Responses to Comments for the draft of "The Cyber/Physical Security Framework"

No.		Affiliation	Place	Comments	Responses to Comments
	1-1	Corporation	Preface	Delete the sentence that starts with "The progress of the networking such as "Connected Industries" will increase..." [Reason] It is hard to relate "more flexible and dynamic supply chain configuration" to "increase the opportunity to create new added value". There is no direct description of the above-mentioned relation in the explanatory documents for the Connected Industries. It is more preferable to delete this sentence to directly connect to and better understand its relation to the need for the cyber security measures, which is described later on. (Reference) "Connected Industries", Tokyo Initiative 2017, Ministry of Economy, Trade and Industry, Oct. 2, 2017	We will revise Preface, including overall structural review, taking into account your comments.
	1-2	Corporation	Ch.1	Change the composition by briefly summarizing the points described in the section 1.1 as an "Overview" and placing it before the section 1.1. [Reason] It is hard to grasp the overall flow, objective, and benefit. Also, the description given in the section 1.1 sounds inconsistent for the most part, with so many leaps in the logical argument. The part "new added value" is emphasized, but it will be easier to understand by also referring to the elements described in the explanatory documents for the Connected Industries, such as "improving productivity" and "solving social challenges". Other opinions regarding minor modification of the contents are given separately in the entries listed below.	We will consider revising the content, including overall structural review, taking into account your comments.
	1-3	Corporation	Ch.1	Change the part "to realize the "Connected Industries" which creates new added value toward "Society5.0" based on various connections." to the expression given below. "to realize the "Connected Industries" for "Society5.0", which creates new added value, improves productivity, and solves social challenges, based on various connections." [Reason] Since creating of new added value is not the sole objective of the Connected Industries, it is better to mention other objectives also to avoid misunderstandings.	We will revise Chapter 1, including overall structural review, taking into account your comments.
	1-4	Corporation	Ch.1	Change the part "the supply chain, which is a series of activities to create added value, mainly for companies, will also change its form" to the expression given below. "the supply chain, which focuses on conventional manufacturing, changes its form to the value chain, which creates new added value." [Reason] It is followed by the phrase "will also change its form", so it will make the point clearer by describing the conventional narrow sense of the term "supply chain" in the first half of the sentence.	We will revise Chapter 1, including overall structural review, taking into account your comments.
	1-5	Corporation	Ch.1	Add the following description about the difference between the conventional supply chain and the Society 5.0-type supply chain. Conventional supply chain: Manufacturing ranging from procurement to production Society 5.0-type supply chain: Value chain including everything from planning to servicing [Reason] The description is confusing since the same term "supply chain" is used for both conventional and Society 5.0-type supply chain. Also, the relationship with the new added value seems weak, since the supply chain mentioned in NIST SP800-161 mainly focuses on the measures that deal with the conventional supply chain, such as malware entering via the supplier of parts and software for the IoT devices. (Reference) U.S. Supply Chain Security Measures (3) Defense Acquisition Studies (Vol. 8, Item 3) Defense Structure Improvement Foundation, Guest researcher, Kyozo Yokoyama https://ssl.bsk-z.or.jp/kakusyu/pdf/26.12sapuraiche-nnhp.pdf	We will revise Chapter 1, including overall structural review, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
1	1-6	Corporation	Ch.3 L1.001～ L1.008 L1.010 L1.013	Change "Cyber Security Management System (CSMS)" to the expression given below. "Cyber Security Management System (CSMS) for Industrial Control Systems" [Reason] The CSMS is for the industrial automation and control systems. Although it is so described in the glossary (2) on page 110, the current expression might give false impression that the CSMS is applicable to a wider range, just like the ISMS.	We will revise the content to make it easier to understand that control systems are covered, taking into account your comments.
	1-7	Corporation	Ch.3 L1.002	Modify the text "Utilize cyber insurance" in the Japanese document. [Reason] Editorial correction.	We will revise the content as suggested in your comments.
	1-8	Corporation	Ch.3 L2.002	Change "Use of IoT devices which are not going through security considerations." to the expression given below. "The device company considers the security measures as an issue that should be dealt on the user-side network." [Reason] The original expression is written from a user's point of view. This should be written from the point of view of the company providing the devices, since the security by design is an act of the company providing the IoT devices to consider security risks at the planning and designing stage.	We will consider revising the content, taking into account your comments.
	1-9	Corporation	Ch.3 L2.003	Change "considering functional safety" to "considering safety". [Reason] For the IEC standards that underlie the safety standards of many devices, the term "function safety" refers to the part where the safety of a product is assured by the normal operation of the protective and safety functions of the electronic control devices (such as controllers and software). It is not required to adopt function safety if it is possible to maintain the safety (generally meaning that there is no smoke, fire, electric shock, nor injury) of the device using the mechanical protective device. The original expression gives false impression that the device that does not have to depend on function safety is dangerous. (Reference) The definition of "function safety" in JIS C0508-4 (harmonized standard of the IEC 61508-4 standard). 3.1.12 Functional safety Part of the overall safety relating to the EUC and the EUC control system that depends on the correct functioning of the E/E/PE safety-related systems and other risk reduction measures. (EUC: Equipment Under Control, E/E/PE: Electrical/Electronic/Programmable Electronic)	We will consider revising the content, taking into account your comments.
	1-10	Corporation	Ch.3 L2.012	Add the sentence given below after the sentence "Prevent the IoT devices at the site from being infected with malware by conducting virus check on a regular basis (at the time of start-up process)." "The company providing the IoT devices should perform security measures on supply chains so that they will not be infected through the supply chains of parts and software." [Reason] The embedded system does not necessarily use an OS that allows to perform the virus check. In this case, the supply chain for the development through servicing process of the device and software should be used to cover the cyber security measures.	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments. In additions, security considerations in parts/software supply chains are described in L2.001 to L2.004.
	1-11	Corporation	Ch.3 L2.013	Change "False operations of IoT devices." to the expression given below. "False operations of IoT devices due to the vulnerability that was not found during the development phase." [Reason] The original expression does not express the main reason why the security patch is required for the vulnerability measure.	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	1-12	Corporation	Ch.3 L2.015	Modify the text "and review regularly." in the Japanese document. [Reason] Editorial correction.	We will revise the content as suggested in your comments.
	1-13	Corporation	Ch.3 L2.019 L3.021	Change the "Restrict wireless connection through Bluetooth." to the expression given below. "Restrict wireless connection through Bluetooth, wireless LAN, etc." [Reason] It is not necessary to put a special emphasis on Bluetooth alone; the wireless LAN should be treated the same.	We will revise the content, taking into account your comments.
	1-14	Corporation	Ch.3 L2.020	A support is expected for the policies that are currently being addressed by the TTC to promote the demonstration of the home-network topology identifying protocol and the implementation to each IoT device, as an example of a mechanism to centrally manage the operation information of the IoT device. (Name of the standard) (A general incorporated association) The Telecommunication Technology Committee JJ.300.00 Already standardized as the Home-Network Topology Identifying Protocol ITU-T G.9973 [Reason] There are not many examples of a specific protocol that fulfills the requirements of this item, and it is deemed more effective to promote practical and wide-spread utilization of this protocol.	We will use your comments as a reference in advancing cyber security policies in the future.
	2-1	Reseaarch Institute	Overall	To achieve a smart society through cyber physical system, the development of this framework is a significant program that evolves our advanced national industrial technologies and the consistency in our international contribution.	Your comments will be considered as positive feedback on this framework.
	2-2	Reseaarch Institute	Appendix.C	For some of the terms used in this framework, it is considered preferable to avoid unique definitions as much as possible, and follow the international standards and the Japanese Industrial Standards, unless there are any specific reasons. Also, if there are similar terms in the international standards with different definitions, the reason for this difference and definition should be explained in the glossary. This is because it is considered important to avoid confusion in the definition of terms, in order to achieve international harmonization that this framework is aiming for. An example of this is the term "security policy", which appears in Chapter 3, “L1.001 Development of security policies and preparation of the structures”. In "Appendix C: Glossary (29)", the "Security policy" is described as the "Rules that specify the roles, responsibilities, and information sharing methods among own organization and relevant parties". On the other hand, ISO/IEC 27000 describes “2.60 policy” as an “overall intention and direction as formally expressed by management”. Also, a more detailed definition is given in ISO/IEC 27001. The definition varies as such.	We will revise the definitions of the terms using standards published by JIS and ISO/IEC as a reference, taking into account your comments.
	2-3	Reseaarch Institute	Appendix.B	In this framework, this section is assumed to indicate a common security measure for entire industry that is included in the “Society 5.0”. If this is true, then it may be necessary to add some references for the supply chain security, which may have significant impact at least on the nearest business, and for the privacy protection. Specifically, “NIST SP800-171” is given along with “ISO/IEC 27001”, as the standard to be compared in this framework. SP800-171 is a standard that shows the requirements recommended to protect the confidentiality of the CUI (Controlled Unclassified Information), and its target of application is limited. It is considered more suitable to cite “NIST SP800-53” as the standard to be compared, since it is a more general list of control with integrity and availability. Also, if a wide range of supply chains in "Society 5.0" is to be accepted in this framework, it is preferable to cite the standards "ISO/IEC 27036" and "NIST SP800-161" for common products not limited to CUI as the standards to be compared. In addition, it should also refer to GDPR, the General Data Protection Regulation in EU, which is planned to be enforced on May 25, 2018 and is a great concern to the related companies. It will also be beneficial to refer to "NIST SP800-53 Rev.5 (draft)", which includes improvement of privacy.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO/IEC 27036 and NIST SP 800-161, etc. and the relationship with GDPR, we will consider appropriate responses while verifying their content.
	2-4	Reseaarch Institute	Ch.2	Chapter 2 "2.2 Concept of the framework structure" of this framework includes a statement "Connections between companies (conventional supply chains) [First layer]". There is a concern that this term "conventional supply chains" might cause misunderstanding as to what it is pointing out to. There are wide varieties of supply chains already constructed. Change "conventional supply chains" to "traditional supply chains that deal with transaction of things".	We will consider revising the content, including overall structural review, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
2	2-5	Reseaarch Institute	Ch.3 L1.012	"L1.012 Protection of privacy" of the First layer describes the need to reference and support the international principle called "OECD's eight core principles". The "OECD's eight core principles" is already adopted as an idea in Japan, the U.S., and in Europe. It is hard to understand what to do next from this description alone, and therefore, it is deemed insufficient. It is considered preferable if the description is beneficial for the examination of the need to promptly respond to the previously mentioned GDPR, or how to think in which field of industry and under which conditions.	We will use your comments as a reference in advancing further discussions on the framework. In addition, for the relationship with GDPR, we will consider appropriate responses while verifying its content.
	2-6	Reseaarch Institute	Ch.3	It is considered preferable to reexamine each measure item by focusing on the similarity and dependency of its details. This is performed to keep the least required number of measure items. Specific examples include "L2.001", "L2.002", and "L2.003". The details of "■ Key aspects of the measure" and "■ Examples of measures for each element" are similar for these examples of measures. It is considered preferable to have the measures combined together or stated so that the difference of each measure is clear.	We will consider revising the content, including overall structural review such as integrating similar countermeasure items as much as possible, taking into account your comments.
	2-7	Reseaarch Institute	Ch.3	It is considered preferable to limit the range of description of the measure to the range directly associated to the main topic, and also to maintain the consistency of its details. Examples for the range of description: There is a description of the "isolation of network" under "○ Organization" in "L2.020". The isolation of network is one of the requirements for the implementation of the "centralized management", but its relation to the main topic of the measure, the "centralized management", is weak. As for the prevention of unauthorized access via network, it has been listed in "L2.017" and this description seems sufficient. Conversely, if there is a need to describe the requirements for the isolation of network in "L2.020", then it is considered preferable to also describe this need in "■ Key aspects of the measure". Examples for the consistency of the description: The user ID assignment is mentioned under "○ System" in "L2.020". However, there is no corresponding description under "○ Organization" or "○ People". For example, descriptions such as "Define the procedures for using and managing the IoT device" and "Follow the procedures for managing the IoT devices to assign users and user IDs to each device" should be given under "○ Organization", and "Follow the procedures for using the IoT devices to perform user authentication process" should be given under "○ People".	We will consider revising the content, including overall structural review such as revising countermeasures for each component, taking into account your comments.
	2-8	Reseaarch Institute	Ch.3 L3.002 Appendix.B	There are some items under "Subcategory ID" of the standard to be compared that does not match the examples of measures given in Chapter 3. Specifically, "A.7.1.1, A.7.1.2, A.7.3.1" is listed as the ISO/IEC 27001 standard to be compared for "L3.002 Introduction of IoT devices and servers etc. using anti-tampering devices". A.7 of the same standard is about "human resources security", and "A.7.1.1 Screening" states that "Control - Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to ... the perceived risks." There are no measures that correspond to A.7.1.1 in "■ Overview of the measure", "■ Key aspects of the measure", and "■ Examples of measures for each element" of L3.002. On the other hand, there is no description of controls for ISO/IEC 27001 "A.10 Cryptography" in "L3.002 Introduction of IoT devices and servers etc. using anti-tampering devices". Is this not necessary? "Appendix B" is regarded as a mandatory and important information to improve the interoperability with other standards and to achieve international harmonization that this framework is aiming for. Therefore, it is necessary to secure the correctness of the description, and update it to the latest information whenever needed.	We will check Appendix B again and consider revising the content, taking into account your comments.
	2-9	Reseaarch Institute	Overall	SP800-53 of NIST and ISO/IEC 27002 are voluminous specifications. We are aware that there is a limit to manual matching and checking to achieve international harmonization. We expect that the partial mechanization of analysis operation for the standards and specifications, the development of analysis support tools, and the civil utilization support services, etc. are carried out. cf. the development of SCAP and OSCAL in NIST.	We will use your comments as a reference in advancing further discussions on the framework.
