1-4	Training courses for cybersecurity	0	331L2-4
332	Cybersecurity Education, Training and Skills	Framework for Professional Training	Uptake	332L1-1	Metrics of uptake of cybersecurity trainings	0	332L2-1
							332L2-2
							332L2-3
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	411L1-1	Discussion of establishing cybersecurity legal framework	0	411L2-1
				411L1-2	Priorities identified in cybersecurity legal framework	0	411L2-2
412	Legal and Regulatory Frameworks	Legal Framework	Privacy, Freedom of Speech & Other Human Rights Online	412L1-1	Partial privacy protection legislation	0	412L2-1
				412L1-2	Freedom of expression	0	412L2-2
				412L1-3	Discussion of establishing digital human rights legislation	0	412L2-3
							412L2-4
							412L2-5
413	Legal and Regulatory Frameworks	Legal Framework	Data Protection Legislation	413L1-1	Partial data protection legislation	0	413L2-1
				413L1-2	Stakeholders' participation in data protection legislation	0	413L2-2
414	Legal and Regulatory Frameworks	Legal Framework	Child Protection Online	414L1-1	Partial online child protection legislation	0	414L2-1
				414L1-2	Stakeholders' participation in online child protection legislation	0	414L2-2

Level 2		Level 3			Level 4		
Keywords	Nb.	ID	Keywords	Nb.	ID	Keywords	Nb.
National programme of awareness raising	0	311L3-1	Sector specific programmes of awareness raising	3	311L4-1	Awareness raising programmes adapted according to effectiveness	0
Consultation with stakeholders in national programme of awareness raising	0	311L3-2	Metrics for effectiveness of awareness raising programmes	1	311L4-2	Revision of national awareness raising programme	0
Cybersecurity information portal	1	311L3-3	Evolution of awareness raising programmes	0	311L4-3	Entire society involved in awareness raising	3
		311L3-4	Contribution to international awareness raising	1	311L4-4	Overall threat reduced by awareness raising	2
Executives' basic understandings of cybersecurity	0	312L3-1	Executives' understandings of cybersecurity measures	1	312L4-1	Cybersecurity as common agenda in board meetings	1
Limited executives' understandings of cybersecurity's affect	0	312L3-2	Executives' ability to reallocate resources	1	312L4-2	Executives' attitude as international role model	0
Raising programmes for awareness of crisis management	0	312L3-3	Executives' understanding of crisis management plans	0			
		312L3-4	Mandatory cybersecurity education for executives	0			
Qualification for cybersecurity educators established	1	321L3-1	Business experts' participation in cybersecurity education	0	321L4-1	Internationally forerunning in cybersecurity education	5
University level courses for cybersecurity	0	321L3-2	Mandatory cybersecutity courses for computer science degrees	1	321L4-2	Balance between core components & adaptive processes	2
Degrees in cybersecurity	0	321L3-3	Cybersecurity specific degree	3	321L4-3	Cybersecurity education adapting to changing needs	5
Seminars for non-specialist	0	321L3-4	Cybersecurity as focusing area	2			
Research & development in cybersecurity promoted	4	321L3-5	Cybersecurity education from primary to post-graduate	2			
Broad discussion for enhancing cybersecurity education	0	322L3-1	Cybersecurity education demand/supply monitored	0	322L4-1	International CoE in cybersecurity	9
Budget for research & education for cybersecurity	4	322L3-2	Adapted budget for cybersecurity education	5	322L4-2	Cooperation between all stakeholders in cybersecurity education	6
Attractiveness of cybersecurity career	0	322L3-3	International cooperation in cybersecurity education	0	322L4-3	Cybersecurity education aligned with practical problems	4
		322L3-4	CoE in cybersecurity	3			
Structured cybersecurity training programmes	0	331L3-1	Cybersecurity training aligned with international best practices	0	331L4-1	Collaboration between public & private in cybersecurity training	3
Security professional certification	0	331L3-2	Cybersecurity training aligned with national strategy	5	331L4-2	Coordination between cybersecurity training & education	1
Cybersecurity training requirements listed	0	331L3-3	Communication skills in cybersecurity training	0	331L4-3	Incentives for cybersecurity trained workforce	2
Cybersecurity training programmes for non-professionals	1	331L3-4	Metrics of effectiveness of cybersecurity training	2			
Cybersecurity trained & certified employees	1	332L3-1	Review of cybersecurity training programmes	1	332L4-1	Cybersecurity trained professionals internationally contributing	0
Knowledge transfer in cybersecurity	0	332L3-2	Coordination of cybersecurity training across sectors	3			
Job creation in cybersecurity	0						
Cybersecurity legal framework established	0	411L3-1	Regular review of cybersecurity legal framework	1	411L4-1	Balance between cybersecurity legal framework & best practices	3
Coverages of cybersecurity legal framework	0				411L4-2	Participation to international cooperation agreements	1
					411L4-3	Exceeding minimum requirement of international cooperation agreement	0
Online privacy protected	0	412L3-1	Cybersecurity legal framework aligned with international best practices	0	412L4-1	Amendment procedures for cybersecurity legal framework	0
Freedom of expression protected	0	412L3-2	Exceeding minimum requirement of international agreement	0	412L4-2	Internet access as human right	0
Privacy protected during investigation	0				412L4-3	Contributing to international digital human rights	1
Stakeholders' participation to discuss digital human rights legislation	0				412L4-4	Contributing to international privacy protection online	1
Participation to international agreements	0						
Data protection legislation established	0	413L3-1	Timeframe of storing personal data during investigation	0	413L4-1	Amendment procedures for data protection legislation	0
Personal data protected	0	413L3-2	Data protection legislation aligned with international best practices	0			
Online child protection legislation established	0	414L3-1	Online child protection legislation aligned with international best practices	0	414L4-1	Amendment procedures for online child protection legislation	0
Legal minors protected	0						

Appendix H

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
415	Legal and Regulatory Frameworks	Legal Framework	Consumer Protection Legislation	415L1-1	Partial consumer protection legislation	0	415L2-1
				415L1-2	Stakeholders' participation in consumer protection legislation	0	415L2-2
416	Legal and Regulatory Frameworks	Legal Framework	Intellectual Property Legislation	416L1-1	Partial intellectual property legislation	0	416L2-1
				416L1-2	Stakeholders' participation in intellectual property legislation	0	
417	Legal and Regulatory Frameworks	Legal Framework	Substantive Cybercrime Legislation	417L1-1	Partial substantive cybercrime legislation	0	417L2-1
							417L2-2
418	Legal and Regulatory Frameworks	Legal Framework	Procedural Cybercrime Legislation	418L1-1	Partial procedural cybercrime legislation	0	418L2-1
							418L2-2
421	Legal and Regulatory Frameworks	Criminal Justice System	Law Enforcement	421L1-1	Limited digital forensics capabilities in law enforcement	0	421L2-1
				421L1-2	Training for law enforcement officers	0	421L2-2
							421L2-3
422	Legal and Regulatory Frameworks	Criminal Justice System	Prosecution	422L1-1	Limited capabilities to prosecute cybercrimes	0	422L2-1
				422L1-2	Training for prosecutors	0	
423	Legal and Regulatory Frameworks	Criminal Justice System	Courts	423L1-1	Limited capabilities to judge cybercrimes	0	423L2-1
				423L1-2	Training for judges	0	423L2-2
431	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Formal Cooperation	431L1-1	Formal international cooperation against cybercrimes	0	431L2-1
				431L1-2	Exchange of information between public & private sectors about cybercrimes	0	431L2-2
							431L2-3
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to Combat Cybercrime	Informal Cooperation	432L1-1	Exchange of information between government & justice about cybercrimes	0	432L2-1
				432L1-2	Cooperation between ISPs & law enforcement	0	432L2-2
				432L1-3	Informal international cooperation in law enforcement	0	432L2-3
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	511L1-1	Standards for information risk management	0	511L2-1
				511L1-2	Standards for information risk management partly used	0	511L2-2
				511L1-3	International standards & best practices implemented	0	511L2-3
							511L2-4
							511L2-5
							511L2-6

Level 2		Level 3			Level 4		
Keywords	Nb.	ID	Keywords	Nb.	ID	Keywords	Nb.
Consumer protection legislation established	0	415L3-1	Consumer protection legislation aligned with international best practices	0	415L4-1	Amendment procedures for consumer protection legislation	1
Responsible agency designated for consumer protection	0						
Intellectual property legislation established	0	416L3-1	Intellectual property legislation aligned with international best practices	0	416L4-1	Balance between intellectual property & open access policy	1
		416L3-2	Stakeholders' participation in amendment of intellectual property legislation	0			
Substantive cybercrime legislation exists	0	417L3-1	Exceeding minimum requirement in international agreements on cybercrime	0	417L4-1	Contributing to international cybercrime treaties	2
Participation to international agreements on cybercrime	0	417L3-2	Amendment procedures for substantive cybercrime legislation	0	417L4-2	Regular review of substantive cybercrime legislation	1
Procedural cybercrime legislation exists	0	418L3-1	Procedural cybercrime legislation enables cross-border investigation	0	418L4-1	Contributing to international cybercrime treaties	2
Participation to international agreements on cybercrime	0	418L3-2	Exceeding minimum requirement in international agreements on cybercrime	0	418L4-2	Regular review of procedural cybercrime legislation	1
		418L3-3	Amendment procedures for procedural cybercrime legislation	0			
Comprehensive investigative capabilities for cybercrimes	0	421L3-1	Dedicated investigative resources for cybercrimes	1	421L4-1	Specialised and continuous training for law enforcement officers	0
Established chain of custody of digital evidence	0	421L3-2	Advanced investigative capabilities for cybercrimes	4	421L4-2	Sophisticated digital forensic tools	0
Standards for training for law enforcement officers	0	421L3-3	Regular training for law enforcement officers	1	421L4-3	Regular review of investigative capabilities for cybercrimes	3
		421L3-4	Cross-border investigation of cybercrimes	3			
		421L3-5	Statistics & analysis of cybercrime investigations	1			
Comprehensive prosecutorial capabilities for cybercrimes	0	422L3-1	Institutional structures in prosecution services	0	422L4-1	Prosecution of cross-border cybercrimes	2
		422L3-2	Statistics & analysis of cybercrime prosecutions	0	422L4-2	Dedicated prosecutorial resources for cybercrimes	1
		422L3-3	Exchange of best practices between prosecutors & judges	0	422L4-3	Specialised and continuous training for prosecutors	0
Sufficient jurisdictional capabilities for cybercrimes	0	423L3-1	Centralised judges for cybercrimes	0	423L4-1	Specialised and continuous training for judges	0
Specialised training for judges	0	423L3-2	Institutional structures of courts	0	423L4-2	Regular review of court system capabilities to judge cybercrimes	1
		423L3-3	Statistics & analysis of cybercrime convictions	0			
Established formal international cooperation	1	431L3-1	Communication channels for international cooperation	1	431L4-1	Regular review of international cooperation	2
Mutual legal assistance & extradition	0	431L3-2	Strategically expanding international cooperation	0	431L4-2	Interoperability of formal & informal international cooperation	0
Legislative requirements on information exchange between public & private sectors	0	431L3-3	Resources for information exchange between public & private sectors	0	431L4-3	Regularly adjusted information exchange between public & private sectors	0
Established informal cooperation between government & justice	0	432L3-1	Established relationship among government, prosecutors, judges & law enforcement	1	432L4-1	Adapted cooperation & exchange of information	0
Established informal cooperation between ISPs & law enforcement	0	432L3-2	Cooperation between foreign ISPs & law enforcement	0	432L4-2	Adapted international cooperation	3
Informal international integration in law enforcement	0	432L3-3	Joint international investigation & prosecution	3	432L4-3	Interoperability of formal & informal international cooperation	0
Established standards & best practices	0	511L3-1	Risk-based adoption of standards & best practices	0	511L4-1	Regular review of adoption of standards & best practices	0
Standards & best practices widely used	1	511L3-2	Resource allocation based on standards	0	511L4-2	Decision making of non-compliance to standards & best practices	0
Metrics of adoption of standards & best practices	1	511L3-3	Contributing to international standards	4	511L4-3	Risk-based decision making of compliance	0
Promotion of use of standards & best practices	4						
Metrics of compliance of standards & best practices	2						
Standards & best practices used by CI supply chains	0						

#	Category	Subcategory	Capacity area	Level 1			
				ID	Keywords	Nb.	ID
512	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	512L1-1	Standards & best practices for procurement	0	512L2-1
				512L1-2	Promotion of use of standards & best practices for procurement	0	512L2-2
							512L2-3
513	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	513L1-1	Standards & best practices for development	0	513L2-1
				513L1-2	Promotion of use of standards & best practices for development	0	513L2-2
				513L1-3	Coding standards	0	
521	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	521L1-1	Limited internet infrastructures	0	521L2-1
				521L1-2	Discussion on resilience of internet infrastructures	0	521L2-2
							521L2-3
							521L2-4
531	Standards, Organisations, and Technologies	Software Quality	Software Quality	531L1-1	Quality & functional requirement of software	0	531L2-1
				531L1-2	Catalogue of secure softwares	0	531L2-2
				531L1-3	Software update policies under development	0	531L2-3
				531L1-4	Software deficiencies information	0	531L2-4
541	Standards, Organisations, and Technologies	Technical Security Controls	Technical Security Controls	541L1-1	Technical security controls deployed	0	541L2-1
				541L1-2	Latest technical security controls promoted	0	541L2-2
				541L1-3	Anti-malware services by ISPs	0	541L2-3
				541L1-4	ISPs' policies of technical security control	0	541L2-4
				541L1-5	IDS/IPS deployed	0	541L2-5
551	Standards, Organisations, and Technologies	Cryptographic Controls	Cryptographic Controls	551L1-1	Cryptographic controls deployed	0	551L2-1
				551L1-2	TLS deployed	0	551L2-2
							551L2-3
							551L2-4
561	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cybersecurity Technologies	561L1-1	Domestic security products market	0	561L2-1
				561L1-2	Cybersecurity consideration in development	0	561L2-2
562	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cyber Insurance	562L1-1	Needs for cybersecurity insurance understood	0	562L2-1
				562L1-2	Development of cybersecurity insurance	0	562L2-2
571	Standards, Organisations, and Technologies	Responsible Disclosure	Responsible Disclosure	571L1-1	Information sharing of vulnerabilities	0	571L2-1
				571L1-2	Ability to address vulnerability reports	0	571L2-2
							571L2-3

Level 2		Level 3			Level 4		
Keywords	**Nb.**	ID	Keywords	**Nb.**	ID	Keywords	**Nb.**
International standards & best practices for procurement implemented	0	512L3-1	Standards & best practices for procurement widely used & complied	2	512L4-1	Realtime monitoring of non-compliance to standards & best practices for procurement	0
Metrics of adoption of standards & best practices for procurement	0	512L3-2	Regular review of procurement	0	512L4-2	Risk-based decision making of non-compliance	0
Metrics of compliance of standards & best practices for procurement	1	512L3-3	Wider resource planning in procurement	0			
		512L3-4	Procurement skills benchmark	0			
		512L3-5	E-sourcing / e-tendering	0			
Metrics of adoption of standards & best practices for development	1	513L3-1	Security consideration in all stages	3	513L4-1	Risk-based decision making of non-compliance	0
Education & training for development	0	513L3-2	Core development activities	0	513L4-2	Adopting standards throughout life-time	0
		513L3-3	Risk-based adoption of standards	0	513L4-3	Explicit requirements by contract	0
Reliable internet infrastructures	0	521L3-1	Metrics of compliance to international standards of internet infrastructures	0	521L4-1	Controlled acquisition of infrastructures	0
Established e-commerce & electronic authentication	0	521L3-2	Investment to new technologies in internet infrastructures	4	521L4-2	Optimised cost for internet infrastructures	0
Internet infrastructures compliant to international standards & best practices	1				521L4-3	Controlled acquisition of critical technologies	0
Internet infrastructures formally managed	0				521L4-4	Independency & persistence of internet infrastructure technologies	0
Established quality & functional requirement of software	0	531L3-1	Monitoring software quality	0	531L4-1	High performance, reliability & usability softwares	0
Softwares complying with international standards	1	531L3-2	Review of software update policies & processes	0	531L4-2	Automated service continuity	0
Established software update processes	0	531L3-3	Business benefit from improving software quality	0	531L4-3	Regular review of quality requirement	0
Software classification	1	531L3-4	Software deficiency handling	1			
Latest technical controls & patch managements widely implemented	4	541L3-1	User side security controls	1	541L4-1	Continuous assess of technical security controls	12
Anti-malware softwares & network firewalls	0	541L3-2	Regular review of technical security controls	2	541L4-2	Business impact by technical security controls understood	0
Physical security controls	0				541L4-3	Supplemental security services by ISPs	1
Established ISPs' policies of technical security control	0						
Technical security controls based on international frameworks	1						
Cryptographic controls widely used	0	551L3-1	Risk-based use of cryptographic controls	0	551L4-1	Regular review of relevance of cryptographic controls	2
Secure communication services	0	551L3-2	Regular review of cryptographic control policies	0	551L4-2	Revision of cryptographic control policies	2
Cryptographic controls complied to international standards	0						
TLS widespread	0						
Domestic providers of security products	0	561L3-1	Security products complied to International standards	5	561L4-1	Automated security functions	0
Lowering dependency on foreign cybersecurity technologies	0	561L3-2	Risk-based product development	0	561L4-2	Exporting superior security products	9
Established cybersecurity insurance market	0	562L3-1	Covering various costs	0	562L4-1	Innovative cybersecurity insurance market	1
Covering additional costs (ex. Forensic investigation etc.)	0	562L3-2	Choice of coverages	0	562L4-2	Emerging risks & various cyber harm	0
		562L3-3	Cybersecurity insurance products for SMEs	0	562L4-3	Premium discount for secure behaviour	1
Established vulnerability disclosure framework	0	571L3-1	Established responsible disclosure processes	0	571L4-1	Regular review of vulnerability disclosure policies	0
Established processes against vulnerability information	0	571L3-2	Analysis & dissemination processes	0	571L4-2	Internationally contributing to responsible disclosure	0
Non legal action	0	571L3-3	Deadlines of update	0	571L4-3	Deadlines of update complied	0
					571L4-4	Reviewing process of deadlines	0

Appendix I Provisional Assessment of Japanese Cybersecurity Capacity

#	Dimension	Factor	Aspect	Formative		
				y/n	Keywords	y/n
111	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Strategy Development	y	Outline of strategy	y
				y	Development process of strategy	y
				y	Stakeholders involved in strategy	y
112	Cybersecurity Policy and Strategy	National Cybersecurity Strategy	Organisation	y	Cybersecurity programme under	y
						y
						y
						y
113	Cybersecurity Policy and Strategy	National Cybersecurity	Content	y	Risk priorities of cybersecurity defined in	y
						y
121	Cybersecurity Policy and Strategy	Incident Response	Identification of Incidents	y	Recording incidents	y
122	Cybersecurity Policy and Strategy	Incident Response	Organisation	y	Key incident response organisations in	y
				y	Ad-hoc responses	y
123	Cybersecurity Policy and Strategy	Incident Response	Coordination	y	Leading incident response organisation	y
						y
						n
124	Cybersecurity Policy and Strategy	Incident Response	Mode of Operation	y	Key incident response processes	y
				y	CSIRT member training	y
						y
131	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Identification	y	List of CI assets	y
						y
132	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Organisation	y	Informal information sharing between CI &	y
						y
						y
						y
133	Cybersecurity Policy and Strategy	Critical Infrastructure (CI) Protection	Risk Management and Response	y	Access control implemented in CI	p
				y	Basic capacity against cyber threat in CI	p
				y	Data security policy in CI	p
141	Cybersecurity Policy and Strategy	Crisis Management	Crisis Management	y	Assessment of exercise of national incident	y
				y	Exercise planning organisation designated for	y
				y	Stakeholders' participation in national	y
						y
						y
						y
151	Cybersecurity Policy and Strategy	Cyber Defence	Strategy	n	National-level threats identified	n
152	Cybersecurity Policy	Cyber Defence	Organisation	y	Dispersed cyber operations	y
153	Cybersecurity Policy and Strategy	Cyber Defence	Coordination	n	Cyber defence capability requirements	n
						p
161	Cybersecurity Policy and Strategy	Communi-cations Redundancy	Communi-cations Redundancy	y	Gaps in emergency communication identified	n
				y	Emergency procedures established	n
						n
211	Cyber Culture and Society	Cybersecurity Mind-set	Government	y	Leading agencies only have mind-set	y
212	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	y	Leading firms only have mind-set	y
				y	Materials for best practices available	
213	Cyber Culture and	Cybersecurity Mind-	Users	y	Limited users only have mind-set	y
221	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust and Confidence on the Internet	y	A few users can use internet securely	y
				y	Promotion of online trust exists	y
						y
222	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-government Services	y	Government's recognition of needs for	y
				y	Stakeholders' recognition of needs for	y
				y	A few users can use e-gov securely	y
				y	Security measures in e-gov	y
						n
223	Cyber Culture and Society	Trust and Confidence on the Internet	User Trust in E-commerce Services	y	Limited e-commerce provided	y
				y	Private sectors' recognition of need for	y
				y	A few users can use e-commerce securely	y
				y	Security measures in e-commerce	y
						p