	2-10	Reseaarch Institute	Overall	The implementation of the programs to promote the usage and utilization of this framework, such as the publishing of guidelines and best practices and the holding of seminars and conferences are expected. The value of NIST CSF to the society is that it is utilized by the companies of the industry at large, let alone the U.S. government agency, to analyze their own effort in cyber security and to review the security plans for achieving their goals. NIST actively supports the promotion by publishing "NISTIR 8183" for the manufacturing industry, and holding the "Cybersecurity Framework Workshop 2017". For this framework to be a specification referred to and utilized by the domestic or foreign companies of both public and private sectors, a more active implementation is expected for the publishing of supplementary and related documents and the promotion programs.	We will promote the efforts in each industrial sector and hold seminars, etc. toward wide utilization of this framework, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	3-1	Reseaarch Institute	Overall	● Result of analysis for the cost A trial calculation of the budget for a small-to-medium-sized business to configure a system that fulfills the 57 items of the Cyber/Physical Security Framework is performed. * Premises Number of employees: 300 (the maximum number of resources in enterprise scale for a small-to-medium-sized business) Number of IoT devices owned by the company: 600 (based on the calculation of the number of IoT device properties performed by Cisco in 2010, which was 1.8 to 2 per person) It turned out that a total of approx. 690 million yen is required. The details are as follows: L1 (relationship between companies): Approx. 130 million yen L2 (relationship between physical space and cyber space): Approx. 340 million yen L3 (relationship in cyber space): Approx. 220 million yen Total: Approx. 690 million yen In contrast, the cost required to conform to SP800-53 (325 items), which has three times more controls than SP800-171 (110items) that has higher severity than this framework, is regarded as approximately 300 million yen. ● Reasons for increased cost • A similar measure is demanded multiple times on the three layers • The required level is unsatisfactory and it must have a high-performance product deployed • There are implementations that seem to be impossible with the existing technology (such as L3.010, L3.011) We believe that this framework of the Ministry of Economy, Trade and Industry requires reconsideration since it costs twice as much and yet lowers security than NIST SP800-171, which has extremely high possibility to become an international standard and is starting to acquire acknowledgment for its effectiveness not only in the U.S. but also in Europe. We suggest reconsideration by accepting more expert opinions to enhance the cost reduction plan and the security.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-2	Reseaarch Institute	Ch.3	• Access control No control is specified in accordance with the account life cycle. Also, it is inferior to NIST, by only insufficiently providing two types of account type, privileged and not privileged, and not indicating the measures that use minimum privilege and separation of responsibilities.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	3-3	Reseaarch Institute	Ch.3	• Awareness and training An appropriate content must be designed based on each user's responsibility and role, or else it will be inferior to NIST, due to its inability to effectively improve security awareness and consider inside crime.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-4	Reseaarch Institute	Ch.3	• Auditing and accountability The act of auditing is not intended to be utilized for the improvement of security. This is inferior to NIST, since it does not mention about the definition of the security events that are the targets of the audit and the confirmation of their implementation, the analysis and review of the audit record, and in addition, the audit function and the security of the record itself.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-5	Reseaarch Institute	Ch.3	• Configuration management This is a provision for the organization of assets and configuration only, and this is inferior to NIST, since the configuration setting and minimization has not been demanded for the purpose of security enhancement.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-6	Reseaarch Institute	Ch.3	• Identification and authentication This is inferior to NIST, since it demands multi-factor authentication to all users, and might create vulnerable locations in terms of security.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
3	3-7	Reseaarch Institute	Ch.3	• Incident response This is inferior to NIST, since it does not prepare for the actual incident while improving the incident response through training, etc. In addition, it has not been continuously improved using the tracking record at its occurrence.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-8	Reseaarch Institute	Ch.3	• Maintenance The adverse effects of maintenance are not considered at all. The maintenance should be planned beforehand to provide grounds for its normality, and in addition, the effects after the maintenance should be monitored. Also, it is inferior to NIST since it is a protection for multi-factor authentication only, regarding the implementation of remote maintenance, and does not restrict the behavior after passing the authentication.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-9	Reseaarch Institute	Ch.3	• Media protection It is inferior to NIST since it does not protect media comprehensively throughout its life cycle, taking into consideration the storage of media, the access to the stored media, the control of the transportation of the media, and so on.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-10	Reseaarch Institute	Ch.3	• Personal security The measures connected to the personnel events (transfer, resignation) are not fully specified, since there is no general idea of the account life cycle management. This is inferior to NIST since the resignation interview is not specified and therefore, the unconscious or malicious acts cannot be prevented.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	3-11	Reseaarch Institute	Ch.3	• Physical protection Unauthorized physical access cannot be rejected since there is no provision to identify those personnel who are permitted to come into physical contact and to review and approve that list of personnel. The remote site has not been considered. Also, this is inferior to NIST since this is not a comprehensive measure connected with the logical measure.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-12	Reseaarch Institute	Ch.3	• Risk assessment This is inferior to NIST since the result of assessment is not used to improve security, and the effect of security is not considered when applying the patch.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-13	Reseaarch Institute	Ch.3	• Security assessment This is inferior to NIST since there is no flow for reviewing and approving changes and modifications in the security provision itself and no provision for its tamper detection.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	3-14	Reseaarch Institute	Ch.3	• Protection of system and communication This is inferior to NIST since both confidentiality and integrity cannot be protected. This is because there is a possibility that this will become a vulnerable implementation without the specification of the strength for the encryption protection, and also because it has not demanded protection and detection for unintentional communication, and therefore a single checksum specified to protect the integrity is not valid.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	3-15	Reseaarch Institute	Ch.3	• Integrity of system and information A heuristic detection of contaminated or executed malicious code, or a real-time scanning while importing external file is required. This is also inferior to NIST since it has not been connected to any action after the monitoring, such as the data linkage to the team responding to the log collection incident in the system monitoring.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	4-1	Business Group	Overall	This framework is considered to be a representative documentation that industries in Japan refer to, regarding the security measures. It is necessary that the indicated measure is complete. Also, it should show that the requirements of the existing framework will be fully satisfied by covering the requirements of this framework. [Reason] This is because the security measures described cannot verify MECE (Mutually Exclusive and Collectively Exhaustive). For example, the requirements of this framework are mapped for each life cycle at each layer of the target. In addition, it shows that the requirements of the existing framework are satisfied when the requirements of this framework are satisfied. This allows to show that this framework is equivalent to or better than the existing framework. Furthermore, it is considered beneficial to examine the introduction of classification that recalls comprehensiveness, such as the classification that corresponds to the life cycle of products and services, the classification of measures for ISO27001, the classification of Identify/Protect/Detect/Respond/Recover used in the NIST Cyber Security Framework, and so on.	We will consider revising the content, including overall structural review on the classification of security measures, taking into account your comments.
	4-2	Business Group	Ch.2	For each measure of each layer, there are examples for organization, people, component, data, system, and procedure. Please describe the concept of extracting these examples of measures before Chapter 3. [Reason] Because the description is made concretely, it will be easier to come up with specific examples not listed. One cannot determine if those with higher priorities are appropriately selected.	We will use your comments as a reference in revising the content.
	4-3	Business Group	Ch.2	Please describe the concept of the configuration that includes organization, people, component, data, system, and procedure items for each measure of each layer, before Chapter 3. [Reason] Generally, the reader varies if the target of security application changes among the organizations, systems, or devices. IEC 62443 uses different document for each organization, system, and device, and for each reader. On the other hand, this document includes all application target for each individual measure. For example, in the first half of this document, it may be possible to result in a simple configuration that defines who to read where, by creating a table with a vertical axis of organization, people, component, data, system, and procedure, and a horizontal axis of life cycle, and then by examining the idea of listing the chapters and sections to refer to in that table. Note, however, that the organization, people, and procedure may be appropriate with a classification different from the life cycle.	We will use your comments as a reference in revising the content.

No.		Affiliation	Place	Comments	Responses to Comments
4	4-4	Business Group	Appendix.B	Those items that does not correspond to any international standard and those that are only described in this document must be specified, and their reasons must be stated. [Reason] If the personnel who implemented the measure is already supporting the items of the international standard, then if this document is mapped with the international standard, it is possible to easily determine whether an additional measure is required or not using this document. In addition, mapping with the international standard is required to explain what this document is focusing on and the unique Japanese measures to the world. For example, a supplementary document of NIST SP800-171 describes the mappings with the NIST Cyber Security Framework subcategories. It also describes a part of items missing from the NIST Cyber Security Framework as "committed to confidentiality". By mapping to all requirements or all measures given, for example, in one of the existing major international standards, it will be obvious what this document is focusing on by clearly stating the reason for not mentioning about the items in this document, if there are any. Or, if there are any items that are only mentioned in this document, point it out and describe it to the world as a measure that Japan has uniquely focused on.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make careful adjustments such as adding descriptions where responses to international standards, etc. are lacking, taking into account your comments. In addition, for the items described only in this framework, some differences may have been caused by clearly describing the cyber and physical transcription functions and safety management of data in this framework. We intend to correct this by clearly stating the need for measures, etc.
	4-5	Business Group	Ch.4	Please clearly state the position of Chapter 4. Specifically, specify how Chapter 4 relates to Chapters 2 and 3. [Reason] Chapter 4 does not refer to the three-layer structure, and uses different terms for six application targets/elements (organization, people, component, data, procedure, and system). A description of the position of this chapter must be stated. This chapter also refers to the security, which may overlap with Chapter 3. It seems to show its awareness of the supply chain security in Figure 8, but it does not explicitly show the typical configuration such as supplier, manufacturer, and consumer, so this is also not identifiable. To notify that the security of the organizations and products is guaranteed by a specialized agency, and that a mechanism to refer to this certificate is required, then it is necessary to clearly describe this mechanism and specify how this relates to the previous chapter.	We will consider revising the content, including overall structural review, taking into account your comments.
	4-6	Business Group	Ch.2	What does "each company" mean in "(1) Expected effects in each company utilizing this framework" [Reason] There is no definition of "company" in this text. The classification of target company may be needed.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	4-7	Business Group	Ch.3 L2.003	Reconsideration may be necessary for the statement "L2.003 Introduction of IoT devices considering functional safety". Also, the definition of "safety" should be specified. [Reason] The risks assumed in this item might be misunderstood that it holds true for almost all current states. For IoT devices, specify the conditions/premises that require function safety, and should add statements to limit the IoT devices that require countermeasures.	We will consider revising the content, taking into account your comments.
	4-8	Business Group	Ch.3	"3. The Cyber/Physical Security Measures" does not have the provisions for procurement requirements. [Reason] To configure a secure system, focus must also be given to the supply chain. It is deemed possible to give a hint to the readers by pointing out in this framework the need to include security requirements in the procurement requirements.	We will consider revising the content, including overall structural review on the provisions concerning procurement requirements, taking into account your comments.
	4-9	Business Group	Ch.3 L2.001 Appendix.C	The statement "EDSA certification (IEC 62443-4-2)" is incorrect. Correction is also required in the description given on p.110. [Reason] The EDSA certification is a certification given by ISCI, and based on the EDSA certification specification (EDSA-100 to EDSA-406). This is not equivalent to IEC 62443-4-2.	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	4-10	Business Group	Ch.3 L3.017 L3.018	Why not put the items L3.017 and L3.018 together instead of keeping them separate. [Reason] The targets (communication paths) and measures are the same for the same risk.	Since the coverages of L3.017 and L3.018 vary as the former covers the communication channel between IoT devices and cyber space while the latter covers inside the cyber space, countermeasures items have been divided. We will consider revising the content, however, taking into account your comments.
	4-11	Business Group	Ch.3 L2.017 L2.018 L3.014 L3.016	Please give specific definitions and examples of the term "channel dedicated". [Reason] The expression "channel dedicated" makes the meaning ambiguous. Add description to Appendix C Glossary.	We will consider revising the content such as adding explanations, etc., taking into account your comments.
	4-12	Business Group	Ch.3	Reconsider the structure so that it is clear who implement the measures and who the readers are. [Reason] The reader (who implements measures) is ambiguous. Specifically, the measures implemented by the manufacturer and developer of the device and the user of the device are mixed for the item (L2) of the IoT devices.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	4-13	Business Group	Appendix.C	The description related to the verification and generation of the signature is missing in (16) Public key, (42) Private key. Also, change the description of (35) Anti-tampering devices to "Devices which are hard to manipulate or read out the internal structure and stored data." to refer to the difficulty of reading out the data. [Reason] This might cause misunderstanding among the readers.	We will revise the definitions of the terms using standards published by JIS and ISO/IEC as a reference, taking into account your comments.
	5-1	Individuals	Overall	This statement is written to demand modification and improvement of "the Cyber/Physical Security Framework (Draft)" (from hereinafter referred to as "this FW"), which is drawn and released by the Ministry, by pointing out its inconsistency with NIST CSF and NIST SP800-171, the globally recognized cyber security standards that this FW specifies as the target of mutual recognition, and showing that "international harmonization" that this FW is aiming for will unlikely be achieved. We fear that this FW will obstruct the normal development of our industry, since by using this FW, which is created based on an incorrect recognition of opinions for internationally general cyber security such as NIST CSF, the products and services that are not accepted internationally will be produced, and consequently cause unintentional loss of competitiveness. In addition, we also fear that the vulnerable products and services, which are released under the name of Connected Industries that the Ministry has raised, to take part in the occurrence of security incident, and consequently destroy our national credit. The 5 viewpoints that show clear inconsistency between this FW and SP800-171 is given below. 1. Functional concept for cyber security For SP800-171, a comprehensively functioning resilient protection is allowed against the cyber attacks, based on the concept of 5 functions, “Identify”, “Protect”, “Detect”, “Respond”, and “Recover”, which are presented in the NIST CSF. For the risks and measures listed in this FW, it is hard to say that they are equivalent to SP800-171, since they are a mere collection of measures with such concept missing. Additionally, although the corresponding relationship with NIST CSF and SP800-171 is shown in "Appendix B" of this document, there are missing items to begin with, and since the corresponding relationship with NIST CSF and SP800-171 that is mapped to the same number of measures as this FW is different from the official publication of NIST, it is inconsistent and beyond description even if it is evaluated at the level of category that each item belongs to.	As pointed out in your comments, this framework provides an overall framework for security measures in an industrial society with a cyber-physical integration, and is different from NIST SP 800-171, which summarizes security measures required when private companies share CUI. In addition, we will revise the mapping table in Appendix B, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
5	5-2	Individuals	Ch.2	2. Target of framework protection SP800-171 calls the protection target information a "CUI", and although it targets the information generated inside the government/company or a naturally generated information, the protection target information is restricted to the "Information collected in physical space" and "Edited information through sharing, analyzing and simulating above information". The definition and range of the protection target information is a fundamental element for the evaluation of the information storage location and the validity of protection strength. Therefore, for SP800-171 and this FW that has different definition and range, there is a large difference in their application range of the information, system, organization, and the security strength aimed in the control measure. In addition, although there is a secretariat and a kind of database organized to clarify the target to define the CUI in the U.S., it is unlikely that this is utilized effectively, since the target information is not clear in this FW.	As pointed out in your comments, NIST SP 800-171 whose objective is to protect CUI and this framework are positioned differently. Data, which is one of the six elements relating to the value creation process, is defined as “information collected in physical space” and “edited information through sharing, analyzing and simulating above information”. From the point of view of “protection target information”, however, measures that already exist in the first and the third layers are mainly described. Although it is clearly described in L3.002 that data should be managed by classification based on the characteristics, etc., this framework does not determine the characteristics of data. As for the clarification of the information to be protected, we henceforth intend to make the information specific, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	5-3	Individuals	Ch.2	Also, there is no point in this classification since the target of this described measure and the purpose of use is unknown. This is because the grounds for the classification of three layers given in "2.2 Concept of the framework structure" of this document is not clear, and also because there is no relationship with a model, such as an OSI reference model, that has its validity generally recognized. As for SP800-171, it will not be equivalent since there is neither a three-layer classification method to begin with, nor the control measure solely for IoT devices.	As pointed out in your comments, NIST SP 800-171 whose objective is to protect CUI and this framework are positioned differently. The ground for classification into a three-layer structure is to “consider such a series of activities for new added value”, as described in p.7, and organizing by layer enables dealing with varying relevant stakeholders.
	5-4	Individuals	Ch.2 Ch.3	3. Details of measures for framework It has been determined through the analysis of the details of measures specified in this FW, that it does not match with the details of the items of SP800-171, that are mapped in many items. There are some items that match in content, but they are mostly a partial reference to the request statements of SP800-171 or the control statements of SP800-53 linked to SP800-171, described only in "Examples of measures for each element", and losing the original intention of NIST. As evidence, there are many quotations from NIST used in the items of this FW for completely irrelevant "Overview of the measure" and "Key aspects of the measure". Also, by taking a look at the details and examples of the specified measures in "Three layers of the industrial society where value creation processes unwind" and "Six elements involved in value creation process" in "2.2 Concept of the framework structure", you can see that it is insufficient to show the classification of the details and examples of the measures and that its contents are mixed.	We will consider revising the content, including overall structural review on security measure items, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	6-1	Corporation	Overall	● Result of analysis for the cost A trial calculation of the budget for a small-to-medium-sized business to configure a system that fulfills the 57 items of the Cyber/Physical Security Framework is performed. * Premises Number of employees: 300 (the maximum number of resources in enterprise scale for a small-to-medium-sized business) Number of IoT devices owned by the company: 600 (based on the calculation of the number of IoT device properties performed by Cisco in 2010, which was 1.8 to 2 per person) It turned out that a total of approx. 690 million yen is required. The details are as follows: L1 (relationship between companies): Approx. 130 million yen L2 (relationship between physical space and cyber space): Approx. 340 million yen L3 (relationship in cyber space): Approx. 220 million yen Total: Approx. 690 million yen In contrast, the cost required to conform to SP800-53 (325 items), which has three times more controls than SP800-171 (110items) that has higher severity than this framework, is regarded as approximately 300 million yen. ● Reasons for increased cost • A similar measure is demanded multiple times on the three layers • The required level is unsatisfactory and it must have a high-performance product deployed • There are implementations that seem to be impossible with the existing technology (such as L3.010, L3.011)	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-2	Corporation	Ch.3	• Access control No control is specified in accordance with the account life cycle. Also, it is inferior to NIST, by only insufficiently providing two types of account type, privileged and not privileged, and not indicating the measures that use minimum privilege and separation of responsibilities.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-3	Corporation	Ch.3	• Awareness and training An appropriate content must be designed based on each user's responsibility and role, or else it will be inferior to NIST, due to its inability to effectively improve security awareness and consider inside crime.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	6-4	Corporation	Ch.3	• Auditing and accountability The act of auditing is not intended to be utilized for the improvement of security. This is inferior to NIST, since it does not mention about the definition of the security events that are the targets of the audit and the confirmation of their implementation, the analysis and review of the audit record, and in addition, the audit function and the security of the record itself.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-5	Corporation	Ch.3	• Configuration management This is a provision for the organization of assets and configuration only, and this is inferior to NIST, since the configuration setting and minimization has not been demanded for the purpose of security enhancement.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-6	Corporation	Ch.3	• Identification and authentication This is inferior to NIST, since it demands multi-factor authentication to all users, and might create vulnerable locations in terms of security.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-7	Corporation	Ch.3	• Incident response This is inferior to NIST, since it does not prepare for the actual incident while improving the incident response through training, etc. In addition, it has not been continuously improved using the tracking record at its occurrence.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
6	6-8	Corporation	Ch.3	• Maintenance The adverse effects of maintenance are not considered at all. The maintenance should be planned beforehand to provide grounds for its normality, and in addition, the effects after the maintenance should be monitored. Also, it is inferior to NIST since it is a protection for multi-factor authentication only, regarding the implementation of remote maintenance, and does not restrict the behavior after passing the authentication.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-9	Corporation	Ch.3	• Media protection It is inferior to NIST since it does not protect media comprehensively throughout its life cycle, taking into consideration the storage of media, the access to the stored media, the control of the transportation of the media, and so on.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-10	Corporation	Ch.3	• Personal security The measures connected to the personnel events (transfer, resignation) are not fully specified, since there is no general idea of the account life cycle management. This is inferior to NIST since the resignation interview is not specified and therefore, the unconscious or malicious acts cannot be prevented.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-11	Corporation	Ch.3	• Physical protection Unauthorized physical access cannot be rejected since there is no provision to identify those personnel who are permitted to come into physical contact and to review and approve that list of personnel. The remote site has not been considered. Also, this is inferior to NIST since this is not a comprehensive measure connected with the logical measure.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	6-12	Corporation	Ch.3	• Risk assessment This is inferior to NIST since the result of assessment is not used to improve security, and the effect of security is not considered when applying the patch.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-13	Corporation	Ch.3	• Security assessment This is inferior to NIST since there is no flow for reviewing and approving changes and modifications in the security provision itself and no provision for its tamper detection.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-14	Corporation	Ch.3	• Protection of system and communication This is inferior to NIST since both confidentiality and integrity cannot be protected. This is because there is a possibility that this will become a vulnerable implementation without the specification of the strength for the encryption protection, and also because it has not demanded protection and detection for unintentional communication, and therefore a single checksum specified to protect the integrity is not valid.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	6-15	Corporation	Ch.3	• Integrity of system and information A heuristic detection of contaminated or executed malicious code, or a real-time scanning while importing external file is required. This is also inferior to NIST since it has not been connected to any action after the monitoring, such as the data linkage to the team responding to the log collection incident in the system monitoring.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
7	7-1	Business Group	Ch.1	I support this very epoch-making idea to think of the cyber/physical security framework that is drawn by the Cyber Security Division of the Ministry of Economy, Trade and Industry, in a value chain of services rather than in a conventional asset-based risk management. [Reason] Up to this day, there was a situation where the discussion of conventional mechanism, or the responsibility boundary, for each company preceded, and the cooperation of companies in the field of smart home did not progress. However, in this framework, the observation of cyber security from the operation side enables the cooperation in operation, regardless of the corporation. I think this approach of focusing on the operation is very effective and valid.	Your comments will be considered as positive feedback on this framework.
	7-2	Business Group	Ch.2	I support this approach of accurately identifying the security risks of the activities that create added values extended from the range of activities of the conventional supply chain, by capturing the security measures of the smart home field with the three-layer structure of the value creation process. [Reason] Because the connections with each company are essential to implement smart home and although there is a vulnerability in the smart home system that no administrator exists, this framework supports the cooperation of companies in terms of security measures, and is regarded as a basis to achieve smart life. In addition, for the smart homes achieved in situation connected via network without being divided into the industrial and household fields, it is recognized that the cyber risks that may occur in a household may directly connect to the social infrastructure and affect the industrial field. It is important to discuss the ideal state of cyber security, recognizing that "everything starts from the home life".	Your comments will be considered as positive feedback on this framework.
	7-3	Business Group	Ch.2	Please do promote to achieve international harmonization listed as a feature of this framework under the leadership of the government. In addition, please implement policies that enable social implementation of the framework. [Reason] The international harmonization and specific policies are considered important for the actual operation of the framework. Our association is planning to develop discussion to apply the framework that suits the characteristics of the smart life field. We would also like the government to continue the study of policies that help the industry to grow, such as by providing incentives that presuppose the assurance of security, through the promotion of international cooperation and the observance of the framework.	We will use your comments as a reference in advancing cyber security policies in the future.
8	8-1	Individuals	Overall	Since there may not be many resources in the cyber crime control division of the prefectural police departments, we request to set sentences such as detention and imprisonment, to reduce such crimes.	The objective is of this framework is to provide an overall framework for security measures and it is not intended to provide penalties for cyber crimes.

No.		Affiliation	Place	Comments	Responses to Comments
9	9-1	Corporation	Ch.3 L1.008	The details should be made clear by separately describing the concepts of security incident and security event. Following text shows where it should be corrected to an event. [Reference] A "security event" is a term that indicates an event that occurs individually, such as unauthorized communication. The security incident is determined when a security event occurs, by analyzing the event itself or the status of other security events. [Revision] ■ Overview of the measure · Organize the system to detect events such as unauthorized communication ■ Key aspects of the measure Identify the occurrence of security incident correctly by implementing the procedure to perform analysis of the correlation of the security events and the analysis of the comparison with the information of external threat. (An omission) ○ People · Report the occurrence of a security event to the security administrators and relevant persons involved.	We will consider revising the content, taking into account your comments.
	9-2	Corporation	Ch.3	The second layer is for transferring components from physical to cyber space, which is specifically considered as an IoT device. The third layer is for the space that transfers the data, which is generated by an IoT device and processed as a system, to other devices. This can be understood as a computer and communication system. However, these concepts may appear complicated in 3.2 and 3.3, and it may be hard to understand. The primary cause of this problem lies in the term "IoT device". The term "IoT device" is used to mean both a device that functions to transfer components from physical to cyber space, and an equipment that incorporates this device to perform information communication process. This is making it hard to understand as a whole. I suggest using separate terms like "IoT device" for the second layer and "IoT system" (or "IoT device system") for the third layer. When the term "IoT device" is used for the second layer, then each of "L2 007, L2.016 IoT, L2.017, L2.018, L2.019, L2.020, L2.021" is regarded as a data space, or in other words, the measures for the third layer. On the other hand, L3.002 seems like a problem with the device. Also, L3.001 seems like a measure that should also be applied to the second layer.	We will consider revising the content regarding the definition of IoT devices, taking into account your comments. In addition, as for the content of the second layer, since not only IoT devices themselves but also channels connecting IoT devices and cyber space are considered to be included in the scope, L2.007, L2.016, L2.017, L2.018, L2.019, L2.020, and L2.021 are also considered to be covered. Furthermore, we will consider applying L3.001 and L3.002 to the second layer, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
10	10-1	Individuals	Ch.3 L2.005	From "■ Key aspects of the measure", "regular" should be removed from "Prevent the change in settings and malfunction of IoT devices ... through the strong password setting and password-sharing among service person and devices, regular changes in passwords...". [Reason] The primary reason for this is because in recent years, a negative view (increase in burden for the user, difficulties in safe operation due to the improvement in attack performance, and so on) for regular changing of password has been given in the major change in the concept of identity authentication in the U.S. NIST SP 800-63b, and also in the national NISC and the educational contents provided by the Ministry of Internal Affairs and Communications. The concept of 800-63b is not reflected to NIST SP 800-53 and 171 described in this document, but this will be dealt with by middle of next year. Secondary, although it is unknown specifically what the "password" of an "IoT device" specifies and what it implements, it is different from the login passwords for PCs and Web services used by people. For many IoT devices that are widely spread out, the password for connecting to the control screen is set differently for each device, and if one administrator is to manage these passwords, it would be very time-consuming to change these passwords regularly. Therefore, this request is assumed unacceptable to administrators. Even if a mechanism to ease this operation is introduced, it may cost more or generate new risks, and there seems to be no merit that matches the benefit of prioritizing to observe the regular changing of passwords. Thirdly, there is no description of "regular changes" in the explanation related to the password management in the measures for the first and the third layers and in other measures in the second layer. This is only adopted in this measure, but no reason is given, and therefore is not convincing. From the above, it can be assumed that regular changing of password should not be notified as a versatile measure.	We will revise the content, taking into account your comments.
	11-1	Corporation	Overall	1. Overall picture of the network society It is assumed that it is not a general idea to add this framework because this is a new framework. It may be better to make the overall picture of the network society clear by describing that the IoT devices include everything connected to the network, including not only the drones illustrated in the example, but also the PCs and smart phones. Also, in the society implemented with 5G, more and more cyber attacks affect the entire supply chain, and it will be necessary to secure the safety of the data. For this reason, not only the IoT devices but 5G should also be mentioned.	This framework provides an overall framework for security measures, and the use cases will be considered by taking into account efforts to formulate specific guidelines for each industrial sector, etc.
	11-2	Corporation	Ch.3 L2.018 L3.003 L3.007 L3.015 L3.016	2. Deficiency in this framework (1) Concept of cyber kill chain There is no description presupposing the invasion of attackers, which is the largest issue of the current network operation focusing on the PC. Although the items and contents are arranged to reduce the risk of malicious attacks, it lacks the approach for the case when the attack passes through that measure, or the concept of the cyber kill chain. For example, it only lists the measures based on the attacks by existing malware and information. Because the future trend of the speed of development for the attacker's ability to get armed is increasing, it should be promoted to the supply chain by adding response to unknown malware and gray reputation in L2.018, L3.003, L3.007, L3.015, and L3.016. The concept of cyber kill chain is necessary in this cyber security framework to build an ecosystem to make the whole society safe, by acquiring unknown information at an early point and by having it shared in the society.	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
11	11-3	Corporation	Ch.3 L2.006 L2.007 L2.014 L2.019 L3.017 L3.018 L3.019 L3.021	(2) Strength of security There will be some difference in the security measures to be implemented (process, product, system, and so on) since there is no description of the strength of security. Consequently, there is a gap between the security measures constructed with reference to this framework and the measures required by the global supply chain. It may decrease the global competitiveness of the domestic industry, due to the additional investment and the time required to construct the security measures. For example, as for access control, it is not possible to figured out that a control more detailed than the conventional domestically implemented access control is required. There should be descriptions of privileged IDs and separation of responsibilities in L2.006, L2.007, L2.014, and L2.019. As for the protection of system communication, there are no provisions for the protection and detection after the occurrence of an unintended communication. Because the areas added in the Cybersecurity Management Guidelines V2.0 for detection, response, and recovery are small, the detection and response in case an unintended communication occurs should be described in L3-017~019, L3.021.	This framework summarizes the key points of security measures and provides a framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide multiple concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by making concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues. Privileged ID and separation of responsibilities are mainly described in L3.023. Detection of and response to the occurrence of unintended communications are described in L3.016, L3.017 “Examples of measures for each element”, L3.019, and L3.020 “Key aspects of the measure” and “Examples of measures for each element”.
	11-4	Corporation	Overall	(3) Appropriate information sharing of security incidents It is required to set target time that matches the global defacto standard, since the GDPR (EU General Data Protection Regulation) and the U.S. DoD "DFARS 252.204-7012" has duty to report within 72 hours.	This framework provides an overall framework for security measures, and the obligation to report incidents, etc. will be considered by taking into account efforts to formulate specific guidelines for each industrial sector, etc.
	11-5	Corporation	Ch.3 L3.010 L3.011	3. Implementation techniques · For L3.010 and L3.011, it is difficult to implement, since not everything that has been defined as an IoT device can be implemented.	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.
	11-6	Corporation	Overall	· The use of cloud services also needs to be described, since the small-to-medium-sized businesses are also the security frameworks that can have the measures applied. Note, however, that it is required that a global standard technique is adopted for the cloud service, to achieve international harmonization.	The government plans to initiate discussions on safety assessment of cloud services this fiscal year, and we will consider revising the content of this framework, taking into account the details of the discussions and your comments.
	12-1	Corporation	Overall	I think that there is a need to define "Cyber/Physical Security Measures" to make the area of problem to be discussed clear. It is possible to interpret the title of this draft in various ways, such as "the security measures from both cyber/physical side" or "the security measures for cyber/physical system". Please add description to make the definition more clearer.	We will revise the content, including overall structural review, taking into account your comments.
	12-2	Corporation	Overall	To propose a framework different from the U.S. NIST Cybersecurity Framework, which is starting to establish general evaluation, as a framework for security measure, is it not better of explicitly point out what the feature of this draft compare to the NIST framework is, or how it should be used separately from the NIST framework? U.S. NIST: Cybersecurity Framework - https://www.nist.gov/cyberframework In addition, a white paper "Baseline Security Recommendations for IoT" is published from ENISA for the cyber/physical system security measures. ENISA has organized this white paper after hours of investigation including considerably comprehensive interviews with the specialists in the Europe area. This document, on the other hand, examines the security measures required by analyzing the risks through the modeling of the IoT system architecture and the analysis of the attacked boundaries that exist in each component. Please reconsider this draft, since the viewpoint of modeling (as stated below) and the threat analysis may be insufficient when compared to the white paper of ENISA. ENISA： Baseline Security Recommendations for IoT - https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot	This framework is characterized by an overall model presented to provide a three-layer view of an industrial society with a cyber-physical integration, and is not inconsistent with the US NIST Cybersecurity Framework. We will further advance discussions on the premise of ensuring the consistency. In doing so, we intend to enhance the content, also using other overseas efforts as a reference.