Established		Strategic		Dynamic
Keywords	y/n	Keywords	y/n	Keywords
Strategy established	y	Reviewing process of strategy	y	Continual revision of strategy
Stakeholders' consultation in strategy	y	Cyber exercises considered in strategy	n	Contributing to international debate of
Implementation of strategy	y	Measurement of cybersecurity defined in		
	y	Capacity building & investment considered		
Cybersecurity programme agreed	y	PDCA processes of cybersecurity	n	Reassignment & reallocation of resources for
Coordinating body of cybersecurity	y	Consolidated budget for cybersecurity	n	Dissemination & feedbacks about
Goals & measurement of cybersecurity				
Discrete budget for cybersecurity				
National objectives of cybersecurity defined	y	Measurement of cybersecurity defined in	y	Continual revision of strategy
Minimum coverage of strategy contents	y	Protection of critical infrastructures defined	n	Contributing to international cooperation
Central registry of incidents	n	Regular revision of incident registry	n	Adapted analysis of incidents
	p	Incident analysis		
National CSIRT	y	Formal roles & responsibilities allocated	n	Sustainability of incident response capability
Roles & responsibilities of national CSIRT	n	Adequate resources for incident response	n	Early warning capability
			n	Capability to manage threat landscape
Coordination established	y	Subnational / sectorial incident response	n	Coordinating all levels / sectors
Communication lines for crisis	n	International coordination	n	Regional coordination
International cooperation in incident response	p	Information sharing across sectors		
Incident response processes & tools	y	Training & accreditation for CSIRT members	n	Scenario testing of incident response
Regular training for CSIRT members	p	Sophisticated incident analysis	n	Evaluating effectiveness of CSIRT members
Limited response to national level incidents	y	Regular review of incident response	n	Tools against zero-day vulnerabilities
	p	Forensics	n	Regional coordination
	n	International coordination		
Audit of CI assets	p	Priority of CI risks	n	Regular review of CI risk priorities
CI assets audit list	n	Vulnerability & asset management of CI		
Information sharing established between CI	n	Centralised management of CI protection	n	Ability to adjust of CI protection
Formal & consistent information sharing	p	Public awareness campaign of CI protection	p	Trust between CI & government
Point of contact	n	Supply chain management of CI		
Government engagement in CI protection				
Standards & best practices in CI	p	Cybersecurity oriented risk management in	p	Regular audit of CI
Risk management processes in CI	p	Regular review of impact analysis of CI	p	Indirect costs inclusive in impact analysis of
National CI incident response plan	p	Regular review of CI incident response plans		
	n	Regular review of resource allocation for CI		
	p	Insider threat detection in CI		
National incident exercise done	n	High-level scenario of national incident	n	Peer observance of national incident exercise
Appropriate resources for national incident	p	Trust between participants of national	n	National incident exercise contributing to
Roles in national incident exercise defined	n	SMART objectives & KPI of national	n	Internationally shared result of national
Incentives to participate in national incident	p	Evaluation of national incident exercise	n	National crisis management established
Trained monitors of national incident	p	National crisis management aligned with		
Evaluation of national incident exercise	y	Tailored reports of national incident exercise		
Cyber defence strategy exists	n	Dedicated resources for cyber defence	n	Rules of engagement in cyberspace
	n	Capturing landscape of national-level threat	n	Military doctrine in cyberspace
	n	Cyber defence strategy meets objectives		
Defined responsibility of cyber defence	n	Advanced capabilities & situational	n	Cross-border response ability
Coordination between CI & defence	p	Analytical capability in cyber defence	n	Leading international debate about cyber
Intelligence sharing between CI & defence	p	Strengths & weaknesses of cyber defence	n	Intelligence shared with allies
Emergency response assets hardwired	n	Redundant communications for key	n	Optimised for extended outages
Communication between emergency	n	Interoperability & functionality under	n	Assisting neighbours
Testing, training, drills of emergency	p	Evaluation of national incident exercise		
	n	Contribution to international communications'		
Most officials have mind-set	y	Mind-set spread in public sector	n	Mind-set commonplace in public sector
	p	Mind-set based strategy in public sector		N/A (same as above)
Most private sector actors have mind-set	y	Mind-set spread in private sector	n	Mind-set commonplace in private sector
	p	Mind-set based strategy in private sector		N/A (same as above)
Growing number of users have mind-set	n	Most users have mind-set	n	Users' mind-set reducing threat
Growing number of users can use internet	y	Most users can use internet securely	p	Users can evaluate risk & adjust behaviour
Promotion of online trust established	p	Users' ability to control providing personal	n	Promotion of online trust revised
User assistance available	n	Promotion of online trust evaluated		
E-gov established	p	Disclosures of activities of government	n	Promotion of e-gov revised
Risk reduction in e-gov	p	Privacy-by-default in e-gov	p	Data protection measures of e-gov
Promotion of e-gov	y	Most users can use e-gov securely		
Growing number of users can use e-gov	y	User feedbacks for e-gov		
Incident disclosure in e-gov				
E-commerce established	y	Resource allocation for e-commerce	y	Continuous improvement of e-commerce
Secure payment	y	Most users can use e-commerce securely	n	Clear terms & conditions of e-commerce
Growing number of users can use e-	y	Investment for e-commerce	y	User feedbacks for e-commerce
Promotion of trust of e-commerce				
Terms & conditions of e-commerce				

Appendix I

#	Dimension	Factor	Aspect	Formative		
				y/n	Keywords	y/n
231	Cyber Culture and Society	User Understanding of Personal Information Protection Online	User Understanding of Personal Information Protection Online	y	Users have only general knowledge about	y
				y	Discussions on protecting personal	p
241	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	y	Reporting channels of incidents	p
						y
251	Cyber Culture and Society	Media and Social Media	Media and Social Media	y	Media coverage of cybersecurity	y
				y	Discussion on social media security	y
						y
311	Cybersecurity Education, Training and Skills	Awareness Raising	Awareness Raising Programmes	y	Awareness raising programmes	n
				n	Awareness raising programmes affected by	n
						n
312	Cybersecurity Education, Training and Skills	Awareness Raising	Executive Awareness Raising	y	Executives' awareness about general	y
				y	Executives of particular sectors have	y
						y
321	Cybersecurity Education, Training and Skills	Framework for Education	Provision	y	Qualification programme for cybersecurity	y
				y	Professional cybersecurity educators	y
				y	Educational courses for cybersecurity	y
				y	Demand exists for cybersecurity education	y
						y
322	Cybersecurity Education, Training and Skills	Framework for Education	Administration	y	Cybersecurity education needs recognised	y
				y	Ad-hoc supply of resources for cybersecurity	y
						y
331	Cybersecurity Education, Training and Skills	Framework for Professional Training	Provision	y	Cybersecurity training needs recognised	y
				y	Cybersecurity training for general IT staff	y
				y	ICT certification with some cybersecurity	y
				y	Training courses for cybersecurity	y
332	Cybersecurity Education, Training and Skills	Framework for Professional Training	Uptake	p	Metrics of uptake of cybersecurity trainings	y
						p
						n
411	Legal and Regulatory Frameworks	Legal Framework	Legislative Framework for ICT Security	y	Discussion of establishing cybersecurity legal	y
				y	Priorities identified in cybersecurity legal	y
412	Legal and Regulatory Frameworks	Legal Framework	Privacy, Freedom of Speech & Other Human Rights Online	y	Partial privacy protection legislation	y
				y	Freedom of expression	y
				y	Discussion of establishing digital human	y
						y
						y
413	Legal and Regulatory Frameworks	Legal Framework	Data Protection Legislation	y	Partial data protection legislation	y
				y	Stakeholders' participation in data protection	y
414	Legal and Regulatory Frameworks	Legal Framework	Child Protection Online	y	Partial online child protection legislation	y
				y	Stakeholders' participation in online child	n
415	Legal and Regulatory Frameworks	Legal Framework	Consumer Protection Legislation	y	Partial consumer protection legislation	y
				y	Stakeholders' participation in consumer	y
416	Legal and Regulatory Frameworks	Legal Framework	Intellectual Property Legislation	y	Partial intellectual property legislation	y
				y	Stakeholders' participation in intellectual	
417	Legal and Regulatory Frameworks	Legal Framework	Substantive Cybercrime	y	Partial substantive cybercrime legislation	y
						y
418	Legal and Regulatory Frameworks	Legal Framework	Procedural Cybercrime Legislation	y	Partial procedural cybercrime legislation	y
						y
421	Legal and Regulatory Frameworks	Criminal Justice System	Law Enforcement	y	Limited digital forensics capabilities in law	y
				y	Training for law enforcement officers	y
						n
422	Legal and Regulatory Frameworks	Criminal Justice System	Prosecution	y	Limited capabilities to prosecute cybercrimes	n
				y	Training for prosecutors	
423	Legal and Regulatory Frameworks	Criminal Justice System	Courts	y	Limited capabilities to judge cybercrimes	n
				y	Training for judges	n
431	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to	Formal Cooperation	y	Formal international cooperation against	n
				p	Exchange of information between public &	y
						n
432	Legal and Regulatory Frameworks	Formal and Informal Cooperation Frameworks to	Informal Cooperation	n	Exchange of information between	n
				y	Cooperation between ISPs & law	y
				y	Informal international cooperation in law	n

Established		Strategic		Dynamic
Keywords	y/n	Keywords	y/n	Keywords
Growing number of users can secure	p	Measures to protect personal information	p	Users can adapt to changing environments
Discussions on balance between security &	y	Privacy rights	n	Wide recognition about personal information
	n	Security & privacy balanced	n	Security & privacy balanced in changing
	p	Privacy-by-default	p	Regular assessment of privacy protection
Incident reporting mechanisms established	n	Coordination of incident reporting channels	n	Regular enhancement of incident reporting
Promotion of incident reporting channels	n	Promotion of incident reporting channels	n	Coordination of response to reported
	n	Metrics of incident reporting		
Cybersecurity as common subject in media	p	Media coverage of information about	n	Discussion changing policy & society
Wide range of issues of cybersecurity in	p	Frequent discussion on social media security		
Broad discussion on social media security				
National programme of awareness raising	n	Sector specific programmes of awareness	n	Awareness raising programmes adapted
Consultation with stakeholders in national	n	Metrics for effectiveness of awareness	n	Revision of national awareness raising
Cybersecurity information portal	n	Evolution of awareness raising programmes	n	Entire society involved in awareness raising
	n	Contribution to international awareness	n	Overall threat reduced by awareness raising
Executives' basic understandings of	p	Executives' understandings of cybersecurity	p	Cybersecurity as common agenda in board
Limited executives' understandings of	p	Executives' ability to reallocate resources	n	Executives' attitude as international role
Raising programmes for awareness of crisis	p	Executives' understanding of crisis		
	n	Mandatory cybersecurity education for		
Qualification for cybersecurity educators	y	Business experts' participation in	n	Internationally forerunning in cybersecurity
University level courses for cybersecurity	n	Mandatory cybersecutity courses for	n	Balance between core components &
Degrees in cybersecurity	y	Cybersecurity specific degree	p	Cybersecurity education adapting to
Seminars for non-specialist	n	Cybersecurity as focusing area		
Research & development in cybersecurity	n	Cybersecurity education from primary to		
Broad discussion for enhancing cybersecurity	n	Cybersecurity education demand/supply	n	International CoE in cybersecurity
Budget for research & education for	y	Adapted budget for cybersecurity education	n	Cooperation between all stakeholders in
Attractiveness of cybersecurity career	p	International cooperation in cybersecurity	p	Cybersecurity education aligned with
	y	CoE in cybersecurity		
Structured cybersecurity training	y	Cybersecurity training aligned with	p	Collaboration between public & private in
Security professional certification	n	Cybersecurity training aligned with national	p	Coordination between cybersecurity training
Cybersecurity training requirements listed	p	Communication skills in cybersecurity	p	Incentives for cybersecurity trained
Cybersecurity training programmes for non-	p	Metrics of effectiveness of cybersecurity		
Cybersecurity trained & certified employees	p	Review of cybersecurity training programmes	p	Cybersecurity trained professionals
Knowledge transfer in cybersecurity	n	Coordination of cybersecurity training across		
Job creation in cybersecurity				
Cybersecurity legal framework established	y	Regular review of cybersecurity legal	n	Balance between cybersecurity legal
Coverages of cybersecurity legal framework			p	Participation to international cooperation
			n	Exceeding minimum requirement of
Online privacy protected	y	Cybersecurity legal framework aligned with	y	Amendment procedures for cybersecurity
Freedom of expression protected	y	Exceeding minimum requirement of	y	Internet access as human right
Privacy protected during investigation			y	Contributing to international digital human
Stakeholders' participation to discuss digital			n	Contributing to international privacy
Participation to international agreements				
Data protection legislation established	n	Timeframe of storing personal data during	y	Amendment procedures for data protection
Personal data protected	n	Data protection legislation aligned with		
Online child protection legislation established	n	Online child protection legislation aligned	y	Amendment procedures for online child
Legal minors protected				
Consumer protection legislation established	y	Consumer protection legislation aligned with	y	Amendment procedures for consumer
Responsible agency designated for consumer				
Intellectual property legislation established	y	Intellectual property legislation aligned with	n	Balance between intellectual property &
	y	Stakeholders' participation in amendment of		
Substantive cybercrime legislation exists	n	Exceeding minimum requirement in	p	Contributing to international cybercrime
Participation to international agreements on	y	Amendment procedures for substantive	n	Regular review of substantive cybercrime
Procedural cybercrime legislation exists	n	Procedural cybercrime legislation enables	p	Contributing to international cybercrime
Participation to international agreements on	n	Exceeding minimum requirement in	n	Regular review of procedural cybercrime
	y	Amendment procedures for procedural		
Comprehensive investigative capabilities for	y	Dedicated investigative resources for	n	Specialised and continuous training for law
Established chain of custody of digital	n	Advanced investigative capabilities for	n	Sophisticated digital forensic tools
Standards for training for law enforcement	n	Regular training for law enforcement officers	n	Regular review of investigative capabilities
	n	Cross-border investigation of cybercrimes		
	n	Statistics & analysis of cybercrime		
Comprehensive prosecutorial capabilities for	y	Institutional structures in prosecution	n	Prosecution of cross-border cybercrimes
	n	Statistics & analysis of cybercrime	n	Dedicated prosecutorial resources for
	n	Exchange of best practices between	n	Specialised and continuous training for
Sufficient jurisdictional capabilities for	n	Centralised judges for cybercrimes	n	Specialised and continuous training for
Specialised training for judges	y	Institutional structures of courts	n	Regular review of court system capabilities
	n	Statistics & analysis of cybercrime		
Established formal international cooperation	y	Communication channels for international	n	Regular review of international cooperation
Mutual legal assistance & extradition	n	Strategically expanding international	n	Interoperability of formal & informal
Legislative requirements on information	n	Resources for information exchange between	n	Regularly adjusted information exchange
Established informal cooperation between	n	Established relationship among government,	n	Adapted cooperation & exchange of
Established informal cooperation between	n	Cooperation between foreign ISPs & law	n	Adapted international cooperation
Informal international integration in law	n	Joint international investigation &	n	Interoperability of formal & informal

Appendix I

#	Dimension	Factor	Aspect	Formative		
				y/n	Keywords	y/n
511	Standards, Organisations, and Technologies	Adherence to Standards	ICT Security Standards	y	Standards for information risk management	y
				y	Standards for information risk management	y
				y	International standards & best practices	n
						y
						n
						p
512	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Procurement	y	Standards & best practices for procurement	y
				y	Promotion of use of standards & best	n
						n
513	Standards, Organisations, and Technologies	Adherence to Standards	Standards in Software Development	y	Standards & best practices for development	n
				y	Promotion of use of standards & best	y
				y	Coding standards	
521	Standards, Organisations, and Technologies	Internet Infrastructure Resilience	Internet Infrastructure Resilience	y	Limited internet infrastructures	y
				y	Discussion on resilience of internet	y
						y
						y
531	Standards, Organisations, and Technologies	Software Quality	Software Quality	y	Quality & functional requirement of software	y
				y	Catalogue of secure softwares	y
				y	Software update policies under development	y
				y	Software deficiencies information	n
541	Standards, Organisations, and Technologies	Technical Security Controls	Technical Security Controls	y	Technical security controls deployed	y
				y	Latest technical security controls promoted	y
				y	Anti-malware services by ISPs	y
				y	ISPs' policies of technical security control	y
				y	IDS/IPS deployed	y
551	Standards, Organisations, and Technologies	Cryptographic Controls	Cryptographic Controls	y	Cryptographic controls deployed	y
				y	TLS deployed	y
						y
						y
561	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	y	Domestic security products market	y
				y	Cybersecurity consideration in development	n
562	Standards, Organisations, and Technologies	Cybersecurity Marketplace	Cyber Insurance	y	Needs for cybersecurity insurance	p
				y	Development of cybersecurity insurance	p
571	Standards, Organisations, and Technologies	Responsible Disclosure	Responsible Disclosure	y	Information sharing of vulnerabilities	y
				y	Ability to address vulnerability reports	p
						y

y: achieved, p:partly achieved, n: not achieved, y%: ratio of "y"

Dimension	Total					Formative					
	y	p	n	Total	y%	y	p	n	Total	y%	y
1	67	23	52	142	47.2%	22	0	2	24	91.7%	30
2	49	16	18	83	59.0%	19	0	0	19	100.0%	19
3	34	16	25	75	45.3%	13	1	1	15	86.7%	16
4	63	4	49	116	54.3%	24	1	1	26	92.3%	21
5	61	29	31	121	50.4%	27	0	0	27	100.0%	24
Total	274	88	175	537	51.0%	105	2	4	111	94.6%	110

Established		Strategic		Dynamic
Keywords	y/n	Keywords	y/n	Keywords
Established standards & best practices	p	Risk-based adoption of standards & best	n	Regular review of adoption of standards &
Standards & best practices widely used	p	Resource allocation based on standards	p	Decision making of non-compliance to
Metrics of adoption of standards & best	y	Contributing to international standards	p	Risk-based decision making of compliance
Promotion of use of standards & best				
Metrics of compliance of standards & best				
Standards & best practices used by CI supply				
International standards & best practices for	p	Standards & best practices for procurement	n	Monitoring of use of standards & best
Metrics of adoption of standards & best	p	Regular review of procurement	n	Realtime monitoring of non-compliance to
Metrics of compliance of standards & best	p	Wider resource planning in procurement	p	Risk-based decision making of non-
	n	Procurement skills benchmark		
	y	E-sourcing / e-tendering		
Metrics of adoption of standards & best	p	Security consideration in all stages	p	Risk-based decision making of non-
Education & training for development	p	Core development activities	p	Adopting standards throughout life-time
	p	Risk-based adoption of standards	p	Explicit requirements by contract
Reliable internet infrastructures	y	Metrics of compliance to international	n	Controlled acquisition of infrastructures
Established e-commerce & electronic	y	Investment to new technologies in internet	p	Optimised cost for internet infrastructures
Internet infrastructures compliant to			n	Controlled acquisition of critical technologies
Internet infrastructures formally managed			n	Independency & persistence of internet
Established quality & functional requirement	n	Monitoring software quality	n	High performance, reliability & usability
Softwares complying with international	n	Review of software update policies &	n	Automated service continuity
Established software update processes	p	Business benefit from improving software	n	Regular review of quality requirement
Software classification	p	Software deficiency handling		
Latest technical controls & patch	y	User side security controls	p	Continuous assess of technical security
Anti-malware softwares & network firewalls	p	Regular review of technical security controls	p	Business impact by technical security
Physical security controls			p	Supplemental security services by ISPs
Established ISPs' policies of technical				
Technical security controls based on				
Cryptographic controls widely used	p	Risk-based use of cryptographic controls	y	Regular review of relevance of cryptographic
Secure communication services	y	Regular review of cryptographic control	y	Revision of cryptographic control policies
Cryptographic controls complied to				
TLS widespread				
Domestic providers of security products	y	Security products complied to International	n	Automated security functions
Lowering dependency on foreign	y	Risk-based product development	n	Exporting superior security products
Established cybersecurity insurance market	p	Covering various costs	n	Innovative cybersecurity insurance market
Covering additional costs (ex. Forensic	p	Choice of coverages	n	Emerging risks & various cyber harm
	n	Cybersecurity insurance products for SMEs	n	Premium discount for secure behaviour
Established vulnerability disclosure	n	Established responsible disclosure processes	n	Regular review of vulnerability disclosure
Established processes against vulnerability	p	Analysis & dissemination processes	n	Internationally contributing to responsible
Non legal action	n	Deadlines of update	n	Deadlines of update complied
			n	Reviewing process of deadlines

Established				Strategic					Dynamic				
p	n	Total	y%	y	p	n	Total	y%	y	p	n	Total	y%
4	6	40	75.0%	13	16	17	46	28.3%	2	3	27	32	6.3%
3	1	23	82.6%	9	9	6	24	37.5%	2	4	11	17	11.8%
1	4	21	76.2%	5	7	11	23	21.7%	0	7	9	16	0.0%
0	9	30	70.0%	12	0	19	31	38.7%	6	3	20	29	20.7%
4	7	35	68.6%	8	15	6	29	27.6%	2	10	18	30	6.7%
12	27	149	73.8%	47	47	59	153	30.7%	12	27	85	124	9.7%