No.		Affiliation	Place	Comments	Responses to Comments
12	12-3	Corporation	Ch.3	The issue indicated in the first layer for the conventional supplier chain mainly questions the policies and systems of separate entities, but this does not seem to go beyond the remarks made to each entity in the past, such as in the IoT Security Guidelines and so on. Also, each item sticks to the discussion of ISMS and CSMS only, but this is a reconfirmation of conventional problem to individual entity, and it seems necessary to refer to the framework for mutual confidence. For example, in NIST IR 8200, refer to the rules such as ISO/IEC 27036:2014, 20243:2015, ISO 28000:2007 to describe Supply Chain Risk Management (SCRM). Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) - https://csrc.nist.gov/publications/detail/nistir/8200/draft In addition, the product evaluation of each IoT products and the conformity to it may be given as specific examples of the concept of mutual confidence. This seems to be already considered by the Ministry of Economy, Trade and Industry in the following investigation, and it may be better to refer to this as well. Investigation of security evaluation for the IoT devices - http://www.meti.go.jp/meti_lib/report/H28FY/000582.pdf With this in mind, although it should be considered in relation to individual standards for each field/product as shown in "Annex D" of NIST IR 8200, it is expected to be able to explain about the range and function of each entity using the same word on the both sides, and it may also be expected to refer to a required mutual confidence other than the "conformity to ISMS and CSMS". Examination in each field is progressing, such as in SAE J3061 for the field of automobile. SAE J3061：Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - https://www.sae.org/standards/content/j3061/	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as NIST IR 8200, etc., we will consider appropriate responses while verifying their content.
	12-4	Corporation	Ch.3	The notes given to the second layer on this document does not seem to be an expected framework, since it is a collection of conventional notes for individual product. These surely do play important roles, but they are already explained in the existing "IoT Security Guidelines" (the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry) or "IoT Safety/Security Development Guidelines" (IPA), and no further description seems to be necessary. These are threats to the society after the implementation of Society 5.0, so these may still change. It may be necessary to perform a threat analysis from the time it is designed to the product and incorporate Secure by Design, for example, in order to prepare for threats that may occur in the value creation process. IoT threat analysis tutorial - https://www.ipa.go.jp/files/000055835.pdf For insufficiency of the third layer, it seems important to be aware of the movements of other countries (ENISA, NIST, etc.) and secure consistency with the authentication system of the U.S. and Europe, to naturally incorporate the concept of incident management into the mechanism because you cannot question the origin of the data in the cyber space at all. In addition, since there is no description of the privacy that may be included in data attribute, it may be necessary to include the discussion of the privacy in IoT, as discussed in ENISA, keeping in mind of the correspondence to GDPR.	For security by design, countermeasure items are provided in L2.002, and we intend to advance discussions in the future, also using documents referred to in your comments as a reference. For ensuring consistency with major certification schemes, we intend to enhance the content in the future, taking into account trends in the EU, etc. The protection of privacy is mentioned in L1.012 and L3.022. We will in any case use your comments as a reference in advancing further discussions on the framework.
	12-5	Corporation	Overall	Because this document targets the supply chain of all industries including small-to-medium-sized businesses, it is preferable to mention the relationship with the existing rules, since it is necessary to keep in mind of the traditional businesses for appropriate consultants to make proposals that match various business categories. For example, in NIST IR 8200, a system is divided into functional features such as the System Security Engineering. The international standard required in each unit will be listed as reference, and if it allows cross comparison, the previously invested standard features may also be utilized.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as NIST IR 8200, etc., we will consider appropriate responses while verifying their content.
	12-6	Corporation	Overall	Each measure should be distinguished since the measures performed by the vendors, end users, and so on are put together under the same subject as a whole.	We will consider revising the content, including overall structural review such as clarifying the subject, taking into account your comments.
	12-7	Corporation	Overall	Maybe it is better to add a list of measures for each layer before the description of individual items, so that each item can be viewed at a glance to easily make forecasts.	We will revise the content, including overall structural review such as adding a list of countermeasure items, taking into account your comments.
	12-8	Corporation	Ch.3	Should there not be a description of item for the viewpoint of privacy data and privacy in L3 and not only in L1?	We will consider revising the content regarding the privacy in L3, taking into account your comments.
	12-9	Corporation	Ch.2	Please give a specific example of how it is "transferred" "accurately" to better understand this idea.	We will use your comments as a reference in revising the content.

No.		Affiliation	Place	Comments	Responses to Comments
	12-10	Corporation	Ch.2	Please give a specific example for "people" "data" and "component" to better understand this idea.	We will use your comments as a reference in revising the content.
	12-11	Corporation	Ch.2	The expression "profiles listing the security measures" appears abrupt. It needs some examples describing the given profiles.	We will use your comments as a reference in revising the content.
	12-12	Corporation	Ch.3 L1.003	It should be added to the document that, for the security incident of one's own company, there is a possibility that it may be interpreted as it should be handled only by one's own company, but generally, this is handled with the support from external vendors and organizations.	When a security incident occurs, it is generally dealt with not only by the company itself but also in cooperation with external organizations. We will therefore consider revising the content, taking into account your comments.
	12-13	Corporation	Ch.3 L1.004	There is a need to consider the verification of support period and measures after the termination of support.	It is considered important in considering maintenance contracts with suppliers. We will therefore consider revising the content of L1.004, taking
	12-14	Corporation	Ch.3 L1.007	A description of physical security assuming theft is wanted. This should be like the contents of L2.008.	Physical security measures against theft such as locking, etc. are described in L2.008 and L3.006. L1.007 only describes about “asset management”.
	12-15	Corporation	Ch.3 L1.008	The description of "outsourcing" should be specified, since it may be interpreted that the detection and analysis of the incident should be performed in one's own company.	We will use your comments as a reference in revising the content.
	12-16	Corporation	Ch.3 L1.013	Consider making modifications as follows. (To show that a wide variety of information needs to be obtained, such as vulnerability information, and not only the incident information) "the latest security incident information from JPCERT/CC" ↓ "the latest security related information from JPCERT/CC"	We will revise the content, taking into account your comments.
	12-17	Corporation	Ch.3 L2.005	Consider making modifications as follows. "Check the initial default setting values before installing the IoT devices." ↓ "Change the initial setting value from default before installing the IoT devices."	We will revise the content, taking into account your comments.
	12-18	Corporation	Ch.3 L2.015	"Restrict the software by … prohibiting these functions (black list)." In this part, the use of black list in the IoT devices means that there is a need for regular update of the black list. Would it not trigger a new risk if there is a failure to update, etc.?	We will revise the content, taking into account your comments.
	12-19	Corporation	Ch.3 L2.018	"Check the existence of any unauthorized connection determined based on by the MAC address of the connection source, installation site of the IoT devices, and access time/frequency." ⇒ This seems inappropriate, since the MAC address of the connection source is no longer available after being connected via the wide area network.	We will consider revising the content such as changing “MAC address” to “IP address”, taking into account your comments.
	12-20	Corporation	Ch.3 L2.019 L3.021	· Although "MAC address filtering" is shown as an example, it can be set arbitrarily, so it is inappropriate as a filtering condition. This is especially true for wireless environment, where interception of communications is possible. This is inappropriate as it is easy to find out the MAC address of a genuine device. · The ESSID may be intercepted also, so setting this will not particularly improve the security. · Why not mention the wide area wireless communication such as LPWA? Above items also applies to "L3.021 Response to unauthorized wireless connection".	We will consider deleting MAC address filtering and ESSID from “Key aspects of the measure” in L2.019 and L3.021, taking into account your comments. In addition, we will consider the impacts of LPWA, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	12-21	Corporation	Ch.3	It is not clear what "service" means from the text. Please provide examples.	We will use your comments as a reference in revising the content.
	12-22	Corporation	Ch.3 L3.003	Some specific examples should be given to specifically understand whether or not the "illegal log-in to the cyber space" means an illegal log-in to the cloud or Web services.	We will use your comments as a reference in revising the content.
	12-23	Corporation	Ch.3 L3.004	When obtaining the data from the sensor using the UDP protocol, it is impossible to identify its sender. It may be implemented with TCP, but implementation like this can be difficult when accommodating a large number of sensors.	We will use your comments as a reference in revising the content.
	12-24	Corporation	Ch.3 L3.005	Authentication using digital certificates and the like may be difficult in case of a small sensor.	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	12-25	Corporation	Ch.3 L3.007	There may be cases where problems may occur due to manipulation, even if the data is within the permissible range.	We will consider revising the content such as adding the case where a sign of falsification is found as an abnormal case, taking into account your comments.
	12-26	Corporation	Ch.3 L3.017	This item and the following items appear to be overlapping. Consider merging these items into one. L3.018 Encrypted communication in the cyber space L3.019 Encryption of sent/received information (data) in the cyber space	Since the coverages of L3.017 and L3.018 vary as the former covers communication channels while the latter covers data, countermeasures items have been divided. We will consider revising the content, however, taking into account your comments.
	12-27	Corporation	Ch.3 L2.005 L2.006 L2.007	Same as above for this item also (These items appear to be overlapping. Consider merging these items into one).	We will consider revising the content such as separating/integrating countermeasure items, taking into account your comments.
	12-28	Corporation	Appendix.B	Provide explanation for the reason of only selecting the four guidelines given in Appendix B as the target of comparison this time, when a large number of reference groups is cited in NIST IR 8200 and the document.	From the Reference Document List in Appendix A, those that are deemed important in considering security measures in the value creation process, in addition to existing supply chain, are selected.
	13-1	Business Group	Overall	There is already a large number of guidelines (*), and it is burdensome for the companies just to reference other guides and the current framework. In each guideline, there are some overlapping descriptions. Organize the relationship so that companies could refer to each guide/framework appropriately to promote security measures. (*) Examples: NISC "Cybersecurity Strategy", NISC "Principles for Formulating of “Safety Standards, Guidelines, etc.” concerning Assurance of Information Security of Critical Infrastructures", the Ministry of Internal Affairs and Communications "IoT Security Comprehensive Measures", the Ministry of Internal Affairs and Communications/the Ministry of Economy, Trade and Industry "IoT Security Guidelines", IPA "Security Development Guide for IoT Development"	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	13-2	Business Group	Ch.1	As an example of the power supply field, there is a description "Power supply control" in the figure, but it is hard to understand how the power supply is controlled in the cyber space. Delete the expression "control" as an expression for the cyber space, since the description "Electric order & control" appears on an arrow that shows connection. Following expressions are suggested. ·Electric power information, etc. ·Information related to electric power supply and demand To match this, on the left side of the figure, an expression "Driving information, etc." is suggested for "Driving information control" Also, the expression "Utility" used in the physical space of the figure may only remind the readers of former general electricity utility. A more extensive expression such as "electric power supplier" is suggested, since various players are entering the electric power industry today, like the Power Producer & Supplier (PPS), aggregators, and retailers.	We will revise the representations of the figure, taking into account your comments.
	13-3	Business Group	Ch.1	A modification of the text to "In the United States, revised versions of the framework (NIST Cybersecurity Framework) were published in April, 2018 which provided the perspective of cyber security measures especially for the critical infrastructure developed by NIST3 in February, 2014." is suggested. [Reason] · The revised version of NIST Cybersecurity Framework Version 1.1 is released on April 16, 2018. （https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework）	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
13	13-4	Business Group	Ch.2	As a feature of this framework, it is stated that "It should include the contents (that) can imagine the balance between the expected risks and the costs for necessary measures and can actually take measures", but it is hard to imagine this balance for the details of specific measures described on and after page 12. For the evaluation and description "in terms of cost", provide or add items to each security measure to deepen understandings and extend the range of utilization.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	13-5	Business Group	Ch.3	There are overlapping descriptions in the overview of the measure, key aspects of the measure, and examples of measures for each element. It may be preferable to think of a different way of organization or description, since there is a concern for the utilization of many overlapping descriptions, especially for the measures related to the IoT devices in L2 and L3.	We will consider revising the content, including overall structural review to make the difference in contents to be implemented for each layer, mainly the second and third layers, easier to understand, taking into account your comments.
	13-6	Business Group	Ch.3 L1.013	A modification of the text from "JPCERT/CC" to "related companies and JPCERT/CC" is suggested, since at the occurrence of a security incident, it is necessary to share the information within the industry and not only in the security authorities such as JPCERT/CC, to make sure that it leads to the prevention of incidents.	We will revise the content, taking into account your comments.
	13-7	Business Group	Ch.3	"IoT devices" There seems to be no need to limit the target to IoT devices to organize "all security measures needed in the industry". (Not all devices that must be ensured security are connected to the Internet, and there are also some devices that does not fall under the definition of IoT devices.) If these devices are specified as "IoT devices", then is it OK to consider those devices other than the IoT devices as not subject to the framework? (If the IoT devices are the target, then it should be so described in "2. Concept of the Cyber/Physical Security Framework" and in other sections.)	This framework also describes security measures for devices, other than IoT devices, connected to the Internet, and we consider that devices other than IoT devices are also within the scope. We will consider revising the content, taking into account your comments.
	13-8	Business Group	Ch.3 L2.001	Instead of giving examples, a modification of the text to "Select IoT devices certified by a third-party or IoT devices confirmed by self-attestation for safe and secure use." is suggested, since there are not many devices that acquired the EDSA certification. In addition, the expression "confirmed by self-attestation" may need to be supplemented, since it is unclear as to whether it is conscious of a particular scheme, or whether it points to the declaration of ensuring the security by the manufactures themselves regardless of the scheme. [Reason] EDSA certified products (http://www.cssc-cl.org/jp/certified_devices/index.html http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices)	We will use your comments as a reference in revising the content.
	13-9	Business Group	Ch.3 L2.011	As for the Key aspects of this measure, since there may be cases where devices are not installed at a remote place, do not make the description sound as if all devices need remote record confirmation function. A modification of the text to "it is preferable to confirm the record of the software start-up process also from remote places" is suggested.	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	14-1	Corporation	Ch.4	· For the cyber/physical security measures, it is important to structure trustworthy (trust) chain of Internet to achieve Society 5.0, and also to build infrastructure that exposes the trust components, data and the organization that provides both, in the supply chain. · From this point, we completely support the need for "trust list" described in "4. Toward Establishing Trust" on page 92 of the Cyber/Physical Security Framework. · In addition to this, we would like to suggest the use of the term "trust" as an idea that shows the level of conformity to the security measures of The Cyber/Physical Security Measures. · For "trust list", there is a need to register a trustworthy company information. There are various methods. For example, the company information may be disclosed by the "Corporate Information" site operated by the country. In addition to this, a "corporate authentication database" may be built, which allows to extract company information, for which the trustworthiness may be evaluated objectively, from the various existing company information that local public organizations and private organizations hold, and select trustworthy suppliers. · It is important that this "trust list" or the "corporate authentication database" is operated by a fair and neutral authority to play their role as the trust anchor. The role-sharing between the public and private sectors and the need for development of relevant legal system should also be widely considered.	Your comments will be considered as positive feedback on this framework. In addition, we will consider revising the content, including overall structural review on building trustworthiness, taking into account your comments.