Appendix J ANC3DB

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0001	Japan	7-111a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.
0002	Japan	7-111a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.
0003	Japan	7-111a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new business harnessing IoT systems.
0004	Japan	7-112a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.
0005	Japan	7-112a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.
0006	Japan	7-112a	Cybersecurity2017	2017	Promoting 'Security-by-Design' in new & large scale business harnessing IoT systems.
0007	Japan	7-112a2	Cybersecurity2017	2017	Promoting secure IoT systems based on "General Framework for Secure IoT Systems".
0008	Japan	7-112b	Cybersecurity2017	2017	Considering measures to exterminate 'bot-net'.
0009	Japan	7-112b	Cybersecurity2017	2017	Considering measures to exterminate 'bot-net'.
0010	Japan	7-112b	Cybersecurity2017	2017	Considering measures to exterminate 'bot-net'.
0011	Japan	7-113a	Cybersecurity2017	2017	Promoting "IoT Security Guidelines".
0012	Japan	7-113a2	Cybersecurity2017	2017	Promoting "IoT Security Guidelines" as international standard.
0013	Japan	7-113b	Cybersecurity2017	2017	Promoting "EDSA certification" (security certification for control systems).
0014	Japan	7-113b	Cybersecurity2017	2017	Promoting "EDSA certification" (security certification for control systems).
0015	Japan	7-113c	Cybersecurity2017	2017	Analysing open source information & warning organisations of vulnerable systems.
0016	Japan	7-113c	Cybersecurity2017	2017	Analysing open source information & warning organisations of vulnerable systems.
0017	Japan	7-113c	Cybersecurity2017	2017	Analysing open source information & warning organisations of vulnerable systems.
0018	Japan	7-113d	Cybersecurity2017	2017	Continuing operation of reporting & dissemination system for vulnerability information.
0019	Japan	7-113d	Cybersecurity2017	2017	Continuing operation of reporting & dissemination system for vulnerability information.
0020	Japan	7-114a	Cybersecurity2017	2017	Researching innovative & advanced technologies.
0021	Japan	7-114a	Cybersecurity2017	2017	Researching innovative & advanced technologies.
0022	Japan	7-114b	Cybersecurity2017	2017	Researching technologies for security countermeasures for IoTs.
0023	Japan	7-114c	Cybersecurity2017	2017	Developing technologies of threat analysis & risk evaluation for control systems.
0024	Japan	7-114c	Cybersecurity2017	2017	Developing technologies of threat analysis & risk evaluation for control systems.
0025	Japan	7-114d	Cybersecurity2017	2017	Researching & developing technologies for automotive security in "SIP: Cross-ministerial
0026	Japan	7-114d	Cybersecurity2017	2017	Researching & developing technologies for automotive security in "SIP: Cross-ministerial
0027	Japan	7-114d	Cybersecurity2017	2017	Researching & developing technologies for automotive security in "SIP: Cross-ministerial
0028	Japan	7-114e	Cybersecurity2017	2017	Promoting countermeasures against vulnerable IoT products in the market based on "Policy
0029	Japan	7-114e	Cybersecurity2017	2017	Promoting countermeasures against vulnerable IoT products in the market based on "Policy
0030	Japan	7-114e	Cybersecurity2017	2017	Promoting countermeasures against vulnerable IoT products in the market based on "Policy
0031	Japan	7-121a	Cybersecurity2017	2017	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of
0032	Japan	7-121a	Cybersecurity2017	2017	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of
0033	Japan	7-121a	Cybersecurity2017	2017	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of
0034	Japan	7-121a	Cybersecurity2017	2017	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of
0035	Japan	7-121a	Cybersecurity2017	2017	Surveying & promoting cybersecurity measures of enterprises based on "Guidelines of
0036	Japan	7-121b	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines".
0037	Japan	7-121b	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines".
0038	Japan	7-121b	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines".
0039	Japan	7-121c	Cybersecurity2017	2017	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring
0040	Japan	7-121c	Cybersecurity2017	2017	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring
0041	Japan	7-121c	Cybersecurity2017	2017	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring
0042	Japan	7-121c	Cybersecurity2017	2017	Promoting cybersecurity insurance & "Cybersecurity Management Guidelines" by requiring
0043	Japan	7-122a	Cybersecurity2017	2017	Promoting human resources development for each category - board members, bridge
0044	Japan	7-122a	Cybersecurity2017	2017	Promoting human resources development for each category - board members, bridge
0045	Japan	7-122a	Cybersecurity2017	2017	Promoting human resources development for each category - board members, bridge
0046	Japan	7-122a	Cybersecurity2017	2017	Promoting human resources development for each category - board members, bridge
0047	Japan	7-122a	Cybersecurity2017	2017	Promoting human resources development for each category - board members, bridge
0048	Japan	7-123a	Cybersecurity2017	2017	Promoting 'Security-by-Design'.
0049	Japan	7-123a	Cybersecurity2017	2017	Promoting 'Security-by-Design'.
0050	Japan	7-123a	Cybersecurity2017	2017	Promoting 'Security-by-Design'.
0051	Japan	7-123b2	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines" to SMEs (small-to medium-sized
0052	Japan	7-123b2	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines" to SMEs (small-to medium-sized
0053	Japan	7-123b2	Cybersecurity2017	2017	Promoting "Cybersecurity Management Guidelines" to SMEs (small-to medium-sized
0054	Japan	7-123c	Cybersecurity2017	2017	Reviewing rules & regulations so as to improve security of whole supply chains of IT
0055	Japan	7-123c	Cybersecurity2017	2017	Reviewing rules & regulations so as to improve security of whole supply chains of IT
0056	Japan	7-123d	Cybersecurity2017	2017	Encouraging corporates to establish CSIRT.
0057	Japan	7-123d	Cybersecurity2017	2017	Encouraging corporates to establish CSIRT.
0058	Japan	7-123e	Cybersecurity2017	2017	Performing practical cyber defence exercise "CYDER" at "National Cyber Training Center".
0059	Japan	7-123e	Cybersecurity2017	2017	Performing practical cyber defence exercise "CYDER" at "National Cyber Training Center".
0060	Japan	7-123e2	Cybersecurity2017	2017	Performing cyber exercises assuming attacks against Tokyo Olympics/Paralympics in 2020,
0061	Japan	7-123e2	Cybersecurity2017	2017	Performing cyber exercises assuming attacks against Tokyo Olympics/Paralympics in 2020,
0062	Japan	7-123f	Cybersecurity2017	2017	Performing practical APT exercises.
0063	Japan	7-123g	Cybersecurity2017	2017	Enhancing "J-CRAT: Cyber Rescue Team" (activity to assist organisational incident
0064	Japan	7-123h	Cybersecurity2017	2017	Performing financial industry-wide cyber exercises.
0065	Japan	7-123i	Cybersecurity2017	2017	Promoting "iLogScanner: Attack Indication Detecting Tool for Websites".
0066	Japan	7-123i	Cybersecurity2017	2017	Promoting "iLogScanner: Attack Indication Detecting Tool for Websites".
0067	Japan	7-123j	Cybersecurity2017	2017	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
0068	Japan	7-123j	Cybersecurity2017	2017	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
0069	Japan	7-123j	Cybersecurity2017	2017	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
0070	Japan	7-123j	Cybersecurity2017	2017	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
0071	Japan	7-123j	Cybersecurity2017	2017	Continuing & enhancing operation of "J-CSIP: Cyber Intelligence Sharing Initiative".
0072	Japan	7-123k	Cybersecurity2017	2017	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-
0073	Japan	7-123k	Cybersecurity2017	2017	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
521L2-1	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	2	Reliable internet infrastructures
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
122L4-2	Cybersecurity Policy and	Incident Response	Organisation	4	Early warning capability
131L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	3	Vulnerability & asset management of CI
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
571L3-1	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	3	Established responsible disclosure processes
571L3-2	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	3	Analysis & dissemination processes
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L2-2	Cybersecurity Education,	Framework for Education	Administration	2	Budget for research & education for
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
221L3-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Most users can use internet securely
311L3-2	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Metrics for effectiveness of awareness raising
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
562L2-1	Standards, Organisations, and	Cybersecurity Marketplace	Cyber Insurance	2	Established cybersecurity insurance market
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
312L3-3	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understanding of crisis
331L2-4	Cybersecurity Education,	Framework for Professional	Provision	2	Cybersecurity training programmes for non-
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
331L3-3	Cybersecurity Education,	Framework for Professional	Provision	3	Communication skills in cybersecurity training
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
212L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	4	Mind-set commonplace in private sector
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
513L4-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	4	Adopting standards throughout life-time
212L3-2	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set based strategy in private sector
312L3-3	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understanding of crisis
124L4-1	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Scenario testing of incident response
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
124L4-1	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Scenario testing of incident response
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
521L2-1	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	2	Reliable internet infrastructures
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L2-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Point of contact
132L2-4	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Government engagement in CI protection
153L2-2	Cybersecurity Policy and	Cyber Defence	Coordination	2	Intelligence sharing between CI & defence
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0074	Japan	7-123k	Cybersecurity2017	2017	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-
0075	Japan	7-123k	Cybersecurity2017	2017	Continuing & enhancing operation of "ICT-ISAC" (expanded & reorganised from Telecom-
0076	Japan	7-123l	Cybersecurity2017	2017	Enhancing "Financial ISAC Japan".
0077	Japan	7-123l	Cybersecurity2017	2017	Enhancing "Financial ISAC Japan".
0078	Japan	7-123l	Cybersecurity2017	2017	Enhancing "Financial ISAC Japan".
0079	Japan	7-123l	Cybersecurity2017	2017	Enhancing "Financial ISAC Japan".
0080	Japan	7-131a	Cybersecurity2017	2017	Cultivating cybersecurity-related business to a growth industry by establishing certification
0081	Japan	7-131a	Cybersecurity2017	2017	Cultivating cybersecurity-related business to a growth industry by establishing certification
0082	Japan	7-131b	Cybersecurity2017	2017	Promoting "Cloud Security Guidelines" & "Cloud Audit System".
0083	Japan	7-131b	Cybersecurity2017	2017	Promoting "Cloud Security Guidelines" & "Cloud Audit System".
0084	Japan	7-131c	Cybersecurity2017	2017	Promoting security investment of SMEs (small-to medium-sized enterprises).
0085	Japan	7-131c	Cybersecurity2017	2017	Promoting security investment of SMEs (small-to medium-sized enterprises).
0086	Japan	7-131c	Cybersecurity2017	2017	Promoting security investment of SMEs (small-to medium-sized enterprises).
0087	Japan	7-131c	Cybersecurity2017	2017	Promoting security investment of SMEs (small-to medium-sized enterprises).
0088	Japan	7-131c	Cybersecurity2017	2017	Promoting security investment of SMEs (small-to medium-sized enterprises).
0089	Japan	7-131d	Cybersecurity2017	2017	Reconsidering "Copyright Act" about reverse engineering for security purposes.
0090	Japan	7-131d	Cybersecurity2017	2017	Reconsidering "Copyright Act" about reverse engineering for security purposes.
0091	Japan	7-132a	Cybersecurity2017	2017	Continuing "Public & Private Sectors Forum for Trade Secret" to share information about
0092	Japan	7-132a	Cybersecurity2017	2017	Continuing "Public & Private Sectors Forum for Trade Secret" to share information about
0093	Japan	7-132b	Cybersecurity2017	2017	Promoting "Handbook for Confidential Information Protection" & "Guide for Handbook for
0094	Japan	7-132b	Cybersecurity2017	2017	Promoting "Handbook for Confidential Information Protection" & "Guide for Handbook for
0095	Japan	7-132c	Cybersecurity2017	2017	Promoting guidelines for deterrence/prevention of internal misconduct within organisations.
0096	Japan	7-132c	Cybersecurity2017	2017	Promoting guidelines for deterrence/prevention of internal misconduct within organisations.
0097	Japan	7-132d	Cybersecurity2017	2017	Communicating & negotiating with countries who apply 'Forced Localization Measures'.
0098	Japan	7-133a	Cybersecurity2017	2017	Supporting international standardization in security through participation to ISO/IEC
0099	Japan	7-133b	Cybersecurity2017	2017	Supporting international standardization in cryptography, certification for cryptograph &
0100	Japan	7-133b	Cybersecurity2017	2017	Supporting international standardization in cryptography, certification for cryptograph &
0101	Japan	7-133b	Cybersecurity2017	2017	Supporting international standardization in cryptography, certification for cryptograph &
0102	Japan	7-133b	Cybersecurity2017	2017	Supporting international standardization in cryptography, certification for cryptograph &
0103	Japan	7-133c	Cybersecurity2017	2017	Supporting international standardization in vulnerability management like SCAP, CVSS etc.
0104	Japan	7-133c	Cybersecurity2017	2017	Supporting international standardization in vulnerability management like SCAP, CVSS etc.
0105	Japan	7-133d	Cybersecurity2017	2017	Supporting international standardization in security evaluation like PP (Protection Profile)
0106	Japan	7-133e	Cybersecurity2017	2017	Assisting ITPEC (IT Professionals Examination Council: organisation for a common IT
0107	Japan	7-133e	Cybersecurity2017	2017	Assisting ITPEC (IT Professionals Examination Council: organisation for a common IT
0108	Japan	7-133e	Cybersecurity2017	2017	Assisting ITPEC (IT Professionals Examination Council: organisation for a common IT
0109	Japan	7-133f	Cybersecurity2017	2017	Assisting security management in ASEAN countries.
0110	Japan	7-133g	Cybersecurity2017	2017	Assisting establishment of 'secure development' in countries where Japanese corporates
0111	Japan	7-133g	Cybersecurity2017	2017	Assisting establishment of 'secure development' in countries where Japanese corporates
0112	Japan	7-133g	Cybersecurity2017	2017	Assisting establishment of 'secure development' in countries where Japanese corporates
0113	Japan	7-133g	Cybersecurity2017	2017	Assisting establishment of 'secure development' in countries where Japanese corporates
0114	Japan	7-133g	Cybersecurity2017	2017	Assisting establishment of 'secure development' in countries where Japanese corporates
0115	Japan	7-133h	Cybersecurity2017	2017	Researching international standards & evaluation system for IoT systems.
0116	Japan	7-133h	Cybersecurity2017	2017	Researching international standards & evaluation system for IoT systems.
0117	Japan	7-211b	Cybersecurity2017	2017	Promoting 'Security-by-Design' in IoT & embedded systems.
0118	Japan	7-211b	Cybersecurity2017	2017	Promoting 'Security-by-Design' in IoT & embedded systems.
0119	Japan	7-211b	Cybersecurity2017	2017	Promoting 'Security-by-Design' in IoT & embedded systems.
0120	Japan	7-211c	Cybersecurity2017	2017	Promoting "How to Secure Your Web Site".
0121	Japan	7-211c	Cybersecurity2017	2017	Promoting "How to Secure Your Web Site".
0122	Japan	7-211c	Cybersecurity2017	2017	Promoting "How to Secure Your Web Site".
0123	Japan	7-211c	Cybersecurity2017	2017	Promoting "How to Secure Your Web Site".
0124	Japan	7-211c	Cybersecurity2017	2017	Promoting "How to Secure Your Web Site".
0125	Japan	7-211c2	Cybersecurity2017	2017	Promoting "AppGoat" (training tool for secure development).
0126	Japan	7-211c2	Cybersecurity2017	2017	Promoting "AppGoat" (training tool for secure development).
0127	Japan	7-211c2	Cybersecurity2017	2017	Promoting "AppGoat" (training tool for secure development).
0128	Japan	7-211d	Cybersecurity2017	2017	Researching technologies for securer development & more sophisticated evaluation.
0129	Japan	7-211d	Cybersecurity2017	2017	Researching technologies for securer development & more sophisticated evaluation.
0130	Japan	7-211d	Cybersecurity2017	2017	Researching technologies for securer development & more sophisticated evaluation.
0131	Japan	7-211f	Cybersecurity2017	2017	Supporting vulnerability management in organisations, by promoting structured languages
0132	Japan	7-211g	Cybersecurity2017	2017	Promoting 'fuzz testing' for pro-active vulnerability detection.
0133	Japan	7-211h	Cybersecurity2017	2017	Upgrading "NICTER: Network Incident Analysis Center for Tactical Emergency Response".
0134	Japan	7-211i	Cybersecurity2017	2017	Continuing operation of "ACTIVE: Advanced Cyber Threat Response Initiative" (assistance
0135	Japan	7-211i	Cybersecurity2017	2017	Continuing operation of "ACTIVE: Advanced Cyber Threat Response Initiative" (assistance
0136	Japan	7-211j	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0137	Japan	7-211j	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0138	Japan	7-211j	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0139	Japan	7-211j	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0140	Japan	7-211k	Cybersecurity2017	2017	Continuing operation of "Council of Anti-Phishing Japan".
0141	Japan	7-211k	Cybersecurity2017	2017	Continuing operation of "Council of Anti-Phishing Japan".
0142	Japan	7-211l	Cybersecurity2017	2017	Promoting "icat: IPA Cyber Security Alert Service".
0143	Japan	7-211l	Cybersecurity2017	2017	Promoting "icat: IPA Cyber Security Alert Service".
0144	Japan	7-211m	Cybersecurity2017	2017	Urging public Wi-Fi service providers to prevent cybercrime & to enable effective tracking
0145	Japan	7-211m	Cybersecurity2017	2017	Urging public Wi-Fi service providers to prevent cybercrime & to enable effective tracking
0146	Japan	7-211m	Cybersecurity2017	2017	Urging public Wi-Fi service providers to prevent cybercrime & to enable effective tracking
0147	Japan	7-211n	Cybersecurity2017	2017	Initiating Wi-Fi service providers & users to safer communication.

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
132L2-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Point of contact
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L2-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Point of contact
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
561L2-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	2	Domestic providers of security products
561L2-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	2	Lowering dependency on foreign
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
541L2-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Anti-malware softwares & network firewalls
121L4-1	Cybersecurity Policy and	Incident Response	Identification of Incidents	4	Adapted analysis of incidents
124L3-2	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Sophisticated incident analysis
311L2-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	2	National programme of awareness raising
431L1-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	1	Exchange of information between public &
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
521L4-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Optimised cost for internet infrastructures
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
412L4-4	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	4	Contributing to international privacy
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
551L4-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Revision of cryptographic control policies
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
571L4-2	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	4	Internationally contributing to responsible
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
322L3-3	Cybersecurity Education,	Framework for Education	Administration	3	International cooperation in cybersecurity
332L4-1	Cybersecurity Education,	Framework for Professional	Uptake	4	Cybersecurity trained professionals
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
513L1-3	Standards, Organisations, and	Adherence to Standards	Standards in Software	1	Coding standards
513L2-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	2	Education & training for development
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
541L2-5	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Technical security controls based on
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
223L2-4	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-commerce	2	Promotion of trust of e-commerce
223L2-4	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-commerce	2	Promotion of trust of e-commerce
513L1-3	Standards, Organisations, and	Adherence to Standards	Standards in Software	1	Coding standards
513L2-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	2	Education & training for development
541L2-5	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Technical security controls based on
513L1-3	Standards, Organisations, and	Adherence to Standards	Standards in Software	1	Coding standards
513L2-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	2	Education & training for development
541L2-5	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Technical security controls based on
513L2-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	2	Education & training for development
541L2-5	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Technical security controls based on
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
571L2-1	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	2	Established vulnerability disclosure
122L4-2	Cybersecurity Policy and	Incident Response	Organisation	4	Early warning capability
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
221L2-3	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	User assistance available
122L4-2	Cybersecurity Policy and	Incident Response	Organisation	4	Early warning capability
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
432L2-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	2	Established informal cooperation between
541L2-4	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Established ISPs' policies of technical security
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0148	Japan	7-211n	Cybersecurity2017	2017	Initiating Wi-Fi service providers & users to safer communication.
0149	Japan	7-211n	Cybersecurity2017	2017	Initiating Wi-Fi service providers & users to safer communication.
0150	Japan	7-211n	Cybersecurity2017	2017	Initiating Wi-Fi service providers & users to safer communication.
0151	Japan	7-211o	Cybersecurity2017	2017	Considering development of intelligence sharing platform for government & private sectors.
0152	Japan	7-211o	Cybersecurity2017	2017	Considering development of intelligence sharing platform for government & private sectors.
0153	Japan	7-211o	Cybersecurity2017	2017	Considering development of intelligence sharing platform for government & private sectors.
0154	Japan	7-211o	Cybersecurity2017	2017	Considering development of intelligence sharing platform for government & private sectors.
0155	Japan	7-212a	Cybersecurity2017	2017	Initiating users to security in cyber space.
0156	Japan	7-212a	Cybersecurity2017	2017	Initiating users to security in cyber space.
0157	Japan	7-212b	Cybersecurity2017	2017	Initiating users to secure use of internet, protection from cybercrimes, latest criminal
0158	Japan	7-212b	Cybersecurity2017	2017	Initiating users to secure use of internet, protection from cybercrimes, latest criminal
0159	Japan	7-212b	Cybersecurity2017	2017	Initiating users to secure use of internet, protection from cybercrimes, latest criminal
0160	Japan	7-212b	Cybersecurity2017	2017	Initiating users to secure use of internet, protection from cybercrimes, latest criminal
0161	Japan	7-212b2	Cybersecurity2017	2017	Initiating educators & staff of local public entities to elimination of cyber environment that is
0162	Japan	7-212b2	Cybersecurity2017	2017	Initiating educators & staff of local public entities to elimination of cyber environment that is
0163	Japan	7-212b2	Cybersecurity2017	2017	Initiating educators & staff of local public entities to elimination of cyber environment that is
0164	Japan	7-212c	Cybersecurity2017	2017	Promoting use of electronic signature.
0165	Japan	7-212c	Cybersecurity2017	2017	Promoting use of electronic signature.
0166	Japan	7-212c	Cybersecurity2017	2017	Promoting use of electronic signature.
0167	Japan	7-212d	Cybersecurity2017	2017	Initiating youth to secure use of internet & smartphones.
0168	Japan	7-212d	Cybersecurity2017	2017	Initiating youth to secure use of internet & smartphones.
0169	Japan	7-212d	Cybersecurity2017	2017	Initiating youth to secure use of internet & smartphones.
0170	Japan	7-212d	Cybersecurity2017	2017	Initiating youth to secure use of internet & smartphones.
0171	Japan	7-212e	Cybersecurity2017	2017	Continuing moral education for information usage at school.
0172	Japan	7-212e	Cybersecurity2017	2017	Continuing moral education for information usage at school.
0173	Japan	7-212f	Cybersecurity2017	2017	Continuing promotion of moral education for internet usage.
0174	Japan	7-212f	Cybersecurity2017	2017	Continuing promotion of moral education for internet usage.
0175	Japan	7-212g	Cybersecurity2017	2017	Promoting "Information Leakage Prevention Tool" (tool to prevent data exfiltration through
0176	Japan	7-212h	Cybersecurity2017	2017	Arousing security awareness of youth.
0177	Japan	7-212i	Cybersecurity2017	2017	Assisting local public entities to raise public awareness of security.
0178	Japan	7-212i	Cybersecurity2017	2017	Assisting local public entities to raise public awareness of security.
0179	Japan	7-212j	Cybersecurity2017	2017	Continuing "Safety Class" to raise public awareness of secure internet usage.
0180	Japan	7-212j	Cybersecurity2017	2017	Continuing "Safety Class" to raise public awareness of secure internet usage.
0181	Japan	7-212j	Cybersecurity2017	2017	Continuing "Safety Class" to raise public awareness of secure internet usage.
0182	Japan	7-212j	Cybersecurity2017	2017	Continuing "Safety Class" to raise public awareness of secure internet usage.
0183	Japan	7-212k	Cybersecurity2017	2017	Assisting local public entities to raise public awareness of security.
0184	Japan	7-212k	Cybersecurity2017	2017	Assisting local public entities to raise public awareness of security.
0185	Japan	7-212l	Cybersecurity2017	2017	Supporting SMEs (small-to medium-sized enterprises) to enhance security by training
0186	Japan	7-212m	Cybersecurity2017	2017	Providing public & SMEs (small-to medium-sized enterprises) with intelligence of security
0187	Japan	7-212m	Cybersecurity2017	2017	Providing public & SMEs (small-to medium-sized enterprises) with intelligence of security
0188	Japan	7-212n	Cybersecurity2017	2017	Supporting incident response of public & SMEs (small-to medium-sized enterprises) through
0189	Japan	7-212n	Cybersecurity2017	2017	Supporting incident response of public & SMEs (small-to medium-sized enterprises) through
0190	Japan	7-212o	Cybersecurity2017	2017	Collecting, analysing & reporting cybersecurity information.
0191	Japan	7-212p	Cybersecurity2017	2017	Urging universities to enhance information security.
0192	Japan	7-212q	Cybersecurity2017	2017	Taking course of action to implement newly effected "Amended Act on the Protection of
0193	Japan	7-213a	Cybersecurity2017	2017	Strengthening capability of investigation of cybercrime.
0194	Japan	7-213a	Cybersecurity2017	2017	Strengthening capability of investigation of cybercrime.
0195	Japan	7-213b	Cybersecurity2017	2017	Enhancing cooperation between public, private & academic sectors, with "JC3: Japan
0196	Japan	7-213b	Cybersecurity2017	2017	Enhancing cooperation between public, private & academic sectors, with "JC3: Japan
0197	Japan	7-213c	Cybersecurity2017	2017	Strengthening capability of investigation of unauthorized access, phishing & illegal
0198	Japan	7-213c	Cybersecurity2017	2017	Strengthening capability of investigation of unauthorized access, phishing & illegal
0199	Japan	7-213c	Cybersecurity2017	2017	Strengthening capability of investigation of unauthorized access, phishing & illegal
0200	Japan	7-213c2	Cybersecurity2017	2017	Providing corporates with intelligence of latest criminal techniques, etc.
0201	Japan	7-213d	Cybersecurity2017	2017	Supporting establishment of anti-cybercrime voluntary corps.
0202	Japan	7-213d	Cybersecurity2017	2017	Supporting establishment of anti-cybercrime voluntary corps.
0203	Japan	7-213d	Cybersecurity2017	2017	Supporting establishment of anti-cybercrime voluntary corps.
0204	Japan	7-213e	Cybersecurity2017	2017	Strengthening capability of investigation of crimes targeting smartphone users.
0205	Japan	7-213e	Cybersecurity2017	2017	Strengthening capability of investigation of crimes targeting smartphone users.
0206	Japan	7-213f	Cybersecurity2017	2017	Training investigators specialized in cybercrime.
0207	Japan	7-213g	Cybersecurity2017	2017	Collecting & disseminating information about phishing through operation of "Council of
0208	Japan	7-213g	Cybersecurity2017	2017	Collecting & disseminating information about phishing through operation of "Council of
0209	Japan	7-213h	Cybersecurity2017	2017	Making the most of High-Tech Crime Technology Division to tackle complicated &
0210	Japan	7-213i	Cybersecurity2017	2017	Training prosecutors for cybercrimes.
0211	Japan	7-213j	Cybersecurity2017	2017	Taking a course of action against cybercrimes upon effectuation of "Cyber Criminal Law".
0212	Japan	7-213j	Cybersecurity2017	2017	Taking a course of action against cybercrimes upon effectuation of "Cyber Criminal Law".
0213	Japan	7-213k	Cybersecurity2017	2017	Promoting "Guidelines Regarding the Protection of Personal Information in the
0214	Japan	7-213k2	Cybersecurity2017	2017	Enhancing capabilities to analyse IoTs.
0215	Japan	7-213k2	Cybersecurity2017	2017	Enhancing capabilities to analyse IoTs.
0216	Japan	7-220b	Cybersecurity2017	2017	Considering & preparing for legislation of security countermeasures for CIIs.
0217	Japan	7-220b	Cybersecurity2017	2017	Considering & preparing for legislation of security countermeasures for CIIs.
0218	Japan	7-220b2	Cybersecurity2017	2017	Monitoring & publishing improvement of security standards annually.
0219	Japan	7-220b2	Cybersecurity2017	2017	Monitoring & publishing improvement of security standards annually.
0220	Japan	7-220b2	Cybersecurity2017	2017	Monitoring & publishing improvement of security standards annually.
0221	Japan	7-220c	Cybersecurity2017	2017	Improving security standards for CIIs including risk assessment, functionality assurance,