			Ch.3 L2.004	[Opinions to source page 37] · In view of preventing contamination of counterfeit/illicit products in the supply chain, it is important to describe the method to "... identify the supplier of each IoT device and software" and to "identify and verify the suppliers of each IoT device and software in order to confirm the product authenticity". · Specifically, to specify and identify the suppliers who provide genuine products, the listing and registration of trustworthy suppliers to the company authentication database operated by a trustworthy neutral authority is suggested. · When assigning the IDs to IoT devices and software, a system that combines the IDs with corporate numbers should be structured to associate the numbers with their owners or administrators. [Draft for corrections and additions to source page 37] L2.004 Introducing genuine products into IoT devices ■ Overview of the measure · Introduce the genuine IoT devices that are approved by the device supplier. · Introduce the genuine software that is approved by the software supplier. · List and register the suppliers of genuine IoT devices and software to a trustworthy company database.	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
	14-2	Corporation		■ Key aspects of this measure Use the IoT devices that can be verified as genuine IoT devices to prevent deterioration of operational efficiencies associated with contamination with fraud information (data), occurrence of a malfunction, and frequent machine failure, that are caused by using low quality or low reliability IoT devices, such as counterfeit products. Also, use the software that can be verified as genuine software to prevent malware infection and deterioration of operational efficiencies associated with contamination with incorrect information (data), that are caused by using low quality or low reliability software, such as counterfeit products. · Check the IDs (identifiers) indicating the uniqueness of each and important information (private key, digital certificate) on the IoT devices and software. · Identify and verify the suppliers of each IoT device and software (verification of integrity) in order to confirm that it is a genuine product. · List and register the suppliers of trustworthy IoT devices and software to a trustworthy company database. · Confirm on a regular basis that IoT devices and software are genuine products (during booting up process). ■ Examples of measures for each element ○ Organization · Introduce the concept of system development life cycle with security risks taken into consideration for the design, development, implementation, and modification of functions related to IoT devices. · Identify and list the suppliers of trustworthy IoT devices and software, and register to a trustworthy company database. · Refer to the list of suppliers registered to a trustworthy company database, and identify and verify the suppliers of trustworthy IoT devices and software in order to confirm that it is a genuine product. ○ Component · Check the IDs (identifiers) indicating the uniqueness of each and important information (private key, digital certificate) on the IoT devices and software. · Define the valid date and year (expiry date) according to the use case of IoT devices and software for digital certification. · Supply the IoT devices and software detecting (or preventing) the falsification/leakage during shipments. - For hardware shipments, security courier, protection seal, etc. - For digital transfer, encryption, hash of the entire transmitted data, etc. ○ Procedure · Identify and verify the suppliers of each IoT device and software (verification of integrity) in order to confirm that it is a genuine product. · Confirm on a regular basis that IoT devices and software are genuine products (during booting up process). ○ System · Introduce the concept of system development life cycle with security risks taken into consideration for the design, development, implementation, and modification of functions related to IoT devices. · Identify the supplier of each IoT device and software, and introduce genuine products from the suppliers. · Assign IDs (identifiers) that uniquely identify the IoT device and software. At that time, a system that combines the IDs with corporate numbers should be structured to associate the numbers with their owners or administrators of the IoT devices and software.	

No.		Affiliation	Place	Comments	Responses to Comments
14	14-3	Corporation	Ch.4	[Opinion 1 to source page 92] · The text "security securement … for each element" means that the entity that manages the component is seeking conformity to a separately set security requirement, and "its confirmation" means an act of a trustworthy entity to evaluate this conformity (hereinafter referred to as "conformity assessment"). · If a trustworthy entity and an entity that manages the components are the same, it is self-declaring and the level of "trust" is generally low. The conformity assessment performed by a trusted third party is called "authentication", and its level of "trust" is generally higher than self-declaration. [Draft 1 for corrections and additions to source page 92] 4. Toward Establishing Trust 4. 1． Concept of securing the trust in framework In order to ensure the security of Cyber/Physical System, improve the trust for overall value creation process by setting security requirements and establishing conformance assessment mechanism for the relevant requirement, repeating securement (creation of trustworthiness) and confirmation (confirmation of trustworthiness) of security requirements, and structuring and maintaining trustworthy chain.	We will use your comments as a reference in advancing further discussions on the framework.
	14-4	Corporation	Ch.4	[Opinion 2 to source page 92] · The conformity of components and data to the security requirements needs to be consistently evaluated or confirmed throughout the value creation process, and not just at the point of generation. · Specifically, it is necessary to manage components and data appropriately , so that they are correctly generated and not changed nor manipulated. · For this appropriate management of components and data, a trustworthy list (trust list) is required as reference to show that they are genuine articles. · Naturally, it is essential to secure the trustworthiness of this trust itself. · Incidentally, the validity confirmation of digital certificates such as digital signatures and time stamps for securing the authenticity of digital data may be regarded as an act of reference to a certain type of trustworthy list through the Internet Trust Center. The certification authority and time stamp authority that manages this trustworthy list are audited by a trustworthy certification body. · Thus, it is important to secure (trust anchor) the trustworthiness (trust) of the trust list itself. · The entity that manages the trust list in the global value creation process should especially be a fair and neutral authority. At the same time, from the point of view of business continuity, it is necessary to consider designing of schemes based on the appropriate role-sharing between the public and private sectors, including the financial independence. [Draft 2 for corrections and additions to source page 92] 1. Creation of Trustworthiness (Trust) ● Creation of components/data that satisfy the security requirements ● Verification of target components/data being created with requirements satisfied 2. Confirmation of Trustworthiness (Trust) ● Creation and management of a list (trust list) to certify that target components/data are properly created ● Verification of the trustworthiness of target components/data by referring to the trust list ● Maintain the trust inside and outside of the country by having a fair and neutral authority manage the trust list 3. Structuring and Maintaining of Trustworthy Chain ● Structuring of trustworthy chain through repeated creation and certification of trust (secured traceability) ● Detection of/protection against external attacks to trustworthy chain ● Improvement of resilience against attacks	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
	14-5	Corporation	Ch.3 L3.001	Examples for "○ Organization" of "■ Examples of measures for each element" on page 60 (Ex: ITSMS Certification (ISO/IEC 20000)) · Nature of opinion: Proposed change (Ex: ITSMS Certification (ISO/IEC 20000-1)) [Reason] It is better to list official standard number, since this is a requirement.	We will revise the content, taking into account your comments.
	14-6	Corporation	Appendix.A	Description of ISO/IEC 27002:2013 on page 93 ISO/IEC 27002:2013 (ISO/IEC) (An international standard that defines the specifications for information management system, providing the best practices for information security management.) · Nature of opinion: Proposed change ISO/IEC 27002:2013 (ISO/IEC) (An international standard that defines the criteria for practicing information security controls, providing the best practices for information security measures.) [Reason] It is better to make changes as shown above, since ISO/IEC 27002 is a standard for information security controls and not for management system. (The above proposed change uses the term "international standard" since this term is used in general.)	We will revise the content, taking into account your comments.
	14-7	Corporation	Appendix.A	○ ITSMS Conformity Assessment Scheme (JIPDEC) (A third-party conformity assessment scheme for IT service management consistent with international assessment scheme.) https://isms.jp/isms.html · Nature of opinion: Proposed change ○ ITSMS Conformity Assessment Scheme (JIPDEC) (An internationally consistent third-party assessment scheme for certification based on accreditation of IT service management. The certification criteria are the international standard ISO/IEC 20000-1.) https://isms.jp/itsms.html [Reason] The international consistency becomes clearer by making the certification criteria of this scheme clearer. It will be easier to understand with the URL for the ITSMS scheme given (it seems like the current URL is the one for the ISMS scheme).	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	14-8	Corporation	Appendix.A	The second item on page 95 ○ Cyber Security Management System (CSMS) Conformity Assessment Scheme (JIPDEC) (A scheme describing a third-party certification scheme for cyber security management systems on the Industrial Automation and Control System (IACS) based on the IEC62443-2 international standard.) https://isms.jp/csms.html · Nature of opinion: Proposed change ○ Cyber Security Management System (CSMS) Conformity Assessment Scheme (JIPDEC) (An internationally consistent third-party assessment scheme for certification based on accreditation of cyber security management systems on the Industrial Automation and Control System (IACS). The certification criteria are the CSMS certification criteria (IEC 62443-2-1:2010) created based on the international standard IEC62443-2.) https://isms.jp/csms.html [Reason] It is deemed more appropriate to clearly state that it is a third-party assessment scheme for certification based on accreditation, in order to show its international consistency. It may be easier to understand by specifying the name of the certification criteria.	We will revise the content, taking into account your comments.
	14-9	Corporation	Appendix.A	The fourth item on page 95 ○ Information Security Management System (ISMS) Conformity Assessment Scheme (JIPDEC) (A third-party certification scheme for information security management systems based on the ISO/IEC27001 international standard.) https://isms.jp/isms.html · Nature of opinion: Proposed change ○ Information Security Management System (ISMS) Conformity Assessment Scheme (JIPDEC) (An internationally consistent third-party assessment scheme for certification based on accreditation of information security management systems. The certification criteria are the international standard ISO/IEC 27001.) https://isms.jp/isms.html [Reason] It is deemed more appropriate to clearly state that it is a third-party assessment scheme for certification based on accreditation, in order to show its international consistency.	We will revise the content, taking into account your comments.
	14-10	Corporation	Appendix.C	(26) on page 106 (26) ITSMS (IT Service Management System) Framework designed for IT service providers to maintain or improve their service quality by managing their services based on the PDCA cycle. The requirements to fulfill are defined in the international standard ISO/IEC 20000. · Nature of opinion: Proposed change (26) ITSMS (IT Service Management System) Framework designed for IT service providers to maintain or improve their service quality by managing their services based on the PDCA cycle. The requirements to be fulfilled are defined in the international standard ISO/IEC 20000-1. [Reason] It is better to list official standard number, since this is a requirement.	We will revise the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	14-11	Corporation	Ch.3 L1.012	It is recommended to document this in accordance with the "OECD's eight principles", but it lacks concreteness to show key aspects or examples of this measure, since it only shows basic principles. It is considered better to introduce the international standard "ISO/IEC 29100 (JIS X 9250)" as the key aspects or examples of this measure. In addition, the implementation of PIA (Privacy impact assessment) may be added as a measure, to define the requirements for the security measures. [Reason] The privacy principles shown in ISO/IEC 29100 is primarily derived from existing principles including the OECD's eight principles, indicates the 11 privacy principles, and describes the method to comply with the principles.	We will consider revising the content such as references to designated standards, etc., taking into account your comments.
	14-12	Corporation	Ch.3 L2.005	The description of "regular changes" in password should be removed. In addition, in the initial setting of the IoT devices, the need to change the initial password should be defined as a requirement. [Reason] As a security setting appropriate to the IoT devices, although its premise is not clear, if one account is used by a number of people due to device restriction, then it is possible to reduce the risk by changing the password regularly. However, if it is possible to use individual account, do not demand regular changing of password, for there are risks of password reuse and unsafe password management, and so on. In addition, the problems such as the take-over of IoT devices have occurred by using the initial password as it is without changing. The need to change the initial password should be defined as a requirement.	We will revise the content, taking into account your comments.
15	15-1	Individuals	Ch.1	· The term for "introduction" on the first line of page 1 and on the third line from the bottom on page 2 of the Japanese document needs to be unified.	We will revise the content as suggested in your comments.
	15-2	Individuals	Appendix.A	· The footnote on page 94 is the same as the one on page 89. There seems to be no need to describe it again on page 94.	We will revise the content, taking into account your comments.
	15-3	Individuals	Appendix.C	· (8) on page 104 and (34) on page 107: These terms are not used in this document.	We will revise Appendix C, taking into account your comments.
	15-4	Individuals	Appendix.C	· The term "PDCA cycle" that appears in (26) of page 106 needs to be described in (31) of page 106.	We will consider revising the content, taking into account your comments.
16	16-1	Research Institute	Overall	In a society where Society 5.0, Connected Industries is achieved, the program to build a security framework that deals with diversified and advanced cyber/physical attacks is considered very important. It can be successfully arranged by classifying it into first, second, and third layer for consideration. On the other hand, because the granularity of each item is different, the target of each problem is either too broad or too strict and therefore vague, giving a loose impression as a whole. There is also a concern about its comprehensiveness. It is too involved in the individual problems with unclear criteria for selection, such as the response to brute force attack, the response of security to wireless LAN devices, and the setting of TV conference system as exception, to be specific. This is far beyond the scope of this document, and as a consequence, an excessive number of pages has increased. In addition, on the first layer, it is described that the building and operation of ISMS or CSMS is efficient, but with various choices of existing guidelines, standards, and systems, it would be easier to understand what is different, what is same, what is new, and so on in the current framework by showing the comparison with the existing systems and its position.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	17-1	Business Group	Ch.2	It is described that "It can be utilized at the operation levels of security measures implemented in each company", so in each measure stated below, it is required to show not only the presented measure, but also give specific examples of threat, which can be prevented using that measure. Please also show specific threats linked to each measure, as a valid reference for the users to utilize. [Reason] Because there is no specific example of threat related to the presented measures, it is hard to feel the specific effect of the implementation of the measures, and may not be able to determine the necessity or seriousness of the measure.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
	17-2	Business Group	Ch.2	For the text "It can make us understand the relation between the necessity of security measures and the costs", it should include the contents that the companies configuring the entire supply chain, including the small-to-medium-sized business, can imagine the balance between the expected risks and the costs for necessary measures. Like the [Opinion 17-1], it is necessary to present in the framework both the expected risks and the examples of vulnerability that were actually generated (such as the cases described for JVN and CVE). Also, there are a number of measures corresponding to the strength of the attack. For example, there are measures against take-over of one's own device, measures that does not ill-affect other IoT devices, and so on. There are various measures, including those that should at least be respected and those that are implemented again to make the protection safer. Therefore, for each measure stated below, it will be easier to understand the cost effectiveness by classifying the frameworks to each level of measures. [Reason] It is hard to assume the actual situation of damage with only the current potential risks. To understand its relationship to the cost, it is necessary to show the level of attack that could be protected by the indicated measure.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	17-3	Business Group	Ch.2	It is stated that "It should contribute to cost reduction without lowering the security level", but in the framework descriptions stated below, no measure is presented that could reduce the cost while keeping stable security level. For example, a cost-conscious arrangement is required, like the case where one measure leads to the prevention of multiple vulnerability risk. [Reason] In the measure shown in this framework, there is no method presented that could minimize the cost while keeping security level stable.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	17-4	Business Group	Ch.2	To actually understand the impact of vulnerability risk, it is necessary to present the risk scenario used to indicate this measure. The content should be changed so that it is possible to implement the idea of considering measures based on the risk scenario by grasping the comprehensiveness of the expected risks. [Reason] To actually understand the impact of vulnerability risk, it is necessary to learn about the specific risk scenario.	We will consider revising the content, including overall structural review by also considering risk scenarios and taking into account your comments.
	17-5	Business Group	Ch.2	In Figure 7 related to the framework, you mention “To Protect” and “Identification of security risk” as threat analysis as the previous states for Countermeasures, in Chapter 3, however, only countermeasures are listed, which does not help us find a use for this framework. Are determination of “To Protect” and “Identification of security risk” mentioned in P.11 meant to be performed separately by each company and used only in the stage for developing countermeasures? [Reason] We cannot find a use for this framework as only countermeasures are listed in Chapter 3, which is not consistent with the structure of the framework shown in Figure 7.	This framework provides an overall framework for security measures, and specific application will be considered by taking into account efforts to formulate specific guidelines for each industrial sector, etc.
	17-6	Business Group	Ch.3	In the entire Chapter 3, no relation with “IoT Security Guidelines” developed by IoT Acceleration Consortium is explicitly mentioned. We think that there is a need to mention the relation between the items (guidelines and key points) defined in the Guidelines and countermeasures in this framework. [Reason] This framework can be used as reference for specific countermeasures in accordance with the policies of “IoT Security Guidelines”.	We will use your comments as a reference in revising the content.

No.		Affiliation	Place	Comments	Responses to Comments
17	17-7	Business Group	Ch.3	Did you identify any potential risks and appropriate countermeasures that are described in the guidelines provided in Reference Document List? Let us know the reason for selecting the countermeasures defined in this framework. (Give a clear reason for promoting the countermeasures in this framework, for example, in order to avoid significant damage to society.) [Reason] It is necessary to show the degree of coverage of security measures required for a life-cycle perspective from design through disposal. You need to explicitly state if these security measures are minimum, essential or sufficient.	Various guidelines, etc. were referenced when creating this framework, and the comparison results with ISO/IEC 27001, NIST CSF, and NIST SP 800-171 are provided. For comparisons with other international standards, we will consider appropriate responses while verifying their content. In addition, we will consider revising the content, including the viewpoint of life cycles, taking into account your comments.
	17-8	Business Group	Ch.3	Chapter 3 contains “Risk factor” and “Risk impact” in each countermeasure, and we think that it is necessary to specifically describe which countermeasures should be taken against which threat. For example, it is preferable to mention actual incidents disclosed in the database such as JVN or CVE. (Similar comments [Comment 17-1][Comment 17-2]) [Reason] In order to link each section to specific threats to IoT devices so that these items can be used as useful information to estimate cost-effectiveness of these countermeasures.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-9	Business Group	Ch.3 L2.001	Only “IoT devices certified by the third party” is written in Key aspects of the measure, however, “IoT devices confirmed by self-attestation for safe and secure use” needs to be added. From the perspective of measures for IoT devices in the used market, it is required to mention a system that can ensure no illegal modification to IoT devices purchased by a purchaser. [Reason] In order to maintain consistency with the description in “Overview of the measure”.	We will consider revising the content regarding authentication, taking into account your comments.
	17-10	Business Group	Ch.3 L2.004	For the description in this section, we should consider when using open source software. [Reason] When open source is used, criteria to judge the validity of products are not clear and no identification or authentication of suppliers may be performed.	We will consider revising the content by also considering software reliability and taking into account your comments.
	17-11	Business Group	Ch.3 L2.005	“the initial setting procedure (password etc.) for the IoT devices” and “the suspension of unneeded services” in this section must be observed in any case, however, additional initial settings must be specified by type of product category. Accordingly, in addition to the items that must be observed in any case, different initial settings procedures/methods need to be provided as examples by type of product category. [Reason] These aspects are requirements as minimum manners required for IoT devices with everything connected, however there are additional initial settings procedures/methods that must be observed by type of product category, which need to be mentioned here.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-12	Business Group	Ch.3 L2.006 L2.007	Same as [Comment 17-11], the measures described in this section are for requirements that must be met in any case, in order to apply to actual IoT devices, however, additional initial settings must be specified by type of product category. As specific examples, different initial settings procedures need to be provided by type of product category. [Reason] The measures described in this section are minimum manners required for IoT devices with everything connected, and there are different initial settings by type of product category which must be added to this section.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
	17-13	Business Group	Ch.3 L2.008	In order to apply the measures described in this section to actual IoT devices, additional initial settings must be specified by type of product category. As specific examples, different initial settings procedures need to be provided by type of product category. In addition, as an example of specific measures, logically-closed debug ports need to be mentioned. [Reason] The measures described in this section are minimum manners required for IoT devices with everything connected, and there are different initial settings by type of product category which must be added to this section.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-14	Business Group	Ch.3 L2.009	Partial or full suspension of service activities need to be added as measures described in this section. [Reason] Partial or full suspension of service activities can not only minimize impact on systems and services but also provide an option to ensure the availability from a long-term perspective.	We will consider revising the content, taking into account your comments.
	17-15	Business Group	Ch.3 L2.011 L2.012 L2.013	When the measures described in this section are applied, some restrictions are imposed depending on the scale or function of target IoT devices; therefore different requirements by type of product category need to be explicitly mentioned separating from L2.001-L2.009 in the previous section. [Reason] For example, different specific measures can be taken against malware on a product basis.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-16	Business Group	Ch.3 L2.013	Description on additional methods or procedures to verify the validity of security patches needs to be added to Key aspects of the measure in this section. [Reason] This is a standard way of thinking in the information security field and additional measures are needed.	We will consider revising the content, taking into account your comments.
	17-17	Business Group	Ch.3 L2.014	This section needs to contain security measures on the server side to respond to possible attacks to the remote update server. [Reason] Attacks to the server are also categorized as an actual incident, which should be treated with appropriate measures.	Security measures in cyber space, including servers, are described in the descriptions of the third layer.
	17-18	Business Group	Ch.3 L2.014	This section must describe update methods and measures considering a case where remote update is difficult to implement. [Reason] All IoT devices are not necessarily able to implement remote update function.	We will use your comments as a reference in revising the content.
	17-19	Business Group	Ch.3 L2.015	When the measures described in this section are applied, some restrictions are imposed depending on the scale or function of target IoT devices; therefore different requirements by type of product category need to be explicitly mentioned separating from L2.001-L2.009 in the previous section. [Reason] For example, different specific measures can be taken against malware on a product basis.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-20	Business Group	Ch.3 L2.018	The contents described in Key aspects of the measure of this section are same as the measures using a white list that are described in “L2.006”, “L2.008” and “L2.012”, and measures applicable to any IoT devices and measures necessary on a product basis are better to be described separately for easier understanding. [Reason] With regard to the contents described in “Overview of the measure” of this section, different measures can be taken actually depending on target IoT devices, these are, however, very important key points as minimum requirements, and as mentioned in the above, clear separation of targets and explanation on measures are necessary.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
	17-21	Business Group	Ch.3 L2.019	For the measures described in this section, additional requirements need to be added in order to apply to actual IoT devices by type of product category. As specific examples, different initial settings procedures need to be provided by type of product category. [Reason] The measures described in this section are minimum manners required for IoT devices with everything connected, and there are other requirements by type of product category which must be added to this section.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	17-22	Business Group	Ch.3 L2.020	With regard to Key aspects of the measure in this section, additional measures need to be added in consideration of a possible risk that failure detection from IoT devices is interfered with. [Reason] This is a standard way of thinking in the information security field and additional measures are needed.	We will use your comments as a reference in revising the content.
	17-23	Business Group	Ch.3 L3.001	With regard to Overview of the measure in this section, selection of service suppliers confirmed by self-attestation for safe and secure use needs to be added. [Reason] There are a wide variety of service businesses using IoT devices and an increasing number of service suppliers will appear in the future, which requires an up-to-the-minute update of evaluation requirements; therefore the existing authentication systems are inappropriate. Accordingly, for example, another system is necessary to flexibly confirm the safety of service suppliers by type of product or industry. Evaluation by any third-party organization can be a bottleneck in businesses from the perspective of cost or time; therefore same as “measures through introduction of IoT devices”, it is important to promote the evaluation on the service suppliers side by self-attestation.	We will consider revising the content regarding the use of self-attestation, taking into account your comments.
	17-24	Business Group	Ch.3 L3.001	In Key aspects of the measure, only “the suppliers that provide safety products and services confirmed through security assessments by a third-party organization” is mentioned but “the suppliers that provide safety products and services confirmed by self-attestation” also needs to be added. [Reason] As there is no consistency with “L2.001 Introduction of secure IoT devices” and because of the reason mentioned in [Comment 17-22] in L3.001, the above needs to be added.	We will consider revising the content regarding the use of self-attestation, taking into account your comments.
	17-25	Business Group	Ch.3 L3.001	In Key aspects of the measure, it is mentioned that “Let the third-party organization assess the requirement definitions and design results obtained during the planning/designing stage from the security viewpoint, but “Confirm the safety by self-attestation” needs to be added. [Reason] As there is no consistency with “L2.001 Introduction of secure IoT devices” and because of the reason mentioned in [Comment 17-22] in L3.001, the above needs to be added.	We will consider revising the content regarding the use of self-attestation, taking into account your comments.
	17-26	Business Group	Ch.3 L3.010	With regard to Key aspects of the measure in this section, additional measures need to be added in consideration of a possible risk that failure detection from IoT devices is interfered with. [Reason] This is a standard way of thinking in the information security field and additional measures are needed.	We will use your comments as a reference in revising the content.
	18-1	Corporation	Overall	If the words Cyber x Physical are used, you need to mention the measures in physical environments other than IoT. [Reason] We agree with the idea of this framework, if this is designed for global use, however, the meaning of the word, physical should not be defined specifically in Japanese. If you intend to use the antonym of cyber, for example, RealSpace may be appropriate.	Measures for physical environment are described in the descriptions of the first layer. In addition, the term “physical” is also used in NIST standards, and therefore this framework likewise uses the term “physical”.

No.		Affiliation	Place	Comments	Responses to Comments
	18-2	Corporation	Overall	The relation with existing overseas frameworks (ex. NIST's Framework for Cyber- Physical Systems) must be explicitly stated. [Reason] Taking the purpose of developing this framework into consideration, no statement about the relation with existing frameworks makes no sense.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards, we will consider appropriate responses while verifying their content.
	18-3	Corporation	Overall	The format of this document is not appropriate to be called a "framework". [Reason] Only Chapter 2 contains contents related to the framework, which consists of only six pages not enough to understand the concept or value of the framework. The contents of this framework is poorer than NIST Cybersecurity Framework, ISMS and METI/IPA Cybersecurity Management Guidelines known as security framework, and if the format of this document is called a framework, this should establish a clear concept that can be shared according to the conditions and be enhanced with easy-understanding contents.	This framework was designed to summarize the key points of security measures and provide an overall framework for security measures through making comparisons with NIST CSF, etc.
	18-4	Corporation	Overall	Through the entire document, the two terms "data" and "information" are not used differently. The definition of data saying "Information collected in physical space, and Edited information through sharing, analyzing and simulating above information" provides a feeling of strangeness. [Reason] Taking the intent of applying this framework to the entire society into account, the use of these terms is inappropriate. Originally "data" and "information" are not the same. For example, personal information and personal data are differentiated in Act on the Protection of Personal Information, and in the IoT field, row data from the sensor, and edited and valued information obtained by analyzing these data can have different risks, which should not collectively be treated as "data".	We will consider revising the content by also considering making distinct use of the terms "data" and "information" and taking into account your comments.
	18-5	Corporation	Ch.2	Show us clear evidence if you insist that the use of the framework described in this document can enhance our competitiveness. [Reason] It is not easy to imagine from the draft that this framework can lead to enhancing competitiveness.	As described in p.7, this framework identifies the security risks of the area of activities to create new added values in the "Society 5.0" type supply chain (value creation process) and provides the managing policy. We believe that, by utilizing this framework, each company can provide new services/products created in the "Society 5.0" type supply chain at an appropriate security level with an appropriate level of investment and improve its competitiveness.
	18-6	Corporation	Ch.2	We cannot understand how to use "Examples of measures for each element" described in respective measures at the operation level. The draft of this framework should describe target operations of each measure completely and concretely. [Reason] "Examples of measures for each element" described in respective measures are just examples with low completeness and concreteness, which does not make us imagine their use at the operation level.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	18-7	Corporation	Ch.2	The contents of this framework draft do not help us to imagine costs. [Reason] There is no description in this document which makes us imagine costs. There is also no explanation on reducing costs while maintaining the security level.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.
	18-8	Corporation	Ch.2	A clear explanation should be provided including a reason, evidence and advantage of sorting into three layers. [Reason] Our industries are obviously aiming to make the barrier between the physical and cyber spaces invisible, however separating and categorizing these spaces as a framework put us at a disadvantage including limited design flexibility. If it is necessary from the security perspective, you need to make clear and convincing explanations so as to have the framework used. With regard to the contents of this framework draft, we cannot completely understand the meaning of the definition to describe the comparison between business and physics using 1. connections between companies; 2. physical space; and 3. cyber space. In addition, you use the expression, conventional supply chain, however non-conventional supply chain does not refer to the Second or Third Layer; therefore comparison among three layers may not mean anything.	We will consider revising the content, including overall structural review on the three-layer structure, taking into account your comments.
	18-9	Corporation	Ch.2	A clear explanation should be provided including a reason, evidence and advantage of sorting into six elements. [Reason] From what we can read in this framework draft, we cannot understand the reason for selecting these six elements as a factor of creating added value. The evidence for “a clearly-defined factor of creating added value can be used in the operation” is not satisfactory. The probability of taking security measures by every factor of creating added value is unknown. As no definition is made for six elements, the granularity of the explanation is different depending on examples of security measures. We do not understand what you want to explain us with Figure 6.	We will consider revising the content, including overall structural review on the six elements, taking into account your comments.
	18-10	Corporation	Ch.2	If you want to “provide guidelines”, you must provide enough contents corresponding to guidelines. [Reason] Only “examples” are provided as measures, which are just a sample and do not serve as guidelines.	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
	18-11	Corporation	Ch.2	The following correction needs to be made (no change in the Third Layer): [First Layer] Old: Connections between companies (conventional supply chains) New: Connections in physical space (real world) [Second Layer] Old: Connections between physical space and cyber space New: Node (channel) between physical space and cyber space [Reason] From the contents of this document, it can be interrupted that the three layers in this document show the following: (The First Layer: physical space) Entity: Real world Security measures: Managerial measures (e.g. rule, contract and operational measures) and physical measures in existing IT security (The Third Layer: cyber space) Entity: Virtual space in computer systems or networks Security measures: Logical measures and technical measures in existing IT security (The Second Layer: Node (channel) between the First and Third Layers; information transformation device) Entity: Input (sensor (monitoring device); ICT input device; receiver)/output (actuator; control device; ICT output device; transmitter) to/from physical space seen from cyber space Security measures: So-called IoT security (not enough to ensure the completeness) When we see the description in Chapter 2 by referring to the above, physical space as the First Layer and cyber space as the Third Layer are easy to imagine but the concept of the Second Layer (Connections between physical space and cyber space) seems difficult to understand. Not describing the Second Layer as an independent space like the First or Third Layer but defining as a node (channel) between between the First and Third Layers may be better. In physical space as the First Layer and cyber space as the Third Layer, horizontal “connections” in each layer are described, if the Second Layer, however, is defined as “Connections between physical space and cyber space”, any horizontal “connections” seem to exist in the Second Layer, which brings a feeling of strangeness. Additionally the First Layer is defined as “Connections between companies”, however “Society5.0” is not necessarily limited to companies. B, C and P (Public) may be connected in a network without being clearly differentiated; therefore the use of the term “supply chain” is limited, which may be unnecessary for the definition of the First Layer.	We will consider revising the content, including overall structural review on the three-layer structure, taking into account your comments.
	18-12	Corporation	Ch.2	Six loop arrows in the Second Layer in “Significance of the three-layers-approach” (The same goes for Figures 4 and 7.) Straight up-down arrows like ↑ ↓ need to be used to avoid misunderstanding by readers. [Reason] In the Second Layer in Figure 5, red loop arrows shown as “correct transcription” must indicate “correct transcription” between the upper and lower sides but look like data transfer in the layer.	We will consider revising the content, including overall structural review on the three-layer structure, taking into account your comments.
	18-13	Corporation	Ch.3 L1.001 L1.002 L1.003 L1.009 L1.010 L1.012 L3.022 L3.023	In the current definition, policies and systems must be related to all layers; therefore it is inappropriate to allocate only to the First Layer. [Reason] If the definitions related to rules, operations and technical measures are aiming to be used in the operation, categorization and sorting must be done in accordance with human understanding and movement.	We will consider revising the content, including overall structural review on the classification of security measures, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
18	18-14	Corporation	Ch.3 L1.001 L1.006	You mention “consistent security measures” but policies must be consistent throughout an organization. [Reason] Information handled and environments used vary depending on organization and measures are generally different according to the organization's situation. If different measures under the same conditions are problematic, some descriptions need to be added to compensate for that.	We will consider revising the content, taking into account your comments.
	18-15	Corporation	Ch.3 L1.001	“After established and communicated priorities of organizational missions, objectives, and activities,” should be corrected to “After communicated organizational missions and objectives, and then established priorities of activities,”. [Reason] Generally no priorities are given to missions or objectives.	We will consider revising the content, taking into account your comments.
	18-16	Corporation	Ch.3 L1.001	“Designate….compliance matters” should be changed to something like “Designate….measures for compliance matters” or “Designate….approach to compliance matters”. [Reason] “Designate….compliance matters” makes no sense.	We will consider revising the content, taking into account your comments.
	18-17	Corporation	Ch.3 L1.001	“Especially the privileged persons in charge” should be corrected to “Especially the responsible persons in charge of security measures and privileged persons in charge”. [Reason] Governance problem caused by a responsible person in name only is serious.	We will consider revising the content, taking into account your comments.