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
541L2-4	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Established ISPs' policies of technical security
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
153L2-2	Cybersecurity Policy and	Cyber Defence	Coordination	2	Intelligence sharing between CI & defence
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
221L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Users' ability to control providing personal
231L2-1	Cyber Culture and Society	User Understanding of	User Understanding of	2	Growing number of users can secure personal
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
221L3-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Most users can use internet securely
251L3-2	Cyber Culture and Society	Media and Social Media	Media and Social Media	3	Frequent discussion on social media security
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
551L2-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	2	Cryptographic controls widely used
551L2-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	2	Secure communication services
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
221L3-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Most users can use internet securely
221L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Users' ability to control providing personal
251L3-2	Cyber Culture and Society	Media and Social Media	Media and Social Media	3	Frequent discussion on social media security
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
221L3-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Most users can use internet securely
221L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Users' ability to control providing personal
251L3-2	Cyber Culture and Society	Media and Social Media	Media and Social Media	3	Frequent discussion on social media security
231L2-1	Cyber Culture and Society	User Understanding of	User Understanding of	2	Growing number of users can secure personal
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
221L3-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Most users can use internet securely
221L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	3	Users' ability to control providing personal
231L2-1	Cyber Culture and Society	User Understanding of	User Understanding of	2	Growing number of users can secure personal
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
241L2-2	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	2	Promotion of incident reporting channels
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
412L3-1	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	3	Cybersecurity legal framework aligned with
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L3-3	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Regular training for law enforcement officers
421L3-5	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Statistics & analysis of cybercrime
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
431L2-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Legislative requirements on information
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
213L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	2	Growing number of users have mind-set
221L2-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Growing number of users can use internet
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
431L1-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	1	Exchange of information between public &
421L4-1	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Specialised and continuous training for law
221L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	2	Promotion of online trust established
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
421L4-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Sophisticated digital forensic tools
422L4-3	Legal and Regulatory	Criminal Justice System	Prosecution	4	Specialised and continuous training for
417L3-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	3	Exceeding minimum requirement in
418L3-2	Legal and Regulatory	Legal Framework	Procedural Cybercrime	3	Exceeding minimum requirement in
432L2-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	2	Established informal cooperation between
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L4-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Sophisticated digital forensic tools
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
411L3-1	Legal and Regulatory	Legal Framework	Legislative Framework for	3	Regular review of cybersecurity legal
131L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	4	Regular review of CI risk priorities
133L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	4	Regular audit of CI
511L4-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Regular review of adoption of standards &
131L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	3	Vulnerability & asset management of CI

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0222	Japan	7-220c	Cybersecurity2017	2017	Improving security standards for CIIs including risk assessment, functionality assurance,
0223	Japan	7-220c	Cybersecurity2017	2017	Improving security standards for CIIs including risk assessment, functionality assurance,
0224	Japan	7-220c	Cybersecurity2017	2017	Improving security standards for CIIs including risk assessment, functionality assurance,
0225	Japan	7-220c2	Cybersecurity2017	2017	Researching for development of information sharing platform for CIIs.
0226	Japan	7-220d	Cybersecurity2017	2017	Improving countermeasures against interference in critical wireless communication.
0227	Japan	7-220e	Cybersecurity2017	2017	Improving stability of telecommunication by analysing incidents in telecommunication.
0228	Japan	7-220f	Cybersecurity2017	2017	Improving incident response ability of CII operators by performing cross-sectional exercises.
0229	Japan	7-220f	Cybersecurity2017	2017	Improving incident response ability of CII operators by performing cross-sectional exercises.
0230	Japan	7-220f	Cybersecurity2017	2017	Improving incident response ability of CII operators by performing cross-sectional exercises.
0231	Japan	7-220f	Cybersecurity2017	2017	Improving incident response ability of CII operators by performing cross-sectional exercises.
0232	Japan	7-220f2	Cybersecurity2017	2017	Performing practical cyber defence exercise "CYDER" for CIIs at "National Cyber Training
0233	Japan	7-220f2	Cybersecurity2017	2017	Performing practical cyber defence exercise "CYDER" for CIIs at "National Cyber Training
0234	Japan	7-220f3	Cybersecurity2017	2017	Performing practical cyber defence exercises with CII operators.
0235	Japan	7-220f3	Cybersecurity2017	2017	Performing practical cyber defence exercises with CII operators.
0236	Japan	7-220f4	Cybersecurity2017	2017	Performing cyber defence exercises in financial services sector.
0237	Japan	7-220f4	Cybersecurity2017	2017	Performing cyber defence exercises in financial services sector.
0238	Japan	7-220g	Cybersecurity2017	2017	Establishing "ICSCoE: Industrial Cyber Security Center of Excellence".
0239	Japan	7-220g	Cybersecurity2017	2017	Establishing "ICSCoE: Industrial Cyber Security Center of Excellence".
0240	Japan	7-221a	Cybersecurity2017	2017	Extending action plans based on "The Basic Policy of Critical Information Infrastructure
0241	Japan	7-221a	Cybersecurity2017	2017	Extending action plans based on "The Basic Policy of Critical Information Infrastructure
0242	Japan	7-222a	Cybersecurity2017	2017	Enhancing information sharing mechanism for CIIs specifically;
0243	Japan	7-222a	Cybersecurity2017	2017	Enhancing information sharing mechanism for CIIs specifically;
0244	Japan	7-222a	Cybersecurity2017	2017	Enhancing information sharing mechanism for CIIs specifically;
0245	Japan	7-222b	Cybersecurity2017	2017	Increasing participants & enhancing shared information of "J-CSIP: Cyber Intelligence
0246	Japan	7-222c	Cybersecurity2017	2017	Assisting CII operators to respond cyber attacks from abroad.
0247	Japan	7-222c	Cybersecurity2017	2017	Assisting CII operators to respond cyber attacks from abroad.
0248	Japan	7-222e	Cybersecurity2017	2017	Enhancing analysis of targeted attacks by using proving environment simulating large scale
0249	Japan	7-222f	Cybersecurity2017	2017	Enhancing information gathering & analysis on cyber attacks & malwares.
0250	Japan	7-222f2	Cybersecurity2017	2017	Enhancing information gathering on cyber attacks.
0251	Japan	7-222f3	Cybersecurity2017	2017	Enhancing information sharing & cooperation with CII operators.
0252	Japan	7-222f4	Cybersecurity2017	2017	Enhancing information sharing with CII operators through "Cyber Terrorism Council".
0253	Japan	7-222g	Cybersecurity2017	2017	Enhancing security countermeasures of credit card settlement system.
0254	Japan	7-222g	Cybersecurity2017	2017	Enhancing security countermeasures of credit card settlement system.
0255	Japan	7-223a	Cybersecurity2017	2017	Supporting local public entities for their cybersecurity.
0256	Japan	7-223a	Cybersecurity2017	2017	Supporting local public entities for their cybersecurity.
0257	Japan	7-223b	Cybersecurity2017	2017	Supporting local public entities to educate & train their personnel for security by holding
0258	Japan	7-223b2	Cybersecurity2017	2017	Supporting local public entities to revise security policies.
0259	Japan	7-223c	Cybersecurity2017	2017	Providing local public entities with intelligence of security incidents & countermeasures
0260	Japan	7-223c	Cybersecurity2017	2017	Providing local public entities with intelligence of security incidents & countermeasures
0261	Japan	7-223d	Cybersecurity2017	2017	Providing local public entities with services of vulnerability scanning & malware detection.
0262	Japan	7-223d2	Cybersecurity2017	2017	Providing local public entities with tools for incident response exercises.
0263	Japan	7-223e	Cybersecurity2017	2017	Establishing integrated cybersecurity network monitoring for government & local public
0264	Japan	7-223e	Cybersecurity2017	2017	Establishing integrated cybersecurity network monitoring for government & local public
0265	Japan	7-223e2	Cybersecurity2017	2017	Supporting local public entities to enhance cybersecurity of their ICTs & to establish cloud
0266	Japan	7-223e2	Cybersecurity2017	2017	Supporting local public entities to enhance cybersecurity of their ICTs & to establish cloud
0267	Japan	7-223e3	Cybersecurity2017	2017	Urging local public entities to isolate "My Number" (Japanese version of Social Security
0268	Japan	7-223e3	Cybersecurity2017	2017	Urging local public entities to isolate "My Number" (Japanese version of Social Security
0269	Japan	7-223e4	Cybersecurity2017	2017	Urging local public entities to comply with "Guidelines for Proper Handling of Specific
0270	Japan	7-223f	Cybersecurity2017	2017	Promoting collaboration of public & private sectors on authentication using "My Number
0271	Japan	7-223g	Cybersecurity2017	2017	Incorporating vulnerability information for control systems into existing operation of
0272	Japan	7-223g	Cybersecurity2017	2017	Incorporating vulnerability information for control systems into existing operation of
0273	Japan	7-223g	Cybersecurity2017	2017	Incorporating vulnerability information for control systems into existing operation of
0274	Japan	7-223h	Cybersecurity2017	2017	Performing practical exercises for control systems of CIIs.
0275	Japan	7-223h	Cybersecurity2017	2017	Performing practical exercises for control systems of CIIs.
0276	Japan	7-223i	Cybersecurity2017	2017	Promoting security assessment & certification for control systems.
0277	Japan	7-223i	Cybersecurity2017	2017	Promoting security assessment & certification for control systems.
0278	Japan	7-223i	Cybersecurity2017	2017	Promoting security assessment & certification for control systems.
0279	Japan	7-230a	Cybersecurity2017	2017	Preparing for next revision of "Common Standards Group for Information Security Measures
0280	Japan	7-230a	Cybersecurity2017	2017	Preparing for next revision of "Common Standards Group for Information Security Measures
0281	Japan	7-230a	Cybersecurity2017	2017	Preparing for next revision of "Common Standards Group for Information Security Measures
0282	Japan	7-231a	Cybersecurity2017	2017	Monitoring & analysing ICT networks of government agencies @24/7.
0283	Japan	7-231b	Cybersecurity2017	2017	Strengthening incident response capabilities of government agencies by enhancing
0284	Japan	7-231b	Cybersecurity2017	2017	Strengthening incident response capabilities of government agencies by enhancing
0285	Japan	7-231b	Cybersecurity2017	2017	Strengthening incident response capabilities of government agencies by enhancing
0286	Japan	7-231c	Cybersecurity2017	2017	Urging government agencies to adopt 'security by design' in procurement.
0287	Japan	7-231c	Cybersecurity2017	2017	Urging government agencies to adopt 'security by design' in procurement.
0288	Japan	7-231c	Cybersecurity2017	2017	Urging government agencies to adopt 'security by design' in procurement.
0289	Japan	7-231c2	Cybersecurity2017	2017	Urging government agencies to consider security upon utilisation of cloud network.
0290	Japan	7-231d	Cybersecurity2017	2017	Reviewing "List of Requirements for Ensuring Security in Procurement of IT Products".
0291	Japan	7-231d2	Cybersecurity2017	2017	Disseminating information including PP (protection profiles) to procurement professionals of
0292	Japan	7-231d2	Cybersecurity2017	2017	Disseminating information including PP (protection profiles) to procurement professionals of
0293	Japan	7-231e	Cybersecurity2017	2017	Reviewing & promoting "JISEC: Japan Information Technology Security and Certification
0294	Japan	7-231e	Cybersecurity2017	2017	Reviewing & promoting "JISEC: Japan Information Technology Security and Certification
0295	Japan	7-231f	Cybersecurity2017	2017	Promoting "JCMVP: Japan Cryptographic Module Validation Program".

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
131L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	4	Regular review of CI risk priorities
132L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Ability to adjust of CI protection
133L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	4	Regular audit of CI
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
133L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	2	Risk management processes in CI
133L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	2	Risk management processes in CI
133L2-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	2	National CI incident response plan
141L2-1	Cybersecurity Policy and	Crisis Management	Crisis Management	2	National incident exercise done
141L2-2	Cybersecurity Policy and	Crisis Management	Crisis Management	2	Appropriate resources for national incident
141L2-3	Cybersecurity Policy and	Crisis Management	Crisis Management	2	Roles in national incident exercise defined
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
511L2-6	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices used by CI supply
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
133L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Regular review of impact analysis of CI
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L2-4	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Government engagement in CI protection
121L3-2	Cybersecurity Policy and	Incident Response	Identification of Incidents	3	Incident analysis
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
431L3-3	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Resources for information exchange between
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
211L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set spread in public sector
211L3-2	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set based strategy in public sector
211L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set spread in public sector
211L3-2	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set based strategy in public sector
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
141L2-1	Cybersecurity Policy and	Crisis Management	Crisis Management	2	National incident exercise done
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
222L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Privacy-by-default in e-gov
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
222L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Privacy-by-default in e-gov
222L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Privacy-by-default in e-gov
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
571L2-1	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	2	Established vulnerability disclosure
571L2-2	Standards, Organisations, and	Responsible Disclosure	Responsible Disclosure	2	Established processes against vulnerability
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
111L4-1	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Continual revision of strategy
113L4-1	Cybersecurity Policy and	National Cybersecurity	Content	4	Continual revision of strategy
511L4-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Regular review of adoption of standards &
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
122L3-2	Cybersecurity Policy and	Incident Response	Organisation	3	Adequate resources for incident response
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
512L3-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Regular review of procurement
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
512L3-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Regular review of procurement
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
512L3-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Regular review of procurement
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0296	Japan	7-231f	Cybersecurity2017	2017	Promoting "JCMVP: Japan Cryptographic Module Validation Program".
0297	Japan	7-231f	Cybersecurity2017	2017	Promoting "JCMVP: Japan Cryptographic Module Validation Program".
0298	Japan	7-231g	Cybersecurity2017	2017	Performing penetration testing to ICT systems of government agencies.
0299	Japan	7-231g	Cybersecurity2017	2017	Performing penetration testing to ICT systems of government agencies.
0300	Japan	7-231h	Cybersecurity2017	2017	Performing vulnerability scanning & examining cybersecurity measures of government
0301	Japan	7-231h	Cybersecurity2017	2017	Performing vulnerability scanning & examining cybersecurity measures of government
0302	Japan	7-231i	Cybersecurity2017	2017	Speeding up detecting & informing incidents to government agencies by enhancing GSOC
0303	Japan	7-231j	Cybersecurity2017	2017	Reviewing policies for obtaining & storing ICT systems logs to enhance incident response
0304	Japan	7-231j	Cybersecurity2017	2017	Reviewing policies for obtaining & storing ICT systems logs to enhance incident response
0305	Japan	7-231k	Cybersecurity2017	2017	Examining CSIRT of government agencies & urging them to enhance incident response
0306	Japan	7-231k	Cybersecurity2017	2017	Examining CSIRT of government agencies & urging them to enhance incident response
0307	Japan	7-231k	Cybersecurity2017	2017	Examining CSIRT of government agencies & urging them to enhance incident response
0308	Japan	7-231l	Cybersecurity2017	2017	Performing cybersecurity exercises for incident response personnel of government agencies.
0309	Japan	7-231l	Cybersecurity2017	2017	Performing cybersecurity exercises for incident response personnel of government agencies.
0310	Japan	7-231l	Cybersecurity2017	2017	Performing cybersecurity exercises for incident response personnel of government agencies.
0311	Japan	7-231l2	Cybersecurity2017	2017	Performing cybersecurity exercises for CYMAT members.
0312	Japan	7-231l2	Cybersecurity2017	2017	Performing cybersecurity exercises for CYMAT members.
0313	Japan	7-231l2	Cybersecurity2017	2017	Performing cybersecurity exercises for CYMAT members.
0314	Japan	7-231l3	Cybersecurity2017	2017	Performing practical cyber defence exercise "CYDER" for government agencies with
0315	Japan	7-231l4	Cybersecurity2017	2017	Performing "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).
0316	Japan	7-231l4	Cybersecurity2017	2017	Performing "NATIONAL 318 (CYBER) EKIDEN" (CTF for government agencies).
0317	Japan	7-231m	Cybersecurity2017	2017	Sharing cybersecurity intelligence with national universities.
0318	Japan	7-231m2	Cybersecurity2017	2017	Supporting national universities to enhance cybersecurity by training security personnel.
0319	Japan	7-231m2	Cybersecurity2017	2017	Supporting national universities to enhance cybersecurity by training security personnel.
0320	Japan	7-231n	Cybersecurity2017	2017	Considering to enhance "NATIONAL 318 (CYBER) EKIDEN" (CTF for government
0321	Japan	7-231n	Cybersecurity2017	2017	Considering to enhance "NATIONAL 318 (CYBER) EKIDEN" (CTF for government
0322	Japan	7-231o	Cybersecurity2017	2017	Training digital forensics professionals.
0323	Japan	7-231o	Cybersecurity2017	2017	Training digital forensics professionals.
0324	Japan	7-231o	Cybersecurity2017	2017	Training digital forensics professionals.
0325	Japan	7-231p	Cybersecurity2017	2017	Promoting "Guidelines for Risk Assessment of Advanced Cyber Attacks Measurements".
0326	Japan	7-231p	Cybersecurity2017	2017	Promoting "Guidelines for Risk Assessment of Advanced Cyber Attacks Measurements".
0327	Japan	7-232a	Cybersecurity2017	2017	Performing audit of all government agencies & related agencies during 2 years based on
0328	Japan	7-232a	Cybersecurity2017	2017	Performing audit of all government agencies & related agencies during 2 years based on
0329	Japan	7-232a	Cybersecurity2017	2017	Performing audit of all government agencies & related agencies during 2 years based on
0330	Japan	7-232b	Cybersecurity2017	2017	Training cybersecurity personnel & experts based on "General Policy for Cybersecurity
0331	Japan	7-232b	Cybersecurity2017	2017	Training cybersecurity personnel & experts based on "General Policy for Cybersecurity
0332	Japan	7-232b	Cybersecurity2017	2017	Training cybersecurity personnel & experts based on "General Policy for Cybersecurity
0333	Japan	7-232c	Cybersecurity2017	2017	Continuing information sharing in cybersecurity community across government.
0334	Japan	7-232d	Cybersecurity2017	2017	Supporting government agencies to develop cybersecurity human resources by training non-
0335	Japan	7-232d	Cybersecurity2017	2017	Supporting government agencies to develop cybersecurity human resources by training non-
0336	Japan	7-232d	Cybersecurity2017	2017	Supporting government agencies to develop cybersecurity human resources by training non-
0337	Japan	7-232e	Cybersecurity2017	2017	Reviewing & reconstructing education & training systems for IT human resources.
0338	Japan	7-232e	Cybersecurity2017	2017	Reviewing & reconstructing education & training systems for IT human resources.
0339	Japan	7-232e	Cybersecurity2017	2017	Reviewing & reconstructing education & training systems for IT human resources.
0340	Japan	7-233a	Cybersecurity2017	2017	Researching & developing security measures for cloud services, standardising if necessary.
0341	Japan	7-233a	Cybersecurity2017	2017	Researching & developing security measures for cloud services, standardising if necessary.
0342	Japan	7-233b	Cybersecurity2017	2017	Promoting 'security-by-design' in obtainment of new ICT systems for administrative
0343	Japan	7-233b	Cybersecurity2017	2017	Promoting 'security-by-design' in obtainment of new ICT systems for administrative
0344	Japan	7-233b	Cybersecurity2017	2017	Promoting 'security-by-design' in obtainment of new ICT systems for administrative
0345	Japan	7-234a	Cybersecurity2017	2017	Performing audit of related agencies (besides government agencies) on cybersecurity.
0346	Japan	7-234a	Cybersecurity2017	2017	Performing audit of related agencies (besides government agencies) on cybersecurity.
0347	Japan	7-234a	Cybersecurity2017	2017	Performing audit of related agencies (besides government agencies) on cybersecurity.
0348	Japan	7-310a	Cybersecurity2017	2017	Performing initial response exercises in preparation for potential large-scale cyber attack.
0349	Japan	7-310b	Cybersecurity2017	2017	Enhancing resources for collection & analysis of cyber attack intelligence from homeland &
0350	Japan	7-311a	Cybersecurity2017	2017	Enhancing counter-intelligence capabilities.
0351	Japan	7-311a	Cybersecurity2017	2017	Enhancing counter-intelligence capabilities.
0352	Japan	7-311c	Cybersecurity2017	2017	Enhancing capability of Cyber Force Center by performing exercises & upgrading
0353	Japan	7-311c	Cybersecurity2017	2017	Enhancing capability of Cyber Force Center by performing exercises & upgrading
0354	Japan	7-311c2	Cybersecurity2017	2017	Performing cybersecurity exercises for large-scale industrial control systems.
0355	Japan	7-311c2	Cybersecurity2017	2017	Performing cybersecurity exercises for large-scale industrial control systems.
0356	Japan	7-311c3	Cybersecurity2017	2017	Enhancing analytic capabilities of malwares.
0357	Japan	7-311d	Cybersecurity2017	2017	Considering education & training of highly professional human resources.
0358	Japan	7-311e	Cybersecurity2017	2017	Enhancing protection & analysis equipment & cyber intelligence collection equipment.
0359	Japan	7-311e2	Cybersecurity2017	2017	Enhancing security of "DII: Defense Information Infrastructure".
0360	Japan	7-311f	Cybersecurity2017	2017	Performing practical exercises on environment simulating defence information systems.
0361	Japan	7-311f	Cybersecurity2017	2017	Performing practical exercises on environment simulating defence information systems.
0362	Japan	7-311g	Cybersecurity2017	2017	Training CSIRT members for response against highly advanced attacks.
0363	Japan	7-311g	Cybersecurity2017	2017	Training CSIRT members for response against highly advanced attacks.
0364	Japan	7-311h	Cybersecurity2017	2017	Preparing for penetration testing of defence information network.
0365	Japan	7-311i	Cybersecurity2017	2017	Researching contingency operation of defence information infrastructures.
0366	Japan	7-311i	Cybersecurity2017	2017	Researching contingency operation of defence information infrastructures.
0367	Japan	7-312a	Cybersecurity2017	2017	Implementing cybersecurity measures of supply chains of defence equipment.
0368	Japan	7-312a	Cybersecurity2017	2017	Implementing cybersecurity measures of supply chains of defence equipment.
0369	Japan	7-312b	Cybersecurity2017	2017	Backing-up National Research and Development Agencies with leading technologies

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
512L3-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Regular review of procurement
551L3-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	3	Regular review of cryptographic control
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
541L3-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	User side security controls
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
541L3-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	User side security controls
124L3-2	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Sophisticated incident analysis
124L3-2	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Sophisticated incident analysis
124L3-4	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Forensics
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
124L2-2	Cybersecurity Policy and	Incident Response	Mode of Operation	2	Regular training for CSIRT members
124L3-3	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Regular review of incident response processes
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
124L2-2	Cybersecurity Policy and	Incident Response	Mode of Operation	2	Regular training for CSIRT members
124L3-3	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Regular review of incident response processes
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
124L2-2	Cybersecurity Policy and	Incident Response	Mode of Operation	2	Regular training for CSIRT members
124L3-3	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Regular review of incident response processes
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
124L3-1	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Training & accreditation for CSIRT members
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
431L1-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	1	Exchange of information between public &
311L3-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Sector specific programmes of awareness
331L2-4	Cybersecurity Education,	Framework for Professional	Provision	2	Cybersecurity training programmes for non-
124L3-1	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Training & accreditation for CSIRT members
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
124L3-2	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Sophisticated incident analysis
124L3-4	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Forensics
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
124L2-2	Cybersecurity Policy and	Incident Response	Mode of Operation	2	Regular training for CSIRT members
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
211L2-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	2	Most officials have mind-set
331L2-4	Cybersecurity Education,	Framework for Professional	Provision	2	Cybersecurity training programmes for non-
124L4-2	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Evaluating effectiveness of CSIRT members
331L3-4	Cybersecurity Education,	Framework for Professional	Provision	3	Metrics of effectiveness of cybersecurity
332L3-1	Cybersecurity Education,	Framework for Professional	Uptake	3	Review of cybersecurity training programmes
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
512L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	1	Promotion of use of standards & best
513L1-2	Standards, Organisations, and	Adherence to Standards	Standards in Software	1	Promotion of use of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
541L1-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	1	Latest technical security controls promoted
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
141L2-1	Cybersecurity Policy and	Crisis Management	Crisis Management	2	National incident exercise done
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
152L3-2	Cybersecurity Policy and	Cyber Defence	Organisation	3	Counter-cyber intelligence activities
152L4-2	Cybersecurity Policy and	Cyber Defence	Organisation	4	Established counter-cyber intelligence
124L3-2	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Sophisticated incident analysis
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
124L3-1	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Training & accreditation for CSIRT members
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
161L4-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	4	Optimised for extended outages
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
511L2-6	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices used by CI supply
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
0370	Japan	7-312b	Cybersecurity2017	2017	Backing-up National Research and Development Agencies with leading technologies
0371	Japan	7-312b2	Cybersecurity2017	2017	Supporting universities with leading technologies to enhance countermeasures against
0372	Japan	7-312b2	Cybersecurity2017	2017	Supporting universities with leading technologies to enhance countermeasures against
0373	Japan	7-312b2	Cybersecurity2017	2017	Supporting universities with leading technologies to enhance countermeasures against
0374	Japan	7-313a	Cybersecurity2017	2017	Enhancing cooperation between MOD & defence industry.
0375	Japan	7-313a	Cybersecurity2017	2017	Enhancing cooperation between MOD & defence industry.
0376	Japan	7-320a	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0377	Japan	7-320a	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0378	Japan	7-320a	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0379	Japan	7-320a	Cybersecurity2017	2017	Continuing operation of "TSUBAME" (Asia & Pacific region internet fixed point
0380	Japan	7-321a	Cybersecurity2017	2017	Positively contributing to international debate of international laws, rules & codes for
0381	Japan	7-321a	Cybersecurity2017	2017	Positively contributing to international debate of international laws, rules & codes for
0382	Japan	7-321a	Cybersecurity2017	2017	Positively contributing to international debate of international laws, rules & codes for
0383	Japan	7-321a	Cybersecurity2017	2017	Positively contributing to international debate of international laws, rules & codes for
0384	Japan	7-321a	Cybersecurity2017	2017	Positively contributing to international debate of international laws, rules & codes for
0385	Japan	7-321b	Cybersecurity2017	2017	Speeding up international assistance in investigation of cybercrimes under treaty for mutual
0386	Japan	7-321b	Cybersecurity2017	2017	Speeding up international assistance in investigation of cybercrimes under treaty for mutual
0387	Japan	7-321b	Cybersecurity2017	2017	Speeding up international assistance in investigation of cybercrimes under treaty for mutual
0388	Japan	7-321c	Cybersecurity2017	2017	Exchanging information with law enforcement of those countries who are related to Japanese
0389	Japan	7-321c	Cybersecurity2017	2017	Exchanging information with law enforcement of those countries who are related to Japanese
0390	Japan	7-321c2	Cybersecurity2017	2017	Positively contributing to international framework for cooperation of anti-cybercrime.
0391	Japan	7-321c2	Cybersecurity2017	2017	Positively contributing to international framework for cooperation of anti-cybercrime.
0392	Japan	7-321c3	Cybersecurity2017	2017	Enhancing relationship with neighbouring countries by holding Asian Pacific Regional Cyber
0393	Japan	7-321c3	Cybersecurity2017	2017	Enhancing relationship with neighbouring countries by holding Asian Pacific Regional Cyber
0394	Japan	7-321d	Cybersecurity2017	2017	Positively contributing to promotion of "Budapest Convention on Cybercrime" (the first
0395	Japan	7-321d	Cybersecurity2017	2017	Positively contributing to promotion of "Budapest Convention on Cybercrime" (the first
0396	Japan	7-321d	Cybersecurity2017	2017	Positively contributing to promotion of "Budapest Convention on Cybercrime" (the first
0397	Japan	7-322a	Cybersecurity2017	2017	Contributing to UN effort to establish international rules to prevent contingencies from
0398	Japan	7-322a	Cybersecurity2017	2017	Contributing to UN effort to establish international rules to prevent contingencies from
0399	Japan	7-322a	Cybersecurity2017	2017	Contributing to UN effort to establish international rules to prevent contingencies from
0400	Japan	7-322a2	Cybersecurity2017	2017	Sharing information about cyber threat & cybersecurity strategies through bilateral meetings.
0401	Japan	7-322b	Cybersecurity2017	2017	Enhancing international relationship & cooperation through participating international
0402	Japan	7-322b	Cybersecurity2017	2017	Enhancing international relationship & cooperation through participating international
0403	Japan	7-322b	Cybersecurity2017	2017	Enhancing international relationship & cooperation through participating international
0404	Japan	7-322b	Cybersecurity2017	2017	Enhancing international relationship & cooperation through participating international
0405	Japan	7-322c	Cybersecurity2017	2017	Continuing & enhancing international coordination & cooperation in incident responses,
0406	Japan	7-322c	Cybersecurity2017	2017	Continuing & enhancing international coordination & cooperation in incident responses,
0407	Japan	7-322c	Cybersecurity2017	2017	Continuing & enhancing international coordination & cooperation in incident responses,
0408	Japan	7-323a	Cybersecurity2017	2017	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace under
0409	Japan	7-323a	Cybersecurity2017	2017	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace under
0410	Japan	7-323a	Cybersecurity2017	2017	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace under
0411	Japan	7-323b	Cybersecurity2017	2017	Enhancing intelligence gathering & analysis of terrorism activities in cyberspace.
412	Japan	7-324a	Cybersecurity2017	2017	Government agencies positively support other nations based on "Basic Policy for Assistance
413	Japan	7-324a	Cybersecurity2017	2017	Government agencies positively support other nations based on "Basic Policy for Assistance
414	Japan	7-324a2	Cybersecurity2017	2017	Supporting countries in Asian Pacific region to build cybersecurity capabilities through
415	Japan	7-324a2	Cybersecurity2017	2017	Supporting countries in Asian Pacific region to build cybersecurity capabilities through
416	Japan	7-324a2	Cybersecurity2017	2017	Supporting countries in Asian Pacific region to build cybersecurity capabilities through
417	Japan	7-324a3	Cybersecurity2017	2017	Contributing to regional cybersecurity awareness raising through "APT: Asia-Pacific
418	Japan	7-324a4	Cybersecurity2017	2017	Supporting ASEAN countries to build cybersecurity capabilities through "Asian Pacific
419	Japan	7-324a4	Cybersecurity2017	2017	Supporting ASEAN countries to build cybersecurity capabilities through "Asian Pacific
420	Japan	7-324a5	Cybersecurity2017	2017	Supporting ASEAN countries to build cybersecurity capabilities by holding seminars of
421	Japan	7-324a5	Cybersecurity2017	2017	Supporting ASEAN countries to build cybersecurity capabilities by holding seminars of
422	Japan	7-324a6	Cybersecurity2017	2017	Supporting countries in Asian Pacific & Africa to build & operate national CSIRTs.
423	Japan	7-324a6	Cybersecurity2017	2017	Supporting countries in Asian Pacific & Africa to build & operate national CSIRTs.
424	Japan	7-324a7	Cybersecurity2017	2017	Holding seminars for 'secure development' for foreign software suppliers.
425	Japan	7-324a7	Cybersecurity2017	2017	Holding seminars for 'secure development' for foreign software suppliers.
426	Japan	7-325a	Cybersecurity2017	2017	Encouraging personnel of government agencies & related agencies to attend international
427	Japan	7-325a	Cybersecurity2017	2017	Encouraging personnel of government agencies & related agencies to attend international
428	Japan	7-325a	Cybersecurity2017	2017	Encouraging personnel of government agencies & related agencies to attend international
429	Japan	7-330b	Cybersecurity2017	2017	Enhancing coordination & cooperation of G7 through "Ise-Shima Cyber Group".
430	Japan	7-330b	Cybersecurity2017	2017	Enhancing coordination & cooperation of G7 through "Ise-Shima Cyber Group".
431	Japan	7-330b	Cybersecurity2017	2017	Enhancing coordination & cooperation of G7 through "Ise-Shima Cyber Group".
432	Japan	7-330c	Cybersecurity2017	2017	Continuing & extending international cooperation through bilateral meetings.
433	Japan	7-330c	Cybersecurity2017	2017	Continuing & extending international cooperation through bilateral meetings.
434	Japan	7-330c	Cybersecurity2017	2017	Continuing & extending international cooperation through bilateral meetings.
435	Japan	7-330d	Cybersecurity2017	2017	Enhancing intelligence sharing with foreign governments.
436	Japan	7-330e	Cybersecurity2017	2017	Contributing to international effort to raise cybersecurity awareness.
437	Japan	7-330f	Cybersecurity2017	2017	Enhancing intelligence sharing with foreign law enforcement & legal communities.
438	Japan	7-330f	Cybersecurity2017	2017	Enhancing intelligence sharing with foreign law enforcement & legal communities.
439	Japan	7-330f	Cybersecurity2017	2017	Enhancing intelligence sharing with foreign law enforcement & legal communities.
440	Japan	7-330g	Cybersecurity2017	2017	Researching technologies for measuring cyber health of countries/regions ("Cyber Green
441	Japan	7-330h	Cybersecurity2017	2017	Enhancing information sharing with foreign agencies for information security like NIST.
442	Japan	7-330j	Cybersecurity2017	2017	Considering possible cooperation in cyberspace between MOD/JSDF & foreign forces.
443	Japan	7-330j	Cybersecurity2017	2017	Considering possible cooperation in cyberspace between MOD/JSDF & foreign forces.

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
511L2-6	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices used by CI supply
122L4-2	Cybersecurity Policy and	Incident Response	Organisation	4	Early warning capability
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
151L4-1	Cybersecurity Policy and	Cyber Defence	Strategy	4	Rules of engagement in cyberspace
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
431L2-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Mutual legal assistance & extradition
431L3-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Strategically expanding international
431L4-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	4	Regular review of international cooperation
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
432L1-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	1	Informal international cooperation in law
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
432L1-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	1	Informal international cooperation in law
417L2-2	Legal and Regulatory	Legal Framework	Substantive Cybercrime	2	Participation to international agreements on
418L2-2	Legal and Regulatory	Legal Framework	Procedural Cybercrime	2	Participation to international agreements on
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
151L4-1	Cybersecurity Policy and	Cyber Defence	Strategy	4	Rules of engagement in cyberspace
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
151L3-2	Cybersecurity Policy and	Cyber Defence	Strategy	3	Capturing landscape of national-level threat
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
411L4-2	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Participation to international cooperation
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
332L4-1	Cybersecurity Education,	Framework for Professional	Uptake	4	Cybersecurity trained professionals
511L2-6	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices used by CI supply
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
331L3-1	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
431L3-2	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Strategically expanding international
432L1-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	1	Informal international cooperation in law
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
444	Japan	7-330j	Cybersecurity2017	2017	Considering possible cooperation in cyberspace between MOD/JSDF & foreign forces.
445	Japan	7-331a2	Cybersecurity2017	2017	Building regional confidence measures through "ARF: ASEAN Regional Forum".
446	Japan	7-331a2	Cybersecurity2017	2017	Building regional confidence measures through "ARF: ASEAN Regional Forum".
447	Japan	7-331b	Cybersecurity2017	2017	Supporting countries in Asian Pacific region to establish cybercrime jurisdiction.
448	Japan	7-331b	Cybersecurity2017	2017	Supporting countries in Asian Pacific region to establish cybercrime jurisdiction.
449	Japan	7-331c	Cybersecurity2017	2017	Establishing cooperation with South-East Asian countries & Australia in cybersecurity.
450	Japan	7-331c	Cybersecurity2017	2017	Establishing cooperation with South-East Asian countries & Australia in cybersecurity.
451	Japan	7-332a	Cybersecurity2017	2017	Enhancing coordination & cooperation with US through "Japan-U.S. Cyber Dialogues".
452	Japan	7-332a	Cybersecurity2017	2017	Enhancing coordination & cooperation with US through "Japan-U.S. Cyber Dialogues".
453	Japan	7-332a	Cybersecurity2017	2017	Enhancing coordination & cooperation with US through "Japan-U.S. Cyber Dialogues".
454	Japan	7-332a2	Cybersecurity2017	2017	Enhancing cyber defence cooperation with European countries through "Japan-UK Bilateral
455	Japan	7-332a2	Cybersecurity2017	2017	Enhancing cyber defence cooperation with European countries through "Japan-UK Bilateral
456	Japan	7-332b	Cybersecurity2017	2017	Enhancing information sharing with US based on "U.S.-Japan Policy Cooperation Dialogue
457	Japan	7-332b2	Cybersecurity2017	2017	Promoting cooperation between Japan's ICT-ISAC & US IT-ISAC.
458	Japan	7-332b2	Cybersecurity2017	2017	Promoting cooperation between Japan's ICT-ISAC & US IT-ISAC.
459	Japan	7-332c	Cybersecurity2017	2017	Enhancing cyber defence cooperation with US through "U.S.-Japan Cyber defence Policy
460	Japan	7-332c	Cybersecurity2017	2017	Enhancing cyber defence cooperation with US through "U.S.-Japan Cyber defence Policy
461	Japan	7-333a	Cybersecurity2017	2017	Enhancing cooperation through bilateral meetings.
462	Japan	7-333b	Cybersecurity2017	2017	Gathering information on latest technologies through consultation with "JIWG: Joint
463	Japan	7-334a	Cybersecurity2017	2017	Enhancing cooperation through bilateral meetings.
464	Japan	7-410a	Cybersecurity2017	2017	Establishing "Strategy for Research & Development of Cybersecurity".
465	Japan	7-410b	Cybersecurity2017	2017	Researching security assessment of cryptographic algorisms & protocols.
466	Japan	7-411a	Cybersecurity2017	2017	Researching technologies for countermeasures against cyber attacks.
467	Japan	7-411a2	Cybersecurity2017	2017	Building up large scale reservoir of cybersecurity related information.
468	Japan	7-411a3	Cybersecurity2017	2017	Improving R&D environment by establishing security validation platform.
469	Japan	7-411b	Cybersecurity2017	2017	Researching technologies for detection & prediction of cyber attacks on control systems.
470	Japan	7-411b	Cybersecurity2017	2017	Researching technologies for detection & prediction of cyber attacks on control systems.
471	Japan	7-411b2	Cybersecurity2017	2017	Researching technologies for vulnerability management on control systems without
472	Japan	7-411b2	Cybersecurity2017	2017	Researching technologies for vulnerability management on control systems without
473	Japan	7-411b2	Cybersecurity2017	2017	Researching technologies for vulnerability management on control systems without
474	Japan	7-411c	Cybersecurity2017	2017	Providing with "NONSTOP" (R&D platform for secure handling of malware samples).
475	Japan	7-411d	Cybersecurity2017	2017	Researching technologies for data analysis & resilience against cyber attacks.
476	Japan	7-411d	Cybersecurity2017	2017	Researching technologies for data analysis & resilience against cyber attacks.
477	Japan	7-412a	Cybersecurity2017	2017	Same as 7-410a2
478	Japan	7-412a	Cybersecurity2017	2017	Same as 7-410a2
479	Japan	7-412a	Cybersecurity2017	2017	Same as 7-410a2
480	Japan	7-412b	Cybersecurity2017	2017	Researching technologies for creation of cyber-physical system.
481	Japan	7-412b	Cybersecurity2017	2017	Researching technologies for creation of cyber-physical system.
482	Japan	7-412b	Cybersecurity2017	2017	Researching technologies for creation of cyber-physical system.
483	Japan	7-412c	Cybersecurity2017	2017	Promoting researching of advanced AI infrastructure & its practical research for
484	Japan	7-412c	Cybersecurity2017	2017	Promoting researching of advanced AI infrastructure & its practical research for
485	Japan	7-412c	Cybersecurity2017	2017	Promoting researching of advanced AI infrastructure & its practical research for
486	Japan	7-413a	Cybersecurity2017	2017	Researching for quantum cryptography communication.
487	Japan	7-413b	Cybersecurity2017	2017	Promoting "The List of Ciphers that should be Referred to in the Procurement for the e-
488	Japan	7-413b2	Cybersecurity2017	2017	Researching technologies for secure cryptography.
489	Japan	7-413b3	Cybersecurity2017	2017	Promoting use of secure cryptography.
490	Japan	7-413c	Cybersecurity2017	2017	Researching innovative & advanced technologies for balancing security & efficiency of
491	Japan	7-413c	Cybersecurity2017	2017	Researching innovative & advanced technologies for balancing security & efficiency of
492	Japan	7-414a	Cybersecurity2017	2017	Positively contributing to international debate of standards for information security by
493	Japan	7-415a	Cybersecurity2017	2017	Researching technologies for monitoring & analysis of control & communication systems
494	Japan	7-415a	Cybersecurity2017	2017	Researching technologies for monitoring & analysis of control & communication systems
495	Japan	7-415a	Cybersecurity2017	2017	Researching technologies for monitoring & analysis of control & communication systems
496	Japan	7-415a	Cybersecurity2017	2017	Researching technologies for monitoring & analysis of control & communication systems
497	Japan	7-420a	Cybersecurity2017	2017	Promoting human resources development based on "Cybersecurity Human Resources
498	Japan	7-420a	Cybersecurity2017	2017	Promoting human resources development based on "Cybersecurity Human Resources
499	Japan	7-421a	Cybersecurity2017	2017	Promoting practical exercise & PBL (problem based learning) on cybersecurity by
500	Japan	7-421a	Cybersecurity2017	2017	Promoting practical exercise & PBL (problem based learning) on cybersecurity by
501	Japan	7-421a	Cybersecurity2017	2017	Promoting practical exercise & PBL (problem based learning) on cybersecurity by
502	Japan	7-421b	Cybersecurity2017	2017	Promoting collaboration of industry, government & academia on practical cyber exercises.
503	Japan	7-421b	Cybersecurity2017	2017	Promoting collaboration of industry, government & academia on practical cyber exercises.
504	Japan	7-421b	Cybersecurity2017	2017	Promoting collaboration of industry, government & academia on practical cyber exercises.
505	Japan	7-421b	Cybersecurity2017	2017	Promoting collaboration of industry, government & academia on practical cyber exercises.
506	Japan	7-421c	Cybersecurity2017	2017	Developing human resources with hybrid careers.
507	Japan	7-421c	Cybersecurity2017	2017	Developing human resources with hybrid careers.
508	Japan	7-421c	Cybersecurity2017	2017	Developing human resources with hybrid careers.
509	Japan	7-421d	Cybersecurity2017	2017	Enhancing cybersecurity education at colleges of technology ("Kosen") based on needs from
510	Japan	7-421d	Cybersecurity2017	2017	Enhancing cybersecurity education at colleges of technology ("Kosen") based on needs from
511	Japan	7-421d	Cybersecurity2017	2017	Enhancing cybersecurity education at colleges of technology ("Kosen") based on needs from
512	Japan	7-421e	Cybersecurity2017	2017	Promoting cybersecurity education for working adults at universities.
513	Japan	7-421e	Cybersecurity2017	2017	Promoting cybersecurity education for working adults at universities.
514	Japan	7-421f	Cybersecurity2017	2017	Incorporating cybersecurity education into public vocational training.
515	Japan	7-421f	Cybersecurity2017	2017	Incorporating cybersecurity education into public vocational training.
516	Japan	7-422a	Cybersecurity2017	2017	Promoting education at elementary, middle & high schools about IT, information security &
517	Japan	7-422a	Cybersecurity2017	2017	Promoting education at elementary, middle & high schools about IT, information security &