	18-18	Corporation	Ch.3 L1.002	The same contents as other sections are provided but some descriptions on “failure of identifying potential threats and lack of knowledge about possible risks” are appropriate for this section. [Reason] Providing the same contents as other sections is unfriendly to readers and the necessity of dividing sections must be shown.	We will consider revising the content, taking into account your comments.
	18-19	Corporation	Ch.3 L1.002	The wording “a person responsible should accompany and watching their behavior” in the fifth line needs to be changed to something like “an appropriate person should accompany to supervise them to stop suspicious behavior”. [Reason] The meaning of “a person responsible” is not clear. As every person who is privileged to enter critical facilities share some of responsibility, “a person responsible” is not limited, and not all privileged persons are a responsible person. aThe expression “watching their behavior” seems slightly excessive.	We will consider revising the content, taking into account your comments.
	18-20	Corporation	Ch.3 L1.002	Modify the text "Utilize cyber insurance" in the 19th line in the Japanese document. [Rationale] Editorial correction.	We will revise the content as suggested in your comments.
	18-21	Corporation	Ch.3 L1.004 L2.001 L2.004 L3.001	You must mention that the selection of suppliers and device installation contracts cannot be divided by layer. [Reason] The contract scope is broad including devices and services (e.g. network and software) and at the same time, many contract types such as purchase and lease are available; therefore it is impossible to use the samples described in this document for measures on a practical level.	Security measures are classified based on the definitions of three layers. We will, however, consider revising the content regarding the classification of security measures concerning the selection of suppliers and contracts for introduction of devices, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	18-22	Corporation	Ch.3 L1.004	The same contents as other sections are provided but some descriptions such as “Entering into no maintenance contract or containing no appropriate security measures in maintenance contract may cause the lack of taking measures” are appropriate for this section. [Reason] Providing the same contents as other sections is unfriendly to readers and the necessity of dividing sections must be shown.	We will consider revising the content, taking into account your comments.
	18-23	Corporation	Ch.3 L1.004	“Procedure of finalizing maintenance contracts with supplies for ..... devices” should be corrected to “Finalize maintenance contracts that ensure the implementation of appropriate security measures with supplies for ..... devices”. [Reason] It may cause misunderstanding that all we have to do is enter into a maintenance contract.	We will consider revising the content, taking into account your comments.
	18-24	Corporation	Ch.3 L1.005	The wording “responding to new security incidents” should be changed to something like “appropriately responding to new threats that are unexpected in existing rules”. [Reason] Even an organization with no standardized PDCA cycle can respond to incidents occurred if necessary.	We will consider revising the content, taking into account your comments.
	18-25	Corporation	Ch.3 L1.005	In the second line, “security incident” should be changed to something like “security threat”. [Reason] “New security incidents” alone can be handled by existing security measures.	We will consider revising the content, taking into account your comments.
	18-26	Corporation	Ch.3 L1.005	“Review the security policy as necessary.” in the second line should be changed to something like “Reflect the guidelines for measures against new threats in the security policy.” [Reason] It is normal to review the security policy as necessary, which provides no good example.	We will consider revising the content, taking into account your comments.
	18-27	Corporation	Ch.3 L1.005	“Monitor the actions of suppliers” in the 13th line should be corrected to “Monitor the communication with suppliers”. [Reason] Monitoring the actions of suppliers the whole time is not realistic and this wording may make suppliers feel bad.	We will consider revising the content, taking into account your comments.
	18-28	Corporation	Ch.3 L1.007	“devices and others that were overlooked when security measures were introduced” needs to be changed to “the lack of taking measures for devices and others”. [Reason] The wording, “devices and others that were overlooked when security measures were introduced” is not appropriate because devices do not overlook themselves.	We will revise the content, taking into account your comments.
	18-29	Corporation	Ch.3 L1.011	As “establish internal controls related to production” does not make sense, it should be changed to something like “establish internal controls related to production records”. [Reason] Some words may be omitted.	We will revise the content, taking into account your comments.
	18-30	Corporation	Ch.3 L1.012	We cannot understand the purpose of picking up only privacy information among a wide variety of information. [Reason] If this framework is targeted to industry, there are many types of information that need to be considered including business confidential information and insider information, and this may cause misunderstanding to readers that only privacy information need to be protected.	As represented by the enforcement of GDPR in this May, privacy protection-related laws and regulations, etc. are expected to continue to be strengthened at a global level, and therefore they are described as important items.

No.		Affiliation	Place	Comments	Responses to Comments
	18-31	Corporation	Ch.3 L1.013	The same contents as other sections are provided but some descriptions such as “in the event of a security incident, necessary information may be unavailable due to lack of regular information sharing related to security measures” are appropriate for this section. [Reason] Providing the same contents as other sections is unfriendly to readers and the necessity of dividing sections must be shown.	We will consider revising the content, taking into account your comments.
	18-32	Corporation	Ch.3 L2.001 L2.002 L2.003 L2.004	With no definition of function safety, these sections make no sense. In addition, if the concept of development life cycle is applied to all introduction-related measures and the same measures are taken, there is no need to separate into different sections. [Reason] If function safety is considered in this document, its requirements must be defined in advance. Appropriate measures vary depending on conditions, but the same measures are defined throughout this framework draft, which may cause misunderstanding to readers.	We will consider revising the content, taking into account your comments.
	18-33	Corporation	Ch.3 L2.005	The description on regular password change should be deleted. [Reason] Different requirements for regular password change according to framework or guideline cause confusion; therefore NISC’s policies should be applied.	We will revise the content, taking into account your comments.
	18-34	Corporation	Ch.3 L2.008	The description, “Implement measures such as locking the areas where IoT devices, introducing entrance/exit control, biometric authentication, surveillance cameras, and inspection on belongings and body weight, etc.” is not appropriate as measures for IoT devices. This may need to be deleted or replaced with another description. [Reason] “Locking and introduction of entrance/exit control and biometric authentication” are measures to protect operational terminal devices used by limited users while “inspection on belongings and body weight” is a measure against taking physical things out by operators, which are both inappropriate for security measures for IoT devices that can be continuously run without operators.	We consider “measures such as locking the areas where IoT devices, introducing entrance/exit control, biometric authentication surveillance cameras, and inspection on belongings and body weight etc.” effective for preventing unauthorized access and IoT devices being taken out.
	18-35	Corporation	Ch.3 L2.009	In this section, the risk that needs to be considered is “potential failures of IoT devices and their communication due to cyber attacks”. [Reason] “Faults and failures” are inevitable for any devices and not appropriate to be treated as a risk factor.	We will consider revising the content, taking into account your comments.
	18-36	Corporation	Ch.3 L2.010	“Misuse disposed IoT devices and manufacture fraud IoT devices.” should be changed to something like “Misuse disposed IoT devices for illicit purposes.” [Reason] “manufacture fraud IoT devices” sounds strange in this context.	We will consider revising the content, taking into account your comments.
	18-37	Corporation	Ch.3 L2.011	“it is required to confirm..... also from remote places.” should be changed to a more moderate expression like “it is desirable to confirm..... also from remote places.” [Reason] It is not realistic to make the remote confirmation function a must for every IoT device, which may be unnecessary depending on purposes or conditions.	We will consider revising the content, taking into account your comments.
	18-38	Corporation	Ch.3 L2.012 L2.014 L2.015 L2.016 L2.017 L2.020	How about adding “(if possible)” at the end of sentences. [Reason] It is not necessarily possible to apply these functions or measure to all IoT devices.	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	18-39	Corporation	Ch.3 L2.013	How about changing “apply them to IoT devices as needed.” to “apply them to IoT devices as needed after verification.” [Reason] It is quite important also for IoT devices to conduct the process to verify that no problem occurs if any patch is applied to our environment.	We will consider revising the content, taking into account your comments.
	18-40	Corporation	Ch.3 L2.021	“Harm the workers by the operations using the IoT devices or damage the devices.” should be changed to something like “IoT devices may not fulfill their original function or may take unintended actions.” [Reason] The effects described here (harm to workers and damage of devices) are improbable for most IoT devices.	We will consider revising the content, taking into account your comments.
	18-41	Corporation	Ch.3 L3.002 L3.006	We do not understand the reason that anti-tampering devices are categorized into the Third Layer. [Reason] Anti-tampering feature is a physical property, which conflicts with the definition of each layer.	Security measures are classified based on the definitions of three layers. We will, however, consider revising the content regarding the classification of security measures, taking into account your comments.
	18-42	Corporation	Ch.3 L3.003	Change “logging in to the system for the privileged user” to “logging in to the system via the network for the privileged user”. [Reason] Two-factor authentication is not always available when the administrator logs in to the console directly connected to the server, which is less considered because of the recent and general use of cloud.	We will consider revising the content, taking into account your comments.
	18-43	Corporation	Ch.3 L3.004 L3.005	Identification and authentication do not need to be considered separately as measures. In addition, authentication and identification are not required only for the Third Layer but required for all layers. [Reason] For operations, measures for identification and authentication need to be defined together to ensure practicality rather than logical accuracy.	We will consider revising the content, taking into account your comments.
	18-44	Corporation	Ch.3 L3.006	You need to review the following description: “Implement measures such as locking the areas where IoT devices and servers etc. are installed, introducing entrance and exit control, biometric authentication, surveillance cameras, and inspection on belongings and body weight.” [Reason] As we made a comment on L2.008 on page 43, these measures are not appropriate for IoT devices. Some measures are appropriate for servers but seem unnecessary as key aspects, which are no more than examples. When thinking of the weight and size of a micro SD card, inspection on belongings and body weight is no longer effective to prevent information leakage; therefore any measures to focus on disabling writing to external devices need to be established.	We consider “measures such as locking the areas where IoT devices, introducing entrance/exit control, biometric authentication surveillance cameras, and inspection on belongings and body weight etc.” effective for preventing unauthorized access and IoT devices being taken out.
	18-45	Corporation	Ch.3 L3.007	The measures provided are not practical and operable. [Reason] Verification beforehand and definition of abnormality in advance are listed as key aspects of the measure, it is actually impossible, however, to make these responses in advance.	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.
	18-46	Corporation	Ch.3 L3.009 L3.010 L3.012 L3.016 L3.017	We do not understand the necessity of providing the same contents in the Third Layer. [Reason] We do not understand why the the same contents as the Second Layer are provided in the Third Layer again. This may cause confusion for readers.	Security measures are classified based on the definitions of three layers. We will, however, consider revising the content regarding the classification of security measures, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	18-47	Corporation	Ch.3 L3.010	How about changing “Apply security patches as needed.....to IoT devices and the servers.” to “Apply security patches as needed after verification.....to IoT devices and the servers.” [Reason] It is quite important also for IoT devices or servers to conduct the process to verify that no problem occurs if any patch is applied to our environment.	We will consider revising the content, taking into account your comments.
	18-48	Corporation	Ch.3 L3.011 L3.017 L3.018 L3.019	It is quite important also for IoT devices or servers to conduct the process to verify that no problem occurs if any patch is applied to our environment. [Reason] It is necessary to consider the risk of reducing the effectiveness of encryption unless proper key management is in place.	We will consider revising the content, taking into account your comments.
	18-49	Corporation	Ch.3 L3.013	Not function but authority should be separated. In addition, these contents are applicable to not only the Third Layer but also all layers. [Reason] The descriptions seem inappropriate or insufficient.	Separation of authorizations in cyber space is described in L3.023.We will, however, consider revising the content regarding other security measures, taking into account your comments.
	18-50	Corporation	Ch.3 L3.014	“in the organization” is not necessarily appropriate. The description makes no sense unless the purpose of separation is clear. [Reason] We cannot understand the intent of limiting to in the organization.	We will consider revising the content, taking into account your comments.
	18-51	Corporation	Ch.3 L3.020	It is not appropriate to limit the target of countermeasures against falsification only to communication path. [Reason] Falsification may occur anywhere not only in communication.	As pointed out in your comments, prevention of falsification on communication paths is described in L3.020. Prevention of falsification other than on communication paths such as during retention is described in L3.002 and L3.011 and during maintenance in L2.014, etc.
	18-52	Corporation	Ch.3 L3.021	This must be handled in the Second Layer. [Reason] We cannot understand the intent of handing in the Third Layer.	Security measures are classified based on the definitions of three layers. We will, however, consider revising the content regarding the classification of security measures, taking into account your comments.
	19-1	Corporation	Overall	For the coming super-smart society, we believe that the framework like this is very useful for increasing social safety and agree to this activity.	Your comments will be considered as positive feedback on this framework.
	19-2	Corporation	Ch.3	In consideration of the establishment of audit/certification system for information management structure mentioned in L1, and venture and small to medium-sized companies, from a more realistic standpoint, outsourcing of information management to qualified third-party organizations should be included in examples of measures.	We will consider revising the content, taking into account your comments.
	19-3	Corporation	Ch.3 L2.002	In a system development life cycle mentioned in Key aspects of the measure and Examples of measures for each element, “manufacturing”, “distribution/installation”, “operation” and “disposal” of IoT devices should be included. (As described in L2.005 and L2.010, the security of IoT devices cannot be protected only by their function and appropriate manufacturing, distribution/installation, operation and disposal are essential.)	We will consider revising the content, taking into account your comments.
	19-4	Corporation	Ch.3 L2.010	For remotely-installed IoT devices, any method to remotely stop (dispose of) them in a safe manner is required. This should be included in Examples of measures.	We will use your comments as a reference in revising the content.
	19-5	Corporation	Ch.3 L2.010	The following method is also useful to ensure necessary security: once store the information to be disposed of in a removable anti-tampering device (see L3.002) in IoT devices, and then dispose of the said device only. This should be included in Examples of measures.	We will use your comments as a reference in revising the content.
	19-6	Corporation	Ch.3 L2.011	Linking a function after confirming appropriate software start up process and a function to prevent counterfeit software start up process to an anti-tampering device (see L3.002) in IoT devices can improve safety. This should be included in Examples of measures.	We will use your comments as a reference in revising the content.
	19-7	Corporation	Ch.3 L2.013	In response to compromising encryption algorithms in the future, it should be recommended to introduce IoT devices that enable migration of encryption algorithms.	We will use your comments as a reference in revising the content.
	19-8	Corporation	Ch.3 L2.013	As described in NIST Guidelines, it should be recommended to select secured encryption algorithms and update encryption keys on a regular basis. (Refer to NIST SP800-57, CRYPTREC)	We will use your comments as a reference in revising the content.

No.		Affiliation	Place	Comments	Responses to Comments
19	19-9	Corporation	Ch.3 L3.002	Besides theft, fraud by malicious users, maintenance personnel and administrators should be included in Risk factor. Anti-tampering devices are useful for preventing such fraud.	We will consider revising the content, taking into account your comments.
	19-10	Corporation	Ch.3 L3.004	As different systems are organically connected and operated, IDs (identifiers) with different schemes are mixed. The necessity of interconnection of IDs among systems should be explicitly explained. Currently system for interconnection of IDs has yet to be fully discussed. For Society 5.0, rules for assigning or interconnecting IDs are necessary.	We will use your comments as a reference in advancing cyber security policies in the future.
	19-11	Corporation	Ch.3 L3.005	In the world of Society 5.0, as many IoT devices are connected each other, a PKI-based authentication system is effective (because for authentication using a common key, distribution of common key is complicated, causing high traffic). The use of PKI should be mentioned in Key aspects of the measure and Examples of measures for each element.	We will use your comments as a reference in revising the content.
	19-12	Corporation	Ch.3 L3.010	For update of security patches, the necessity of full consideration of wiretapping and tampering should be explicitly mentioned (See L2.014).	We will consider revising the content, taking into account your comments.