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
411L4-4	Legal and Regulatory	Legal Framework	Legislative Framework for	4	International and/or regional cooperation of
432L4-4	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	International and/or regional cooperation of
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
432L3-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	3	Cooperation between foreign ISPs & law
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
123L2-3	Cybersecurity Policy and	Incident Response	Coordination	2	International cooperation in incident response
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
551L4-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Revision of cryptographic control policies
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
551L2-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	2	Cryptographic controls widely used
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
521L4-3	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of critical technologies
521L4-4	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Independency & persistence of internet
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
332L3-1	Cybersecurity Education,	Framework for Professional	Uptake	3	Review of cybersecurity training programmes
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
331L4-2	Cybersecurity Education,	Framework for Professional	Provision	4	Coordination between cybersecurity training
332L3-2	Cybersecurity Education,	Framework for Professional	Uptake	3	Coordination of cybersecurity training across
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
331L3-3	Cybersecurity Education,	Framework for Professional	Provision	3	Communication skills in cybersecurity training
331L4-3	Cybersecurity Education,	Framework for Professional	Provision	4	Incentives for cybersecurity trained workforce
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
331L2-4	Cybersecurity Education,	Framework for Professional	Provision	2	Cybersecurity training programmes for non-
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
213L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	4	Users' mind-set reducing threat

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
518	Japan	7-422a	Cybersecurity2017	2017	Promoting education at elementary, middle & high schools about IT, information security &
519	Japan	7-422a	Cybersecurity2017	2017	Promoting education at elementary, middle & high schools about IT, information security &
520	Japan	7-422b	Cybersecurity2017	2017	Training teachers for IT skills & information moral
521	Japan	7-422b	Cybersecurity2017	2017	Training teachers for IT skills & information moral
522	Japan	7-422b	Cybersecurity2017	2017	Training teachers for IT skills & information moral
523	Japan	7-422b	Cybersecurity2017	2017	Training teachers for IT skills & information moral
524	Japan	7-423a	Cybersecurity2017	2017	Continuing to hold "Security Camp" to raise awareness of youth & to discover prominent
525	Japan	7-423a	Cybersecurity2017	2017	Continuing to hold "Security Camp" to raise awareness of youth & to discover prominent
526	Japan	7-423b	Cybersecurity2017	2017	Jointly promoting CTFs with "JNSA: Japan Network Security Association".
527	Japan	7-423c	Cybersecurity2017	2017	Conducting "MITOU Program: Exploratory IT Human Resources Project" to discover
528	Japan	7-423c	Cybersecurity2017	2017	Conducting "MITOU Program: Exploratory IT Human Resources Project" to discover
529	Japan	7-424a	Cybersecurity2017	2017	Promoting "Information Technology Engineers Examination" to develop highly skilled IT
530	Japan	7-424a	Cybersecurity2017	2017	Promoting "Information Technology Engineers Examination" to develop highly skilled IT
531	Japan	7-424a	Cybersecurity2017	2017	Promoting "Information Technology Engineers Examination" to develop highly skilled IT
532	Japan	7-424b	Cybersecurity2017	2017	Promoting "Information Security Management Examination" (a subject of "Information
533	Japan	7-424c	Cybersecurity2017	2017	Supporting young engineers & student to design their career pass in IT industry.
534	Japan	7-424d	Cybersecurity2017	2017	Promoting new national qualification "Registered Information Security Specialist".
535	Japan	7-424d	Cybersecurity2017	2017	Promoting new national qualification "Registered Information Security Specialist".
536	Japan	7-424d	Cybersecurity2017	2017	Promoting new national qualification "Registered Information Security Specialist".
537	Japan	7-424e	Cybersecurity2017	2017	Training youth to cybersecurity expert at "National Cyber Training Center".
538	Japan	7-424e	Cybersecurity2017	2017	Training youth to cybersecurity expert at "National Cyber Training Center".
539	Japan	7-425a	Cybersecurity2017	2017	Sending officials to study at graduate schools.
540	Japan	7-425a	Cybersecurity2017	2017	Sending officials to study at graduate schools.
541	Japan	7-425a	Cybersecurity2017	2017	Sending officials to study at graduate schools.
542	Japan	7-425b	Cybersecurity2017	2017	Performing upgraded practical cyber defence exercise "(New) CYDER" at "National Cyber
543	Japan	7-425c	Cybersecurity2017	2017	Establishing practical exercise environment of communication system of JSDF.
544	Japan	7-425d	Cybersecurity2017	2017	Enhancing cooperation between MOD/JSDF & defence industry.
545	Japan	7-425d2	Cybersecurity2017	2017	Enhancing cooperation between MOD/JSDF & operators of infrastructures affecting
546	Japan	7-425d2	Cybersecurity2017	2017	Enhancing cooperation between MOD/JSDF & operators of infrastructures affecting
547	U.K.	5105-1	Strategy2016-2023	2016	Blocking known malware sources
548	U.K.	5105-1	Strategy2016-2023	2016	Blocking known malware sources
549	U.K.	5105-1	Strategy2016-2023	2016	Blocking known malware sources
550	U.K.	5105-2	Strategy2016-2023	2016	Promoting email verification systems
551	U.K.	5105-2	Strategy2016-2023	2016	Promoting email verification systems
552	U.K.	5105-3	Strategy2016-2023	2016	Promoting security best practices
553	U.K.	5105-3	Strategy2016-2023	2016	Promoting security best practices
554	U.K.	5105-4	Strategy2016-2023	2016	Implementing secure routing
555	U.K.	5105-4	Strategy2016-2023	2016	Implementing secure routing
556	U.K.	5105-5	Strategy2016-2023	2016	Enhancing capabilities against state-sponsored cyber activities
557	U.K.	5105-5	Strategy2016-2023	2016	Enhancing capabilities against state-sponsored cyber activities
558	U.K.	5105-6	Strategy2016-2023	2016	Promoting technical development
559	U.K.	5106-1	Strategy2016-2023	2016	Metrics
560	U.K.	5106-1	Strategy2016-2023	2016	Metrics
561	U.K.	5205-1	Strategy2016-2023	2016	Security settings by default
562	U.K.	5205-1	Strategy2016-2023	2016	Security settings by default
563	U.K.	5205-1	Strategy2016-2023	2016	Security settings by default
564	U.K.	5205-2	Strategy2016-2023	2016	Developing IP reputation informing service
565	U.K.	5205-2	Strategy2016-2023	2016	Developing IP reputation informing service
566	U.K.	5205-2	Strategy2016-2023	2016	Developing IP reputation informing service
567	U.K.	5205-3	Strategy2016-2023	2016	Software integrity assuarance
568	U.K.	5205-3	Strategy2016-2023	2016	Software integrity assuarance
569	U.K.	5205-4	Strategy2016-2023	2016	Promoting out-of-date browsers filtering
570	U.K.	5205-4	Strategy2016-2023	2016	Promoting out-of-date browsers filtering
571	U.K.	5205-4	Strategy2016-2023	2016	Promoting out-of-date browsers filtering
572	U.K.	5205-5	Strategy2016-2023	2016	Investing new technologies like TPM, FIDO
573	U.K.	5205-5	Strategy2016-2023	2016	Investing new technologies like TPM, FIDO
574	U.K.	5205-5	Strategy2016-2023	2016	Investing new technologies like TPM, FIDO
575	U.K.	5205-5	Strategy2016-2023	2016	Investing new technologies like TPM, FIDO
576	U.K.	5205-5	Strategy2016-2023	2016	Investing new technologies like TPM, FIDO
577	U.K.	5206-1	Strategy2016-2023	2016	Introducing security ratings for products
578	U.K.	5206-1	Strategy2016-2023	2016	Introducing security ratings for products
579	U.K.	5207-1	Strategy2016-2023	2016	Metrics
580	U.K.	5303-1	Strategy2016-2023	2016	Promoting e-government
581	U.K.	5303-2	Strategy2016-2023	2016	'Security-by-default' in e-government
582	U.K.	5303-2	Strategy2016-2023	2016	'Security-by-default' in e-government
583	U.K.	5304-1	Strategy2016-2023	2016	Eliminating unsupported softwares in public sector
584	U.K.	5304-1	Strategy2016-2023	2016	Eliminating unsupported softwares in public sector
585	U.K.	5305-1	Strategy2016-2023	2016	Comprehensive knowledge about all public sector systems
586	U.K.	5305-2	Strategy2016-2023	2016	Promoting best practices in public sector
587	U.K.	5305-3	Strategy2016-2023	2016	Cyber exercise
588	U.K.	5305-3	Strategy2016-2023	2016	Cyber exercise
589	U.K.	5305-3	Strategy2016-2023	2016	Cyber exercise
590	U.K.	5305-4	Strategy2016-2023	2016	Participation of lower levels of public sector
591	U.K.	5305-5	Strategy2016-2023	2016	Automated vulnerability scan on e-government

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
311L4-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Entire society involved in awareness raising
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
213L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	4	Users' mind-set reducing threat
311L4-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Entire society involved in awareness raising
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
332L3-2	Cybersecurity Education,	Framework for Professional	Uptake	3	Coordination of cybersecurity training across
321L3-3	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity specific degree
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
331L2-1	Cybersecurity Education,	Framework for Professional	Provision	2	Structured cybersecurity training programmes
331L2-2	Cybersecurity Education,	Framework for Professional	Provision	2	Security professional certification
332L2-1	Cybersecurity Education,	Framework for Professional	Uptake	2	Cybersecurity trained & certified employees
331L1-2	Cybersecurity Education,	Framework for Professional	Provision	1	Cybersecurity training for general IT staff
322L2-3	Cybersecurity Education,	Framework for Education	Administration	2	Attractiveness of cybersecurity career
331L2-2	Cybersecurity Education,	Framework for Professional	Provision	2	Security professional certification
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
332L2-3	Cybersecurity Education,	Framework for Professional	Uptake	2	Job creation in cybersecurity
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
331L4-2	Cybersecurity Education,	Framework for Professional	Provision	4	Coordination between cybersecurity training
124L3-1	Cybersecurity Policy and	Incident Response	Mode of Operation	3	Training & accreditation for CSIRT members
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
153L2-1	Cybersecurity Policy and	Cyber Defence	Coordination	2	Coordination between CI & defence
153L2-2	Cybersecurity Policy and	Cyber Defence	Coordination	2	Intelligence sharing between CI & defence
521L3-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	3	Investment to new technologies in internet
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
541L4-3	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Supplemental security services by ISPs
541L3-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	User side security controls
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
521L3-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	3	Investment to new technologies in internet
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
531L2-2	Standards, Organisations, and	Software Quality	Software Quality	2	Softwares complying with international
541L2-5	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Technical security controls based on
222L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	2	Risk reduction in e-gov
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov
521L3-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	3	Investment to new technologies in internet
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
531L3-4	Standards, Organisations, and	Software Quality	Software Quality	3	Software deficiency handling
222L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	2	Risk reduction in e-gov
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
222L2-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	2	Risk reduction in e-gov
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov
521L3-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	3	Investment to new technologies in internet
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
551L4-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Revision of cryptographic control policies
531L2-4	Standards, Organisations, and	Software Quality	Software Quality	2	Software classification
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
513L2-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	2	Metrics of adoption of standards & best
222L2-3	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	2	Promotion of e-gov
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
111L3-2	Cybersecurity Policy and	National Cybersecurity	Strategy Development	3	Cyber exercises considered in strategy
124L2-1	Cybersecurity Policy and	Incident Response	Mode of Operation	2	Incident response processes & tools
141L2-1	Cybersecurity Policy and	Crisis Management	Crisis Management	2	National incident exercise done
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
592	U.K.	5305-5	Strategy2016-2023	2016	Automated vulnerability scan on e-government
593	U.K.	5306-1	Strategy2016-2023	2016	Awarenes raising in public sector
594	U.K.	5306-1	Strategy2016-2023	2016	Awarenes raising in public sector
595	U.K.	5306-2	Strategy2016-2023	2016	Development of cyber expertise
596	U.K.	5306-2	Strategy2016-2023	2016	Development of cyber expertise
597	U.K.	5307-1	Strategy2016-2023	2016	Developing new guidance
598	U.K.	5307-1	Strategy2016-2023	2016	Developing new guidance
599	U.K.	5307-2	Strategy2016-2023	2016	Making cyber threat infomation easily available
600	U.K.	5307-2	Strategy2016-2023	2016	Making cyber threat infomation easily available
601	U.K.	5308-1	Strategy2016-2023	2016	Improving highest classification networks
602	U.K.	5309-1	Strategy2016-2023	2016	Promoting new standards in health & care industries
603	U.K.	5310-1	Strategy2016-2023	2016	Awareness raising in Armed Forces
604	U.K.	5310-2	Strategy2016-2023	2016	Enhancing detection & reaction functions
605	U.K.	5310-2	Strategy2016-2023	2016	Enhancing detection & reaction functions
606	U.K.	5311-1	Strategy2016-2023	2016	Metrics
607	U.K.	5311-1	Strategy2016-2023	2016	Metrics
608	U.K.	5311-1	Strategy2016-2023	2016	Metrics
609	U.K.	5311-1	Strategy2016-2023	2016	Metrics
610	U.K.	5404-1	Strategy2016-2023	2016	Awareness raising of board members
611	U.K.	5404-1	Strategy2016-2023	2016	Awareness raising of board members
612	U.K.	5404-2	Strategy2016-2023	2016	Urging organisations & companies to invest in security
613	U.K.	5404-2	Strategy2016-2023	2016	Urging organisations & companies to invest in security
614	U.K.	5404-2	Strategy2016-2023	2016	Urging organisations & companies to invest in security
615	U.K.	5404-2	Strategy2016-2023	2016	Urging organisations & companies to invest in security
616	U.K.	5404-3	Strategy2016-2023	2016	Urging organisations & companies to excercise incident response
617	U.K.	5404-3	Strategy2016-2023	2016	Urging organisations & companies to excercise incident response
618	U.K.	5404-4	Strategy2016-2023	2016	Cybersecurity in CNI
619	U.K.	5404-4	Strategy2016-2023	2016	Cybersecurity in CNI
620	U.K.	5404-4	Strategy2016-2023	2016	Cybersecurity in CNI
621	U.K.	5404-4	Strategy2016-2023	2016	Cybersecurity in CNI
622	U.K.	5404-4	Strategy2016-2023	2016	Cybersecurity in CNI
623	U.K.	5405-1	Strategy2016-2023	2016	Government to understand cybersecurity levels in CNI
624	U.K.	5405-1	Strategy2016-2023	2016	Government to understand cybersecurity levels in CNI
625	U.K.	5406-1	Strategy2016-2023	2016	Sharing information with CNI
626	U.K.	5406-2	Strategy2016-2023	2016	Setting a new standard by collaborating with industries & academia
627	U.K.	5406-2	Strategy2016-2023	2016	Setting a new standard by collaborating with industries & academia
628	U.K.	5406-3	Strategy2016-2023	2016	Encouraging investment in the latest technologies
629	U.K.	5406-3	Strategy2016-2023	2016	Encouraging investment in the latest technologies
630	U.K.	5406-3	Strategy2016-2023	2016	Encouraging investment in the latest technologies
631	U.K.	5406-4	Strategy2016-2023	2016	Exercising with CNI
632	U.K.	5408-1	Strategy2016-2023	2016	Private sector mind-set
633	U.K.	5408-2	Strategy2016-2023	2016	Flexible policies for private sector cybersecurity
634	U.K.	5408-3	Strategy2016-2023	2016	Promoting growth of cybersecurity industries
635	U.K.	5408-3	Strategy2016-2023	2016	Promoting growth of cybersecurity industries
636	U.K.	5408-3	Strategy2016-2023	2016	Promoting growth of cybersecurity industries
637	U.K.	5408-4	Strategy2016-2023	2016	Coordinating international legal framework
638	U.K.	5408-4	Strategy2016-2023	2016	Coordinating international legal framework
639	U.K.	5408-4	Strategy2016-2023	2016	Coordinating international legal framework
640	U.K.	5408-4	Strategy2016-2023	2016	Coordinating international legal framework
641	U.K.	5408-4	Strategy2016-2023	2016	Coordinating international legal framework
642	U.K.	5409-1	Strategy2016-2023	2016	Cybersecurity as a regulation
643	U.K.	5410-1	Strategy2016-2023	2016	Metrics
644	U.K.	5410-1	Strategy2016-2023	2016	Metrics
645	U.K.	5410-1	Strategy2016-2023	2016	Metrics
646	U.K.	5503-1	Strategy2016-2023	2016	Public awareness raising
647	U.K.	5503-1	Strategy2016-2023	2016	Public awareness raising
648	U.K.	5503-1	Strategy2016-2023	2016	Public awareness raising
649	U.K.	5503-1	Strategy2016-2023	2016	Public awareness raising
650	U.K.	5504-1	Strategy2016-2023	2016	Using cybersecurity insurance for corporate awareness raising
651	U.K.	5504-1	Strategy2016-2023	2016	Using cybersecurity insurance for corporate awareness raising
652	U.K.	5505-1	Strategy2016-2023	2016	Making information, education, tools easily available to public & corporates
653	U.K.	5505-1	Strategy2016-2023	2016	Making information, education, tools easily available to public & corporates
654	U.K.	5505-1	Strategy2016-2023	2016	Making information, education, tools easily available to public & corporates
655	U.K.	5505-1	Strategy2016-2023	2016	Making information, education, tools easily available to public & corporates
656	U.K.	5505-2	Strategy2016-2023	2016	Intelligence sharing between government & law enforcement
657	U.K.	5606-1	Strategy2016-2023	2016	Enhancing cooperation in incident response between government & private sector
658	U.K.	5606-1	Strategy2016-2023	2016	Enhancing cooperation in incident response between government & private sector
659	U.K.	5606-2	Strategy2016-2023	2016	Performing inter-sectoral exercise
660	U.K.	5607-1	Strategy2016-2023	2016	Trust between government & private sector
661	U.K.	5608-1	Strategy2016-2023	2016	Automated information sharing system
662	U.K.	5609-1	Strategy2016-2023	2016	Metrics
663	U.K.	5609-1	Strategy2016-2023	2016	Metrics
664	U.K.	5609-1	Strategy2016-2023	2016	Metrics
665	U.K.	6205-1	Strategy2016-2023	2016	Enhancing law enforcement capability in national, regional & local levels

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
211L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	4	Mind-set commonplace in public sector
311L3-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Sector specific programmes of awareness
311L3-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Sector specific programmes of awareness
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
121L2-1	Cybersecurity Policy and	Incident Response	Identification of Incidents	2	Central registry of incidents
311l2-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	2	Cybersecurity information portal
161L3-1	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Redundant communications for key
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
311L3-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Sector specific programmes of awareness
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
311L3-2	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Metrics for effectiveness of awareness raising
331L3-4	Cybersecurity Education,	Framework for Professional	Provision	3	Metrics of effectiveness of cybersecurity
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
512L2-3	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	2	Metrics of compliance of standards & best
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
312L4-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	4	Cybersecurity as common agenda in board
312L3-1	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' understandings of cybersecurity
312L3-2	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Executives' ability to reallocate resources
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
541L3-2	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	Regular review of technical security controls
331L2-4	Cybersecurity Education,	Framework for Professional	Provision	2	Cybersecurity training programmes for non-
332L2-1	Cybersecurity Education,	Framework for Professional	Uptake	2	Cybersecurity trained & certified employees
131L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	3	Vulnerability & asset management of CI
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
133L3-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Cybersecurity oriented risk management in CI
133L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Regular review of impact analysis of CI
133L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Regular review of CI incident response plans
131L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	4	Regular review of CI risk priorities
132L4-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Trust between CI & government
132L2-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Information sharing established between CI &
132L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Ability to adjust of CI protection
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
133L3-4	Cybersecurity Policy and	Critical Infrastructure (CI)	Risk Management and	3	Regular review of resource allocation for CI
141L3-4	Cybersecurity Policy and	Crisis Management	Crisis Management	3	Evaluation of national incident exercise
161L3-3	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Evaluation of national incident exercise
141L3-1	Cybersecurity Policy and	Crisis Management	Crisis Management	3	High-level scenario of national incident
212L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	4	Mind-set commonplace in private sector
411L4-1	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Balance between cybersecurity legal
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
411L4-1	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Balance between cybersecurity legal
411L4-2	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Participation to international cooperation
412L4-3	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	4	Contributing to international digital human
412L4-4	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	4	Contributing to international privacy
416L4-1	Legal and Regulatory	Legal Framework	Intellectual Property	4	Balance between intellectual property & open
411L4-1	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Balance between cybersecurity legal
112L4-1	Cybersecurity Policy and	National Cybersecurity	Organisation	4	Reassignment & reallocation of resources for
131L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	4	Regular review of CI risk priorities
132L4-1	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Ability to adjust of CI protection
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
222L3-3	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Most users can use e-gov securely
223L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-commerce	3	Most users can use e-commerce securely
311L4-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Entire society involved in awareness raising
562L4-1	Standards, Organisations, and	Cybersecurity Marketplace	Cyber Insurance	4	Innovative cybersecurity insurance market
562L4-3	Standards, Organisations, and	Cybersecurity Marketplace	Cyber Insurance	4	Premium discount for secure behaviour
212L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	4	Mind-set commonplace in private sector
213L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	4	Users' mind-set reducing threat
311L4-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Entire society involved in awareness raising
311L4-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Overall threat reduced by awareness raising
432L3-1	Legal and Regulatory	Formal and Informal	Informal Cooperation	3	Established relationship among government,
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
141L2-1	Cybersecurity Policy and	Crisis Management	Crisis Management	2	National incident exercise done
141L3-2	Cybersecurity Policy and	Crisis Management	Crisis Management	3	Trust between participants of national incident
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
141L3-4	Cybersecurity Policy and	Crisis Management	Crisis Management	3	Evaluation of national incident exercise
141L4-4	Cybersecurity Policy and	Crisis Management	Crisis Management	4	National crisis management established
161L3-3	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Evaluation of national incident exercise
421L3-1	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Dedicated investigative resources for

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
666	U.K.	6205-1	Strategy2016-2023	2016	Enhancing law enforcement capability in national, regional & local levels
667	U.K.	6205-2	Strategy2016-2023	2016	Making UK inefficient cybercrime target based on understanding of cybercrime business
668	U.K.	6205-2	Strategy2016-2023	2016	Making UK inefficient cybercrime target based on understanding of cybercrime business
669	U.K.	6205-3	Strategy2016-2023	2016	International juridical partnership
670	U.K.	6205-3	Strategy2016-2023	2016	International juridical partnership
671	U.K.	6205-3	Strategy2016-2023	2016	International juridical partnership
672	U.K.	6205-3	Strategy2016-2023	2016	International juridical partnership
673	U.K.	6205-3	Strategy2016-2023	2016	International juridical partnership
674	U.K.	6205-4	Strategy2016-2023	2016	Discouraging individuals being involved in cybercrime
675	U.K.	6205-4	Strategy2016-2023	2016	Discouraging individuals being involved in cybercrime
676	U.K.	6205-5	Strategy2016-2023	2016	Exchanging intelligence with industry
677	U.K.	6205-5	Strategy2016-2023	2016	Exchanging intelligence with industry
678	U.K.	6205-6	Strategy2016-2023	2016	New 24/7 reporting system
679	U.K.	6205-6	Strategy2016-2023	2016	New 24/7 reporting system
680	U.K.	6205-6	Strategy2016-2023	2016	New 24/7 reporting system
681	U.K.	6205-7	Strategy2016-2023	2016	Reducing vulnerabilities in infrastructures
682	U.K.	6205-7	Strategy2016-2023	2016	Reducing vulnerabilities in infrastructures
683	U.K.	6205-7	Strategy2016-2023	2016	Reducing vulnerabilities in infrastructures
684	U.K.	6205-8	Strategy2016-2023	2016	Making use of stolen credentials difficult in UK
685	U.K.	6205-8	Strategy2016-2023	2016	Making use of stolen credentials difficult in UK
686	U.K.	6206-1	Strategy2016-2023	2016	Metrics
687	U.K.	6206-1	Strategy2016-2023	2016	Metrics
688	U.K.	6206-1	Strategy2016-2023	2016	Metrics
689	U.K.	6206-1	Strategy2016-2023	2016	Metrics
690	U.K.	6303-1	Strategy2016-2023	2016	Applying international law in cyberspace
691	U.K.	6303-1	Strategy2016-2023	2016	Applying international law in cyberspace
692	U.K.	6303-2	Strategy2016-2023	2016	Confidence building
693	U.K.	6303-3	Strategy2016-2023	2016	Enhancing NATO cooperation
694	U.K.	6303-3	Strategy2016-2023	2016	Enhancing NATO cooperation
695	U.K.	6303-4	Strategy2016-2023	2016	Understanding cyber activity of adversaries
696	U.K.	6303-4	Strategy2016-2023	2016	Understanding cyber activity of adversaries
697	U.K.	6303-4	Strategy2016-2023	2016	Understanding cyber activity of adversaries
698	U.K.	6303-5	Strategy2016-2023	2016	Generating all available options
699	U.K.	6303-5	Strategy2016-2023	2016	Generating all available options
700	U.K.	6303-5	Strategy2016-2023	2016	Generating all available options
701	U.K.	6303-6	Strategy2016-2023	2016	Intenational information sharing
702	U.K.	6303-7	Strategy2016-2023	2016	Attributing specific identities
703	U.K.	6304-1	Strategy2016-2023	2016	Metrics
704	U.K.	6403-1	Strategy2016-2023	2016	Enhancing detection of cyber terrorism
705	U.K.	6403-1	Strategy2016-2023	2016	Enhancing detection of cyber terrorism
706	U.K.	6403-1	Strategy2016-2023	2016	Enhancing detection of cyber terrorism
707	U.K.	6403-1	Strategy2016-2023	2016	Enhancing detection of cyber terrorism
708	U.K.	6403-2	Strategy2016-2023	2016	Enhancing investigation of cyber terrorism
709	U.K.	6403-2	Strategy2016-2023	2016	Enhancing investigation of cyber terrorism
710	U.K.	6403-3	Strategy2016-2023	2016	International cooperation
711	U.K.	6403-3	Strategy2016-2023	2016	International cooperation
712	U.K.	6403-3	Strategy2016-2023	2016	International cooperation
713	U.K.	6404-1	Strategy2016-2023	2016	Metrics
714	U.K.	6404-1	Strategy2016-2023	2016	Metrics
715	U.K.	6404-1	Strategy2016-2023	2016	Metrics
716	U.K.	6503-1	Strategy2016-2023	2016	Enhancing development of cyber HR
717	U.K.	6503-1	Strategy2016-2023	2016	Enhancing development of cyber HR
718	U.K.	6503-1	Strategy2016-2023	2016	Enhancing development of cyber HR
719	U.K.	6503-1	Strategy2016-2023	2016	Enhancing development of cyber HR
720	U.K.	6503-2	Strategy2016-2023	2016	Developing offensive cyber capability
721	U.K.	6503-2	Strategy2016-2023	2016	Developing offensive cyber capability
722	U.K.	6503-2	Strategy2016-2023	2016	Developing offensive cyber capability
723	U.K.	6503-2	Strategy2016-2023	2016	Developing offensive cyber capability
724	U.K.	6503-3	Strategy2016-2023	2016	Integrating offensive cyber capability to armed forces
725	U.K.	6503-3	Strategy2016-2023	2016	Integrating offensive cyber capability to armed forces
726	U.K.	6504-1	Strategy2016-2023	2016	Metrics
727	U.K.	6504-1	Strategy2016-2023	2016	Metrics
728	U.K.	6603-1	Strategy2016-2023	2016	Creating new requirement of cryptography
729	U.K.	6603-1	Strategy2016-2023	2016	Creating new requirement of cryptography
730	U.K.	6604-1	Strategy2016-2023	2016	Metrics
731	U.K.	7106-1	Strategy2016-2023	2016	Including cybersecurity into computer science education
732	U.K.	7106-1	Strategy2016-2023	2016	Including cybersecurity into computer science education
733	U.K.	7107-1	Strategy2016-2023	2016	Making clear rolls of government & private sector in cybersecurity training
734	U.K.	7107-1	Strategy2016-2023	2016	Making clear rolls of government & private sector in cybersecurity training
735	U.K.	7107-1	Strategy2016-2023	2016	Making clear rolls of government & private sector in cybersecurity training
736	U.K.	7107-2	Strategy2016-2023	2016	Urging corporate management to train employees
737	U.K.	7107-2	Strategy2016-2023	2016	Urging corporate management to train employees
738	U.K.	7107-3	Strategy2016-2023	2016	More attractive careers of cybersecurity professionals
739	U.K.	7108-1	Strategy2016-2023	2016	Inter-sectoral coordination of education/training

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
422L4-2	Legal and Regulatory	Criminal Justice System	Prosecution	4	Dedicated prosecutorial resources for
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L3-5	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Statistics & analysis of cybercrime
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
421L3-4	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Cross-border investigation of cybercrimes
422L4-1	Legal and Regulatory	Criminal Justice System	Prosecution	4	Prosecution of cross-border cybercrimes
432L3-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	3	Joint international investigation & prosecution
311L4-3	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Entire society involved in awareness raising
311L4-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	4	Overall threat reduced by awareness raising
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
431L2-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	2	Established formal international cooperation
121L2-1	Cybersecurity Policy and	Incident Response	Identification of Incidents	2	Central registry of incidents
241L2-1	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	2	Incident reporting mechanisms established
241L2-2	Cyber Culture and Society	Reporting Mechanisms	Reporting Mechanisms	2	Promotion of incident reporting channels
131L3-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Identification	3	Vulnerability & asset management of CI
521L2-3	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	2	Internet infrastructures compliant to
541L2-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	2	Latest technical controls & patch
411L3-1	Legal and Regulatory	Legal Framework	Legislative Framework for	3	Regular review of cybersecurity legal
415L4-1	Legal and Regulatory	Legal Framework	Consumer Protection	4	Amendment procedures for consumer
417L4-2	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Regular review of substantive cybercrime
418L4-2	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Regular review of procedural cybercrime
421L4-3	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Regular review of investigative capabilities
423L4-2	Legal and Regulatory	Criminal Justice System	Courts	4	Regular review of court system capabilities to
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
111L4-2	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Contributing to international debate of
141L4-2	Cybersecurity Policy and	Crisis Management	Crisis Management	4	National incident exercise contributing to
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
151L3-2	Cybersecurity Policy and	Cyber Defence	Strategy	3	Capturing landscape of national-level threat
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
153L3-2	Cybersecurity Policy and	Cyber Defence	Coordination	3	Strengths & weaknesses of cyber defence
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
151L3-3	Cybersecurity Policy and	Cyber Defence	Strategy	3	Cyber defence strategy meets objectives
151L3-2	Cybersecurity Policy and	Cyber Defence	Strategy	3	Capturing landscape of national-level threat
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
153L2-1	Cybersecurity Policy and	Cyber Defence	Coordination	2	Coordination between CI & defence
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L3-4	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Cross-border investigation of cybercrimes
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
431L3-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	3	Communication channels for international
432L3-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	3	Joint international investigation & prosecution
421L4-3	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Regular review of investigative capabilities
431L4-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	4	Regular review of international cooperation
432L4-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	Adapted international cooperation
321L3-4	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity as focusing area
322L3-2	Cybersecurity Education,	Framework for Education	Administration	3	Adapted budget for cybersecurity education
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
152L4-1	Cybersecurity Policy and	Cyber Defence	Organisation	4	Cross-border response ability
151L3-3	Cybersecurity Policy and	Cyber Defence	Strategy	3	Cyber defence strategy meets objectives
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
551L4-2	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Revision of cryptographic control policies
551L4-1	Standards, Organisations, and	Cryptographic Controls	Cryptographic Controls	4	Regular review of relevance of cryptographic
321L3-2	Cybersecurity Education,	Framework for Education	Provision	3	Mandatory cybersecutity courses for
321L3-4	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity as focusing area
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
332L3-2	Cybersecurity Education,	Framework for Professional	Uptake	3	Coordination of cybersecurity training across
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
332L3-2	Cybersecurity Education,	Framework for Professional	Uptake	3	Coordination of cybersecurity training across
331L4-3	Cybersecurity Education,	Framework for Professional	Provision	4	Incentives for cybersecurity trained workforce
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
740	U.K.	7108-1	Strategy2016-2023	2016	Inter-sectoral coordination of education/training
741	U.K.	7108-1	Strategy2016-2023	2016	Inter-sectoral coordination of education/training
742	U.K.	7109-1	Strategy2016-2023	2016	Specialist education targeting 14-18 years
743	U.K.	7109-1	Strategy2016-2023	2016	Specialist education targeting 14-18 years
744	U.K.	7109-2	Strategy2016-2023	2016	Degree-level apprenticeship in energy, finance & transport
745	U.K.	7109-2	Strategy2016-2023	2016	Degree-level apprenticeship in energy, finance & transport
746	U.K.	7109-3	Strategy2016-2023	2016	Retraining funds
747	U.K.	7109-4	Strategy2016-2023	2016	Supporting high quality post graduate education
748	U.K.	7109-5	Strategy2016-2023	2016	Accredition of teachers
749	U.K.	7109-6	Strategy2016-2023	2016	Identifying excellent organisation
750	U.K.	7109-6	Strategy2016-2023	2016	Identifying excellent organisation
751	U.K.	7109-7	Strategy2016-2023	2016	Defence cyber academy to CoE
752	U.K.	7109-7	Strategy2016-2023	2016	Defence cyber academy to CoE
753	U.K.	7109-7	Strategy2016-2023	2016	Defence cyber academy to CoE
754	U.K.	7109-8	Strategy2016-2023	2016	Collaborating between government, forces, industry & academia
755	U.K.	7109-8	Strategy2016-2023	2016	Collaborating between government, forces, industry & academia
756	U.K.	7109-9	Strategy2016-2023	2016	CyberFirst: nurturing young talent programme
757	U.K.	7109-10	Strategy2016-2023	2016	Cybersecurity education from primary to postgraduate
758	U.K.	7110-1	Strategy2016-2023	2016	Metrics
759	U.K.	7110-1	Strategy2016-2023	2016	Metrics
760	U.K.	7203-1	Strategy2016-2023	2016	Supporting commercialisation of academic innovation
761	U.K.	7203-1	Strategy2016-2023	2016	Supporting commercialisation of academic innovation
762	U.K.	7203-1	Strategy2016-2023	2016	Supporting commercialisation of academic innovation
763	U.K.	7203-1	Strategy2016-2023	2016	Supporting commercialisation of academic innovation
764	U.K.	7203-2	Strategy2016-2023	2016	Establishing innovation centres
765	U.K.	7203-2	Strategy2016-2023	2016	Establishing innovation centres
766	U.K.	7203-2	Strategy2016-2023	2016	Establishing innovation centres
767	U.K.	7203-2	Strategy2016-2023	2016	Establishing innovation centres
768	U.K.	7203-3	Strategy2016-2023	2016	Allocating funds
769	U.K.	7203-3	Strategy2016-2023	2016	Allocating funds
770	U.K.	7203-4	Strategy2016-2023	2016	Providing testing facilities
771	U.K.	7203-5	Strategy2016-2023	2016	Enhancing cooperation between industry & government
772	U.K.	7203-6	Strategy2016-2023	2016	Supporting scaling-up
773	U.K.	7203-7	Strategy2016-2023	2016	Promoting international standards for easier market access
774	U.K.	7203-7	Strategy2016-2023	2016	Promoting international standards for easier market access
775	U.K.	7204-1	Strategy2016-2023	2016	Easier access to government procurement for start-ups
776	U.K.	7204-1	Strategy2016-2023	2016	Easier access to government procurement for start-ups
777	U.K.	7205-1	Strategy2016-2023	2016	Metrics
778	U.K.	7303-1	Strategy2016-2023	2016	Making research funding more effective
779	U.K.	7303-1	Strategy2016-2023	2016	Making research funding more effective
780	U.K.	7303-1	Strategy2016-2023	2016	Making research funding more effective
781	U.K.	7303-1	Strategy2016-2023	2016	Making research funding more effective
782	U.K.	7303-2	Strategy2016-2023	2016	Human & behavioural aspects of cyber science
783	U.K.	7303-2	Strategy2016-2023	2016	Human & behavioural aspects of cyber science
784	U.K.	7303-2	Strategy2016-2023	2016	Human & behavioural aspects of cyber science
785	U.K.	7303-2	Strategy2016-2023	2016	Human & behavioural aspects of cyber science
786	U.K.	7304-1	Strategy2016-2023	2016	Enhancing 'secure-by-default'
787	U.K.	7304-1	Strategy2016-2023	2016	Enhancing 'secure-by-default'
788	U.K.	7305-1	Strategy2016-2023	2016	Establishing Cyber Science and Technology Strategy
789	U.K.	7305-1	Strategy2016-2023	2016	Establishing Cyber Science and Technology Strategy
790	U.K.	7305-1	Strategy2016-2023	2016	Establishing Cyber Science and Technology Strategy
791	U.K.	7305-1	Strategy2016-2023	2016	Establishing Cyber Science and Technology Strategy
792	U.K.	7306-1	Strategy2016-2023	2016	Supporting academic CoE, research institutes & doctral training
793	U.K.	7306-1	Strategy2016-2023	2016	Supporting academic CoE, research institutes & doctral training
794	U.K.	7306-2	Strategy2016-2023	2016	Establishing new research institute
795	U.K.	7306-2	Strategy2016-2023	2016	Establishing new research institute
796	U.K.	7307-1	Strategy2016-2023	2016	Supporting PhD
797	U.K.	7307-1	Strategy2016-2023	2016	Supporting PhD
798	U.K.	7308-1	Strategy2016-2023	2016	Encouraging collaboration between government, industry & academia
799	U.K.	7309-1	Strategy2016-2023	2016	Funding 'grand challenge'
800	U.K.	7309-1	Strategy2016-2023	2016	Funding 'grand challenge'
801	U.K.	7309-1	Strategy2016-2023	2016	Funding 'grand challenge'
802	U.K.	7309-1	Strategy2016-2023	2016	Funding 'grand challenge'
803	U.K.	7310-1	Strategy2016-2023	2016	Metrics
804	U.K.	7403-1	Strategy2016-2023	2016	Promoting inter-disciplinary research for development of horizon scanning
805	U.K.	7403-2	Strategy2016-2023	2016	Integration of cybersecurity & behavioural science
806	U.K.	7403-3	Strategy2016-2023	2016	Monitoring cyber criminal market
807	U.K.	7403-3	Strategy2016-2023	2016	Monitoring cyber criminal market
808	U.K.	7403-4	Strategy2016-2023	2016	Investigating new technologies
809	U.K.	7403-5	Strategy2016-2023	2016	-do-
810	U.K.	7403-6	Strategy2016-2023	2016	Early defence technology
811	U.K.	7403-6	Strategy2016-2023	2016	Early defence technology
812	U.K.	7404-1	Strategy2016-2023	2016	Including cybersecurity into any other research areas for horizon scanning
813	U.K.	7407-1	Strategy2016-2023	2016	Metrics

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
331L4-2	Cybersecurity Education,	Framework for Professional	Provision	4	Coordination between cybersecurity training
321L3-3	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity specific degree
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
332L3-2	Cybersecurity Education,	Framework for Professional	Uptake	3	Coordination of cybersecurity training across
332L3-1	Cybersecurity Education,	Framework for Professional	Uptake	3	Review of cybersecurity training programmes
321L3-3	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity specific degree
321L2-1	Cybersecurity Education,	Framework for Education	Provision	2	Qualification for cybersecurity educators
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
331L4-3	Cybersecurity Education,	Framework for Professional	Provision	4	Incentives for cybersecurity trained workforce
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
331L3-4	Cybersecurity Education,	Framework for Professional	Provision	3	Metrics of effectiveness of cybersecurity
321L4-2	Cybersecurity Education,	Framework for Education	Provision	4	Balance between core components & adaptive
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
321L4-2	Cybersecurity Education,	Framework for Education	Provision	4	Balance between core components & adaptive
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
322L4-3	Cybersecurity Education,	Framework for Education	Administration	4	Cybersecurity education aligned with practical
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L2-2	Cybersecurity Education,	Framework for Education	Administration	2	Budget for research & education for
322L3-2	Cybersecurity Education,	Framework for Education	Administration	3	Adapted budget for cybersecurity education
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L2-2	Cybersecurity Education,	Framework for Education	Administration	2	Budget for research & education for
322L3-2	Cybersecurity Education,	Framework for Education	Administration	3	Adapted budget for cybersecurity education
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
513L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Software	3	Security consideration in all stages
561L3-1	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	3	Security products complied to International
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L2-2	Cybersecurity Education,	Framework for Education	Administration	2	Budget for research & education for
322L3-2	Cybersecurity Education,	Framework for Education	Administration	3	Adapted budget for cybersecurity education
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
322L3-4	Cybersecurity Education,	Framework for Education	Administration	3	CoE in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
321L3-3	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity specific degree
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
322L2-2	Cybersecurity Education,	Framework for Education	Administration	2	Budget for research & education for
322L3-2	Cybersecurity Education,	Framework for Education	Administration	3	Adapted budget for cybersecurity education
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
421L3-2	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Advanced investigative capabilities for
421L4-3	Legal and Regulatory	Criminal Justice System	Law Enforcement	4	Regular review of investigative capabilities
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
122L4-2	Cybersecurity Policy and	Incident Response	Organisation	4	Early warning capability
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
321L4-3	Cybersecurity Education,	Framework for Education	Provision	4	Cybersecurity education adapting to changing

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
814	U.K.	84---1	Strategy2016-2023	2016	Contributing to international debate of international law in cyber space
815	U.K.	84---2	Strategy2016-2023	2016	-do-
816	U.K.	84---3	Strategy2016-2023	2016	-do-
817	U.K.	84---4	Strategy2016-2023	2016	Confidence building measures
818	U.K.	84---5	Strategy2016-2023	2016	Cross-border prosecution
819	U.K.	84---5	Strategy2016-2023	2016	Cross-border prosecution
820	U.K.	84---5	Strategy2016-2023	2016	Cross-border prosecution
821	U.K.	84---6	Strategy2016-2023	2016	Enhancing law enforcement
822	U.K.	84---6	Strategy2016-2023	2016	Enhancing law enforcement
823	U.K.	84---6	Strategy2016-2023	2016	Enhancing law enforcement
824	U.K.	84---7	Strategy2016-2023	2016	Promoting international standards & best practices in emerging technologies
825	U.K.	84---7	Strategy2016-2023	2016	Promoting international standards & best practices in emerging technologies
826	U.K.	84---8	Strategy2016-2023	2016	Cross-border cooperation in capabilities & new technologies
827	U.K.	84---8	Strategy2016-2023	2016	Cross-border cooperation in capabilities & new technologies
828	U.K.	84---8	Strategy2016-2023	2016	Cross-border cooperation in capabilities & new technologies
829	U.K.	84---9	Strategy2016-2023	2016	Assist other countries to build capabilities
830	U.K.	84---9	Strategy2016-2023	2016	Assist other countries to build capabilities
831	U.K.	84---9	Strategy2016-2023	2016	Assist other countries to build capabilities
832	U.K.	84---9	Strategy2016-2023	2016	Assist other countries to build capabilities
833	U.K.	84---9	Strategy2016-2023	2016	Assist other countries to build capabilities
834	U.K.	84---10	Strategy2016-2023	2016	Assist other countries to enhance cybersecurity
835	U.K.	84---10	Strategy2016-2023	2016	Assist other countries to enhance cybersecurity
836	U.K.	84---10	Strategy2016-2023	2016	Assist other countries to enhance cybersecurity
837	U.K.	84---10	Strategy2016-2023	2016	Assist other countries to enhance cybersecurity
838	U.K.	84---10	Strategy2016-2023	2016	Assist other countries to enhance cybersecurity
839	U.K.	84---11	Strategy2016-2023	2016	Enhancing NATO's capability in cyber space
840	U.K.	84---11	Strategy2016-2023	2016	Enhancing NATO's capability in cyber space
841	U.K.	84---12	Strategy2016-2023	2016	-do-
842	U.K.	84---12	Strategy2016-2023	2016	-do-
843	U.K.	84---13	Strategy2016-2023	2016	Contributing international norm development in cyber space
844	U.K.	84---13	Strategy2016-2023	2016	Contributing international norm development in cyber space
845	U.K.	85---1	Strategy2016-2023	2016	Enhancing cooperation with allies
846	U.K.	85---1	Strategy2016-2023	2016	Enhancing cooperation with allies
847	U.K.	85---2	Strategy2016-2023	2016	Contributing to international oganisations
848	U.K.	85---2	Strategy2016-2023	2016	Contributing to international oganisations
849	U.K.	85---3	Strategy2016-2023	2016	Cooperating international non-government actors
850	U.K.	86---1	Strategy2016-2023	2016	Metrics
851	U.K.	86---1	Strategy2016-2023	2016	Metrics
852	U.K.	86---1	Strategy2016-2023	2016	Metrics
853	U.K.	86---1	Strategy2016-2023	2016	Metrics
854	U.S.A.	1.1.1	Commision	2016	The President should direct senior federal executives to launch a private–public initiative,
855	U.S.A.	1.1.1	Commision	2016	The President should direct senior federal executives to launch a private–public initiative,
856	U.S.A.	1.1.1	Commision	2016	The President should direct senior federal executives to launch a private–public initiative,
857	U.S.A.	1.2.1	Commision	2016	The President should create, through executive order, the National Cybersecurity Private–
858	U.S.A.	1.2.1	Commision	2016	The President should create, through executive order, the National Cybersecurity Private–
859	U.S.A.	1.2.1	Commision	2016	The President should create, through executive order, the National Cybersecurity Private–
860	U.S.A.	1.2.1	Commision	2016	The President should create, through executive order, the National Cybersecurity Private–
861	U.S.A.	1.2.2	Commision	2016	The private sector and Administration should launch a joint cybersecurity operation program
862	U.S.A.	1.2.2	Commision	2016	The private sector and Administration should launch a joint cybersecurity operation program
863	U.S.A.	1.2.2	Commision	2016	The private sector and Administration should launch a joint cybersecurity operation program
864	U.S.A.	1.2.2	Commision	2016	The private sector and Administration should launch a joint cybersecurity operation program
865	U.S.A.	1.2.3	Commision	2016	The federal government should provide companies the option to engage proactively and
866	U.S.A.	1.2.3	Commision	2016	The federal government should provide companies the option to engage proactively and
867	U.S.A.	1.2.3	Commision	2016	The federal government should provide companies the option to engage proactively and
868	U.S.A.	1.2.4	Commision	2016	Federal agencies should expand the current implementation of the information-sharing
869	U.S.A.	1.2.4	Commision	2016	Federal agencies should expand the current implementation of the information-sharing
870	U.S.A.	1.2.5	Commision	2016	With the increase in wireless network communications across all organizations, and the
871	U.S.A.	1.2.5	Commision	2016	With the increase in wireless network communications across all organizations, and the
872	U.S.A.	1.3.1	Commision	2016	The next Administration should require that all Internet-based federal government services
873	U.S.A.	1.3.1	Commision	2016	The next Administration should require that all Internet-based federal government services
874	U.S.A.	1.3.1	Commision	2016	The next Administration should require that all Internet-based federal government services
875	U.S.A.	1.3.2	Commision	2016	The next Administration should direct that all federal agencies require the use of strong
876	U.S.A.	1.3.2	Commision	2016	The next Administration should direct that all federal agencies require the use of strong
877	U.S.A.	1.3.3	Commision	2016	The government should serve as a source to validate identity attributes to address online
878	U.S.A.	1.3.3	Commision	2016	The government should serve as a source to validate identity attributes to address online
879	U.S.A.	1.3.4	Commision	2016	The next Administration should convene a body of experts from the private and public
880	U.S.A.	1.3.4	Commision	2016	The next Administration should convene a body of experts from the private and public
881	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
882	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
883	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
884	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
885	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
886	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics
887	U.S.A.	1.4.1	Commision	2016	NIST, in coordination with the NCP3, should establish a Cybersecurity Framework Metrics

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
111L4-2	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Contributing to international debate of
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
422L4-1	Legal and Regulatory	Criminal Justice System	Prosecution	4	Prosecution of cross-border cybercrimes
421L3-3	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Regular training for law enforcement officers
421L3-4	Legal and Regulatory	Criminal Justice System	Law Enforcement	3	Cross-border investigation of cybercrimes
432L3-3	Legal and Regulatory	Formal and Informal	Informal Cooperation	3	Joint international investigation & prosecution
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
161L3-4	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	3	Contribution to international communications'
161L4-2	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	4	Assisting neighbours
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
161L4-2	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	4	Assisting neighbours
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
123L4-2	Cybersecurity Policy and	Incident Response	Coordination	4	Regional coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
124L4-4	Cybersecurity Policy and	Incident Response	Mode of Operation	4	Regional coordination
161L4-2	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	4	Assisting neighbours
141L4-2	Cybersecurity Policy and	Crisis Management	Crisis Management	4	National incident exercise contributing to
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
141L4-2	Cybersecurity Policy and	Crisis Management	Crisis Management	4	National incident exercise contributing to
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
111L4-2	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Contributing to international debate of
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
141L4-2	Cybersecurity Policy and	Crisis Management	Crisis Management	4	National incident exercise contributing to
153L4-2	Cybersecurity Policy and	Cyber Defence	Coordination	4	Intelligence shared with allies
123L3-2	Cybersecurity Policy and	Incident Response	Coordination	3	International coordination
124L3-5	Cybersecurity Policy and	Incident Response	Mode of Operation	3	International coordination
432L4-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	Adapted international cooperation
111L4-1	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Continual revision of strategy
113L4-1	Cybersecurity Policy and	National Cybersecurity	Content	4	Continual revision of strategy
431L4-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	4	Regular review of international cooperation
432L4-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	Adapted international cooperation
152L2-1	Cybersecurity Policy and	Cyber Defence	Organisation	2	Defined responsibility of cyber defence
153L3-1	Cybersecurity Policy and	Cyber Defence	Coordination	3	Analytical capability in cyber defence
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L4-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Trust between CI & government
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
132L4-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	4	Trust between CI & government
132L2-2	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	2	Formal & consistent information sharing
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
123L3-3	Cybersecurity Policy and	Incident Response	Coordination	3	Information sharing across sectors
132L3-3	Cybersecurity Policy and	Critical Infrastructure (CI)	Organisation	3	Supply chain management of CI
521L3-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	3	Investment to new technologies in internet
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
222L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Privacy-by-default in e-gov
222L3-3	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Most users can use e-gov securely
222L4-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	4	Data protection measures of e-gov
211L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set spread in public sector
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
222L3-3	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Most users can use e-gov securely
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
222L3-3	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-government	3	Most users can use e-gov securely
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
121L2-1	Cybersecurity Policy and	Incident Response	Identification of Incidents	2	Central registry of incidents
121L3-1	Cybersecurity Policy and	Incident Response	Identification of Incidents	3	Regular revision of incident registry
211L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Government	3	Mind-set spread in public sector
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
562L2-1	Standards, Organisations, and	Cybersecurity Marketplace	Cyber Insurance	2	Established cybersecurity insurance market

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
888	U.S.A.	1.4.2	Commision	2016	All federal agencies should be required to use the Cybersecurity Framework.
889	U.S.A.	1.4.2	Commision	2016	All federal agencies should be required to use the Cybersecurity Framework.
890	U.S.A.	1.4.3	Commision	2016	Regulatory agencies should harmonize existing and future regulations with the Cybersecurity
891	U.S.A.	1.4.3	Commision	2016	Regulatory agencies should harmonize existing and future regulations with the Cybersecurity
892	U.S.A.	1.4.4	Commision	2016	The private sector should develop conformity assessment programs that are effective and
893	U.S.A.	1.4.4	Commision	2016	The private sector should develop conformity assessment programs that are effective and
894	U.S.A.	1.4.5	Commision	2016	The government should extend additional incentives to companies that have implemented
895	U.S.A.	1.5.1	Commision	2016	The National Institute of Standards and Technology (NIST) should expand its support of
896	U.S.A.	1.5.1	Commision	2016	The National Institute of Standards and Technology (NIST) should expand its support of
897	U.S.A.	1.5.1	Commision	2016	The National Institute of Standards and Technology (NIST) should expand its support of
898	U.S.A.	1.5.2	Commision	2016	DHS and NIST, through the National Cybersecurity Center of Excellence (NCCoE), in
899	U.S.A.	1.5.2	Commision	2016	DHS and NIST, through the National Cybersecurity Center of Excellence (NCCoE), in
900	U.S.A.	1.5.3	Commision	2016	Sector-specific agencies (SSAs) and industry associations and organizations should
901	U.S.A.	1.5.3	Commision	2016	Sector-specific agencies (SSAs) and industry associations and organizations should
902	U.S.A.	2.1.1	Commision	2016	To facilitate the development of secure IoT devices and systems, within 60 days the
903	U.S.A.	2.1.1	Commision	2016	To facilitate the development of secure IoT devices and systems, within 60 days the
904	U.S.A.	2.1.1	Commision	2016	To facilitate the development of secure IoT devices and systems, within 60 days the
905	U.S.A.	2.1.2	Commision	2016	Regulatory agencies should assess whether effective cybersecurity practices and
906	U.S.A.	2.1.2	Commision	2016	Regulatory agencies should assess whether effective cybersecurity practices and
907	U.S.A.	2.1.3	Commision	2016	The Department of Justice should lead an interagency study with the Departments of
908	U.S.A.	2.1.4	Commision	2016	The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should
909	U.S.A.	2.1.4	Commision	2016	The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should
910	U.S.A.	2.1.4	Commision	2016	The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) should
911	U.S.A.	2.2.1	Commision	2016	The Director of the Office of Science and Technology Policy (OSTP) should lead the
912	U.S.A.	2.2.1	Commision	2016	The Director of the Office of Science and Technology Policy (OSTP) should lead the
913	U.S.A.	2.2.2	Commision	2016	The U.S. government should support cybersecurity-focused research into traditionally
914	U.S.A.	2.2.2	Commision	2016	The U.S. government should support cybersecurity-focused research into traditionally
915	U.S.A.	2.2.2	Commision	2016	The U.S. government should support cybersecurity-focused research into traditionally
916	U.S.A.	2.2.2	Commision	2016	The U.S. government should support cybersecurity-focused research into traditionally
917	U.S.A.	3.1.1	Commision	2016	To improve consumers' purchasing decisions, an independent organization should develop
918	U.S.A.	3.1.1	Commision	2016	To improve consumers' purchasing decisions, an independent organization should develop
919	U.S.A.	3.1.1	Commision	2016	To improve consumers' purchasing decisions, an independent organization should develop
920	U.S.A.	3.1.2	Commision	2016	Within the first 100 days of the new Administration, the White House should convene a
921	U.S.A.	3.1.2	Commision	2016	Within the first 100 days of the new Administration, the White House should convene a
922	U.S.A.	3.1.3	Commision	2016	The FTC should convene consumer organizations and industry stakeholders in an initiative
923	U.S.A.	3.1.3	Commision	2016	The FTC should convene consumer organizations and industry stakeholders in an initiative
924	U.S.A.	3.1.3	Commision	2016	The FTC should convene consumer organizations and industry stakeholders in an initiative
925	U.S.A.	3.1.3	Commision	2016	The FTC should convene consumer organizations and industry stakeholders in an initiative
926	U.S.A.	3.1.3	Commision	2016	The FTC should convene consumer organizations and industry stakeholders in an initiative
927	U.S.A.	3.2.1	Commision	2016	The next Administration and Congress should prioritize research on human behavior and
928	U.S.A.	3.2.1	Commision	2016	The next Administration and Congress should prioritize research on human behavior and
929	U.S.A.	3.2.1	Commision	2016	The next Administration and Congress should prioritize research on human behavior and
930	U.S.A.	4.1.1	Commision	2016	The next President should initiate a national cybersecurity workforce program to train
931	U.S.A.	4.1.1	Commision	2016	The next President should initiate a national cybersecurity workforce program to train
932	U.S.A.	4.1.2	Commision	2016	The next President should initiate a national cybersecurity apprenticeship program to train
933	U.S.A.	4.1.2	Commision	2016	The next President should initiate a national cybersecurity apprenticeship program to train
934	U.S.A.	4.1.3	Commision	2016	To better prepare students as individuals and future employees, federal programs supporting
935	U.S.A.	4.1.3	Commision	2016	To better prepare students as individuals and future employees, federal programs supporting
936	U.S.A.	4.1.3	Commision	2016	To better prepare students as individuals and future employees, federal programs supporting
937	U.S.A.	4.1.4	Commision	2016	The federal government should develop a mandatory training program to introduce managers
938	U.S.A.	4.1.4	Commision	2016	The federal government should develop a mandatory training program to introduce managers
939	U.S.A.	4.1.5	Commision	2016	The federal government, SLTT governments, and private-sector organizations should create
940	U.S.A.	4.1.6	Commision	2016	The Office of Personnel Management (OPM) should establish a Presidential Cybersecurity
941	U.S.A.	4.1.7	Commision	2016	NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the
942	U.S.A.	4.1.7	Commision	2016	NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the
943	U.S.A.	4.1.7	Commision	2016	NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the
944	U.S.A.	4.1.7	Commision	2016	NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the
945	U.S.A.	4.1.7	Commision	2016	NIST, the National Science Foundation (NSF), the National Security Agency (NSA), and the
946	U.S.A.	4.1.8	Commision	2016	In order to attract more students to pursue cybersecurity degree programs and enter the
947	U.S.A.	4.1.8	Commision	2016	In order to attract more students to pursue cybersecurity degree programs and enter the
948	U.S.A.	4.1.8	Commision	2016	In order to attract more students to pursue cybersecurity degree programs and enter the
949	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
950	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
951	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
952	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
953	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
954	U.S.A.	5.1.1	Commision	2016	The Administration should establish a program to consolidate all civilian agencies' network
955	U.S.A.	5.2.1	Commision	2016	The Administration should expand on the recently proposed Information Technology
956	U.S.A.	5.2.1	Commision	2016	The Administration should expand on the recently proposed Information Technology
957	U.S.A.	5.2.1	Commision	2016	The Administration should expand on the recently proposed Information Technology
958	U.S.A.	5.2.2	Commision	2016	The General Services Administration (GSA) should lead efforts on integrating technology
959	U.S.A.	5.2.2	Commision	2016	The General Services Administration (GSA) should lead efforts on integrating technology
960	U.S.A.	5.2.2	Commision	2016	The General Services Administration (GSA) should lead efforts on integrating technology
961	U.S.A.	5.3.1	Commision	2016	The Office of Management and Budget (OMB) should require federal agencies to use the

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
411L3-1	Legal and Regulatory	Legal Framework	Legislative Framework for	3	Regular review of cybersecurity legal
411L4-1	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Balance between cybersecurity legal
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
212L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Private Sector	3	Mind-set spread in private sector
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L3-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Risk-based adoption of standards & best
511L4-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Regular review of adoption of standards &
511L4-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Risk-based decision making of compliance
511L4-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Regular review of adoption of standards &
511L4-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Risk-based decision making of compliance
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
511L4-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	4	Regular review of adoption of standards &
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
411L3-1	Legal and Regulatory	Legal Framework	Legislative Framework for	3	Regular review of cybersecurity legal
511L2-1	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Established standards & best practices
511L2-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Standards & best practices widely used
511L2-4	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Promotion of use of standards & best
521L4-1	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of infrastructures
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
411L3-1	Legal and Regulatory	Legal Framework	Legislative Framework for	3	Regular review of cybersecurity legal
521L4-1	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of infrastructures
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
213L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	4	Users' mind-set reducing threat
223L3-2	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-commerce	3	Most users can use e-commerce securely
223L4-1	Cyber Culture and Society	Trust and Confidence on the	User Trust in E-commerce	4	Continuous improvement of e-commerce
311L2-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	2	National programme of awareness raising
311L2-2	Cybersecurity Education,	Awareness Raising	Awareness Raising	2	Consultation with stakeholders in national
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
213L4-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	4	Users' mind-set reducing threat
221L4-1	Cyber Culture and Society	Trust and Confidence on the	User Trust and Confidence on	4	Users can evaluate risk & adjust behaviour
412L4-3	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	4	Contributing to international digital human
412L4-4	Legal and Regulatory	Legal Framework	Privacy, Freedom of Speech &	4	Contributing to international privacy
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
541L3-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	3	User side security controls
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
331L3-2	Cybersecurity Education,	Framework for Professional	Provision	3	Cybersecurity training aligned with national
331L4-3	Cybersecurity Education,	Framework for Professional	Provision	4	Incentives for cybersecurity trained workforce
213L3-1	Cyber Culture and Society	Cybersecurity Mind-set	Users	3	Most users have mind-set
251L2-3	Cyber Culture and Society	Media and Social Media	Media and Social Media	2	Broad discussion on social media security
321L3-5	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity education from primary to post-
311L2-1	Cybersecurity Education,	Awareness Raising	Awareness Raising	2	National programme of awareness raising
312L3-4	Cybersecurity Education,	Awareness Raising	Executive Awareness Raising	3	Mandatory cybersecurity education for
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
331L4-1	Cybersecurity Education,	Framework for Professional	Provision	4	Collaboration between public & private in
321L2-5	Cybersecurity Education,	Framework for Education	Provision	2	Research & development in cybersecurity
321L3-4	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity as focusing area
321L4-1	Cybersecurity Education,	Framework for Education	Provision	4	Internationally forerunning in cybersecurity
322L4-1	Cybersecurity Education,	Framework for Education	Administration	4	International CoE in cybersecurity
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
321L3-3	Cybersecurity Education,	Framework for Education	Provision	3	Cybersecurity specific degree
322L4-2	Cybersecurity Education,	Framework for Education	Administration	4	Cooperation between all stakeholders in
331L4-3	Cybersecurity Education,	Framework for Professional	Provision	4	Incentives for cybersecurity trained workforce
122L3-1	Cybersecurity Policy and	Incident Response	Organisation	3	Formal roles & responsibilities allocated
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
521L4-1	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of infrastructures
521L4-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Optimised cost for internet infrastructures
521L4-3	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of critical technologies
541L4-1	Standards, Organisations, and	Technical Security Controls	Technical Security Controls	4	Continuous assess of technical security
521L4-2	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Optimised cost for internet infrastructures
521L4-3	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Controlled acquisition of critical technologies
521L4-4	Standards, Organisations, and	Internet Infrastructure	Internet Infrastructure	4	Independency & persistence of internet
512L3-1	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Standards & best practices for procurement
512L3-2	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Regular review of procurement
512L3-3	Standards, Organisations, and	Adherence to Standards	Standards in Procurement	3	Wider resource planning in procurement
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best

Appendix J

Ref.	Approaches				
	Nation	National #	Source	Year	Action Item
962	U.S.A.	5.3.2	Commision	2016	In the first 100 days of the Administration, OMB should work with NIST and DHS to clarify
963	U.S.A.	5.3.3	Commision	2016	OMB should integrate cybersecurity metrics with agency performance metrics, review these
964	U.S.A.	5.3.3	Commision	2016	OMB should integrate cybersecurity metrics with agency performance metrics, review these
965	U.S.A.	5.3.3	Commision	2016	OMB should integrate cybersecurity metrics with agency performance metrics, review these
966	U.S.A.	5.4.1	Commision	2016	The President should appoint and empower an Assistant to the President for Cybersecurity,
967	U.S.A.	5.4.1	Commision	2016	The President should appoint and empower an Assistant to the President for Cybersecurity,
968	U.S.A.	5.4.2	Commision	2016	The Administration should clarify OMB's role—and specifically, that of the Federal Chief
969	U.S.A.	5.4.2	Commision	2016	The Administration should clarify OMB's role—and specifically, that of the Federal Chief
970	U.S.A.	5.5.1	Commision	2016	The President should issue a National Cybersecurity Strategy within the first 180 days of his
971	U.S.A.	5.5.1	Commision	2016	The President should issue a National Cybersecurity Strategy within the first 180 days of his
972	U.S.A.	5.5.2	Commision	2016	Congress should consolidate cybersecurity and infrastructure protection functions under the
973	U.S.A.	5.5.2	Commision	2016	Congress should consolidate cybersecurity and infrastructure protection functions under the
974	U.S.A.	5.5.3	Commision	2016	The governors in each state should consider seeking necessary legislative authority and
975	U.S.A.	5.5.3	Commision	2016	The governors in each state should consider seeking necessary legislative authority and
976	U.S.A.	6.1.1	Commision	2016	Within the first 180 days of the next Administration, the President should appoint an
977	U.S.A.	6.1.1	Commision	2016	Within the first 180 days of the next Administration, the President should appoint an
978	U.S.A.	6.1.1	Commision	2016	Within the first 180 days of the next Administration, the President should appoint an
979	U.S.A.	6.1.1	Commision	2016	Within the first 180 days of the next Administration, the President should appoint an
980	U.S.A.	6.1.2	Commision	2016	The federal government should increase its engagement in the international standards arena
981	U.S.A.	6.1.3	Commision	2016	The Department of State should continue its work with like-minded nations to promote
982	U.S.A.	6.1.3	Commision	2016	The Department of State should continue its work with like-minded nations to promote
983	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
984	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
985	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
986	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
987	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
988	U.S.A.	6.1.4	Commision	2016	Congress should provide sufficient resources to the Department of Justice (DOJ) to fully
989	U.S.A.	6.1.5	Commision	2016	NIST and the Department of State should proactively seek international partners to extend
990	U.S.A.	6.1.5	Commision	2016	NIST and the Department of State should proactively seek international partners to extend
991	U.S.A.	6.1.6	Commision	2016	The Department of State, DHS, and other agencies should continue to assist countries with
992	U.S.A.	6.1.6	Commision	2016	The Department of State, DHS, and other agencies should continue to assist countries with
993	U.S.A.	6.1.6	Commision	2016	The Department of State, DHS, and other agencies should continue to assist countries with
994	U.S.A.	6.1.6	Commision	2016	The Department of State, DHS, and other agencies should continue to assist countries with
995	U.S.A.	6.1.6	Commision	2016	The Department of State, DHS, and other agencies should continue to assist countries with

Categorization / Classification					
ID	Category	Subcategory	Capacity area	Level	Requirement (keyword)
112L4-1	Cybersecurity Policy and	National Cybersecurity	Organisation	4	Reassignment & reallocation of resources for
511L2-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of adoption of standards & best
511L2-5	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	2	Metrics of compliance of standards & best
511L3-2	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Resource allocation based on standards
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
152L3-1	Cybersecurity Policy and	Cyber Defence	Organisation	3	Advanced capabilities & situational
122L3-1	Cybersecurity Policy and	Incident Response	Organisation	3	Formal roles & responsibilities allocated
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
111L4-1	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Continual revision of strategy
113L4-1	Cybersecurity Policy and	National Cybersecurity	Content	4	Continual revision of strategy
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
151L3-3	Cybersecurity Policy and	Cyber Defence	Strategy	3	Cyber defence strategy meets objectives
123L3-1	Cybersecurity Policy and	Incident Response	Coordination	3	Subnational / sectorial incident response
123L4-1	Cybersecurity Policy and	Incident Response	Coordination	4	Coordinating all levels / sectors
111L4-2	Cybersecurity Policy and	National Cybersecurity	Strategy Development	4	Contributing to international debate of
113L4-2	Cybersecurity Policy and	National Cybersecurity	Content	4	Contributing to international cooperation
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
153L4-1	Cybersecurity Policy and	Cyber Defence	Coordination	4	Leading international debate about cyber
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
411L4-2	Legal and Regulatory	Legal Framework	Legislative Framework for	4	Participation to international cooperation
417L4-1	Legal and Regulatory	Legal Framework	Substantive Cybercrime	4	Contributing to international cybercrime
418L4-1	Legal and Regulatory	Legal Framework	Procedural Cybercrime	4	Contributing to international cybercrime
431L4-1	Legal and Regulatory	Formal and Informal	Formal Cooperation	4	Regular review of international cooperation
432L4-2	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	Adapted international cooperation
422L4-1	Legal and Regulatory	Criminal Justice System	Prosecution	4	Prosecution of cross-border cybercrimes
311L3-4	Cybersecurity Education,	Awareness Raising	Awareness Raising	3	Contribution to international awareness
511L3-3	Standards, Organisations, and	Adherence to Standards	ICT Security Standards	3	Contributing to international standards
113L4-2	Cybersecurity Policy and	National Cybersecurity	Content	4	Contributing to international cooperation
161L4-2	Cybersecurity Policy and	Communications Redundancy	Communications Redundancy	4	Assisting neighbours
411L4-4	Legal and Regulatory	Legal Framework	Legislative Framework for	4	International and/or regional cooperation of
432L4-4	Legal and Regulatory	Formal and Informal	Informal Cooperation	4	International and/or regional cooperation of
561L4-2	Standards, Organisations, and	Cybersecurity Marketplace	Cybersecurity Technologies	4	Exporting superior security products