	19-13	Corporation	Ch.3 L3.019	We understand that L3.018 recommends encryption of the communication path while L3.019 recommends encryption of data on the communication path, but the difference is difficult to understand. Show as Examples of measures for each element or change Overview of the measure to something like “Send and receipt encrypting information (data) itself, separating from encrypting communication path." * The important thing for security in the IoT field is not encrypting communication path in L3.018 but encrypting information (data) in L3.019. Especially in the society targeted in this framework in which supply chains are complexly linked, it is actually difficult to confirm the safety throughout the communication path and encryption of information (data) is required.	Encryption on communication paths is described in L3.018 and encryption of information (data) itself in L3.019. We will consider revising the content, however, taking into account your comments.
	19-14	Corporation	Ch.3 L3.019	Storing the encryption key used here in an anti-tampering device (see L3.002) connected to IoT devices or servers can improve safety. This should be included in Key aspects of the measure or Examples of measures.	We will use your comments as a reference in revising the content.
	19-15	Corporation	Ch.3 L1.012	This must be included in OECD’s eight principles, functional aspects, however, such as comprehensive agreement, traceability and opt-out also need to be included.	We will consider revising the content, taking into account your comments.
	19-16	Corporation	Ch.3 L1.012	Principle 3 in the OECD's eight principles says “The purposes for which personal data are collected should be specified”, however when considering a case where sensor data is always acquired and distributed, as the data is flow data, some purposes may not be specified when the data is acquired; therefore rules for comprehensive agreement need to be examined.	We will consider revising the content, taking into account your comments.
20	20-1	Corporation	Ch.3 L2.001	1. As described in L2.001, we understand that being certified by a third-party organization is very important for IoT devices. Electrical Appliance and Material Safety Act stipulates that home appliance manufacturers and importers must meet the technical requirements and affix the PSE mark on the product for sale, and it is important to meet requirements also for cyber security. Besides the above, being certified and authenticated by a third-party organization is meaningful to develop highly-secured products. 2. In addition, users can identify secured products with the PSE mark that indicates the acquired certification/authentication. 3. EDSE and IEC62443-4-2 are taken as examples of standards, and as you may know, we would like to mention, just for reference, that ANSI/UL 2900 has been developed and used in U.S.	We will use your comments as a reference in advancing cyber security policies in the future.
	20-2	Corporation	Ch.3 L2.004	4. As proposed in L2.004, we understand that measures against counterfeit products are also very important. We expect that the certification/authentication system and display of the authentication mark can contribute to measures against counterfeit products.	We will use your comments as a reference in advancing cyber security policies in the future.
	21-1	Corporation	Ch.3 L1.011	We recommend changing the wording “by assigning the numbers” in Key aspects of the measure to “by assigning IDs (identifiers) and important information (e.g. secret key and digital certificate) to guarantee uniqueness”. [Reason] There is no description on “identification of components” as a premise for managing and identifying production records of components. Uniqueness is important for identification.	We will consider revising the content, taking into account your comments.
	21-2	Corporation	Ch.3 L2.005	We recommend changing the wording “through the strong password setting and password-sharing among service person and devices, regular changes in passwords” in Key aspects of the measure to “through advanced authentication systems including certificate authentication and multi-factor authentication, strong password setting and password-sharing among service person and devices, regular changes in passwords”. [Reason] Even if a strong password is chosen, vulnerability cannot be eliminated due to the mechanism of passwords; therefore more advanced authentication systems are expected to be used if possible. “L3.003 Countermeasures against illegal log-in to the cyber space” describes advanced authentication. Authentication should be applied to not only people but also components.	We will consider revising the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
21	21-3	Corporation	Ch.3 L2.006	We recommend changing “L2.006 Restricted access to IoT devices” to “L2.006 Access control to IoT devices”. [Reason] In this section, not only restricted access from unauthorized access sources but also permitted (identified, authenticated or authorized) access from authorized access sources are included. Access control has a wider meaning.	We will consider revising the content, taking into account your comments.
	21-4	Corporation	Ch.3 L2.011	We recommend changing the wording “by checking the integrity of activated software” to “by checking the integrity of activated software using code signing”. [Reason] Code signing is useful for checking the integrity as described in https://www.ipa.go.jp/security/pki/075.html.	We will consider revising the content, taking into account your comments.
	21-5	Corporation	Ch.3 L2.014	We recommend changing “Carefully handle software updates against wiretapping and tampering.” to “Carefully handle software updates against tampering (ensuring the integrity using code signing).” [Reason] Security patches are generally available. (Security patches for Windows, Office and applications are available to everyone. Accordingly it is not only unnecessary to consider wiretapping (but rather impossible to wiretap). Code signing is useful for tampering prevention as described in https://www.ipa.go.jp/security/pki/075.html.	We will consider revising the content, taking into account your comments.
	21-6	Corporation	Ch.3 L2.015	We recommend changing the wording “Check installed software” to “Perform checking of the integrity of installed software and the authentication of distribution sources.” [Reason] The wording “Check .....” lacks concreteness. Here the word “check” must mean authenticating the integrity and distribution sources.	We will consider revising the content, taking into account your comments.
	21-7	Corporation	Ch.3 L3.003	We recommend changing the wording “authentication function combining two factors” to “authentication function combining two or more factors”. [Reason] It doesn't make much sense to limit to two factors. Ref. : In the authentication standards provided in https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html and https://pages.nist.gov/800-63-3/sp800-63b.html, multi-factor authentication is used more than two-factor authentication.	We will revise the content, taking into account your comments.
	21-8	Corporation	Ch.3 L3.003	We recommend changing “Adopt an authentication method with anti-tampering devices as the other factor of the two for the method.” to “Adopt an authentication method with anti-tampering devices as the other factor of the two for the method (in which a different anti-tampering device from that used for the first authentication should be used).” [Reason] The above is an easy-to-understand example to minimize changes, and what we want to recommend is to use another device because if any certificate is installed in an anti-tampering device on the PC, the PC may be taken over by malware, which may be inevitable resulting in low authentication strength. (It is recommended to mention the whole measures for enhancing authentication using multiple devices or paths.) Ref.: https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html https://pages.nist.gov/800-63-3/sp800-63b.html	We will consider revising the content, taking into account your comments.
	22-1	Individuals	Ch.3 L1.002	> When outsiders enter critical facilities, a person responsible should accompany and watching their behavior. With regard to the above, in order to detect/prevent the increasing number of crimes by insiders, the wording “In addition, monitor/record entry of insiders to specific areas.” should be added.	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
22	22-2	Individuals	Ch.3 L1.002	We would like to request you to explicitly mention in “Organizations” about the organizational introduction of devices that are conscious of electromagnetic wave leakage (that may be related to both the First and Second Layers). If you think you'll find out soon that a physical environment consisting of communication-related devices enclosed in a full-metal case, and optical cable LAN and properly-processed STP cable is much more better tolerated against tempest technology than that consisting of visible and tangible UTP cables. Whether we can construct such a tolerant environment depends on the decision-making of organizations, and the government must give notice and guidance for measures against tempest technology to both the public and private sectors; therefore we ask that you make sure to mention electromagnetic wave leakage in the guidelines that contain both cyber and physical security.	We will use your comments as a reference in advancing further discussions on the framework.
23	23-1	Research Institute	Overall	In order to apply IoT(Internet of Things) or CPS(Cyber Physical System) to the real world and operate it, it is necessary to think a structure includeing the human in the real world as part of process (HITLCPS: Human-in-The-Loop CPS). The framework proposes three-layer structure and includes "companies", which is satisfactory from the viewpoint of business innovation. However, no reference has been made to human (The role of human in HITLCPS is an intelligent controller that determine the behavior of controlled objects based on analysis results of data gathered from sensors) becoming an element of the control process by involved in the business. Therefore, the framework shoul be prepared to raise a discussion on where "Cyber Physical Security" is operated dynamically. In order to include "human" in the real world as part of process of the system, the framework should propote a safe system structure that keeps the system running normally and a resilient system structure that keeps the safe system structure when disturbance (including cyber attacks) occurs. Furthermore, considering General Data Protection Regulation enacted in the EU, the framework should be able to determine the scope of measures by considering how "human" is incorporatd into the international supply chain and setting the boundary of "human" data protection.	We will use your comments as a reference in advancing further discussions on the framework.
	24-1	Research Institute	Overall	1. Defining authorities with regards to risk. One of the most discussed areas of cyber security policy within Australia is that of authority. When a Chief Information Security Officer (CISO) makes a decisions to implement a specific control, that position is often challenged. Defining who has the power to interpret and designate risk against specific categories. Within Japanese Government agencies and private-sector corporations, this debate will be repeatedly undertaken. We have found it very useful to provide guidance to decision makers and practitioners around who has the power to categories risk.	We will use your comments as a reference in advancing further discussions on the framework.
	24-2	Research Institute	Overall	2. Identifying a common view of risk. Within the Australian Government's Protective Security Policy Framework (PSPF), objective categories of risk are clearly defined for all Australian Government agencies. While private sector agencies define their own risk thresholds, Government policy defines them for departments. This sets an expectation upon all government departments around how to categorize controls against risk. While the draft framework provides significant and meaningful measures around how to build and govern security, an objective whole of government risk matrix would ensure that these measures are consistently defined when they move towards implementation (https://www.protectivesecurity.gov.au/governance/security-risk-management/Documents/Business-impact-levels.pdf).	We will use your comments as a reference in advancing cyber security policies in the future.
	24-3	Research Institute	Overall	3. Critical infrastructure Australia has recently begun a national discussion around how to secure critical infrastructure. While the Government has the power to define risk within Australian Government agencies, not all critical infrastructure sits within Government. As a result, our discussion has moved strongly towards partnering with the private sector to secure critical infrastructure. The Japanese draft security framework is in many ways further ahead of Australia on calling out the importance of IoT and national connectedness. However, at its core, the relationship of supply chains and IoT could be more strongly connected to their context in relation to critical infrastructure.	We will use your comments as a reference in advancing cyber security policies in the future.
	24-4	Research Institute	Overall	4. Accreditation The measures detailed within the draft framework, while strongly worded and likely to promote real change in security, could use additional support. Within Australia, there has been a strong discussion over who has the power to audit government systems. Accordingly, the Australian Government certifies individuals as being empowered to conduct audits and certify that systems meet security standards. This ensures that auditors meet the expectations of the government with regards to quality. It would also allow the Government to define the training and standards to be used in audit. The auditors themselves can also regularly share information with the Government and act as Subject Matter Experts (SME's).	We will use your comments as a reference in advancing cyber security policies in the future.

No.		Affiliation	Place	Comments	Responses to Comments
	24-5	Research Institute	Overall	5. Private-Public Partnership One of the things I admire most about the Japanese system of government is its strong relationships with the private sector. The framework, while ambitious in taking a whole-of-nation approach to cyber security could leverage the private sector. My suggestion would be for Japan to create a Joint Cyber Security Centre (JCSC). Within Australia, the private sector can partner with Government (https://www.cert.gov.au/jcsc) this allows for greater collaboration and intelligence sharing.	We will use your comments as a reference in advancing cyber security policies in the future.
	24-6	Research Institute	Overall	6. Action Plan The draft framework offers a strong view on the future state of the Japanese cyber security landscape. However, to support this, we have learned that it is highly valuable to define key steps towards establishing this view. The document is bold but it would be very useful to international partners to see the priorities of the Japanese Government set out in terms of a timeline and the key steps to be completed to reach this future state.	We will use your comments as a reference in advancing cyber security policies in the future.
	24-7	Research Institute	Overall	7. International engagement The document admirably engages with the realities of international cyber security standards. However, I would encourage METI to commit to the development of an international cyber engagement strategy. While the broad themes discussed above refer to strategic matters of cyber security, smaller items will be listed below: * Consider selecting a specific international cyber security standard. * Define the interpretive power of controls (e.g. define what is mandatory and what is suggested). * Outline the legislative powers which enable the framework. * Consider a private sector security clearance system. * Identify disclosure roles for cyber incidents. * Establish committees for various industries where closed door sessions and briefings can be given privately (https://www.fsisac.com/).	We will use your comments as a reference in advancing cyber security policies in the future.
	25-1	Corporation	Overall	The the term "measure" when used will have many different meanings - strategy, - processes, - countermeasure That makes the document difficult to read, especially for beginners in this topic. Recommendation would be to use the above terms strategy, process, countermeasure in respective context instead.	We will consider revising the content regarding distinct use of the terms, taking into account your comments.
	25-2	Corporation	Overall	Operational measures and technical measures are mixed throughout the document. Clearly distingish between both in the document.	We will consider revising the content, including overall structural review on the classification of operational measures and technical measures, taking into account your comments.
	25-3	Corporation	Overall	Indicate for each measure who is responsible and should implement the measure, e.g. L.3.010 is only possible if patches exist, so - asset owner need to apply patches - product supplier needs to develop, apply and distribute patches such could be made visible by a tag in each layer's measure	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	25-4	Corporation	Overall	Recommendation: Add to each "measure" a description to whom (asset owner, product supplier, service provider, …) it applies.	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
25	25-5	Corporation	Overall	IEC 62443 is less prominent in this document, even thought it is an international standard. Should be mentioned similar to NIST and others. See topic 3	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as IEC 62443, etc., we will consider appropriate responses while verifying their content.
	25-6	Corporation	Ch.4	The creation of mutual trust is the ultimate goal of this framework. This goal should be made more prominent in the beginning of the document. The reader should know the goal in advance. So consider to bring chapter 4 in the beginning of the document.	In addition, we will consider revising the content, including overall structural review on “establishing trust”, taking into account your comments.
	25-7	Corporation	Overall	Measures on - how to select trusted cloud providers, - how to evaluate/assess threats & risks of could providers, - how to design a secure system including cloud services are are essentail but few and mostly missing. Spend more ideas on such.	The government plans to initiate discussions on safety assessment of cloud services this fiscal year, and we will consider revising the content of this framework, taking into account the details of the discussions and your comments.
	25-8	Corporation	Ch.2	The creation of **Trust** among the participants is the central element. Thus "Trust" should be prominent in the chapter and the figure 5.	We will consider revising the content, including overall structural review on “trust”, taking into account your comments.
	25-9	Corporation	Overall	Organizations have different roles like product manufacturer, system integrator, service provider, user of equipment. These roles are important to understand which "measures" to apply. Unfortunately this document does not further look into this topic in detail.	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	25-10	Corporation	Ch.2	Not clear what the meaning of this graph is or should be.	We will consider revising the content of Figure 6, taking into account your comments.
	25-11	Corporation	Ch.3 L1.001	The term measure should be replaced by strategy and processes.	We will consider revising the content regarding distinct use of the terms, taking into account your comments.
	25-12	Corporation	Ch.3 L1.001	It becomes important to have/define KPIs to measure the company's progress / the importance of development of KPIs is somehow missing. The assigned persons in charge need to be able to measure their advance, their success.	We will use your comments as a reference in revising the content.
	25-13	Corporation	Ch.3 L1.002	We should clearly distinguish between organizational measures and technical measures.	We will consider revising the content, including overall structural review on the classification of organizational measures and technical measures, taking into account your comments.
	25-14	Corporation	Ch.3 L1.011	Formulated very unspecific: Should be made more security specific. Unclear whom it adresses, a product supplier ? , - an end-user of a product ?	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	25-15	Corporation	Ch.3 L1.012	Correct classication of the information is essential / So each stakeholder should classify the information asset first.Than apply the correct measures depending on the classification.	Classification of information assets is described in L1.002, and data management based on appropriate classification in L3.002.
	25-16	Corporation	Ch.3 L1.012	The eight rules may be not enought as governmental laws and regulations exist e.g. DPGR. The check for compliance with existing laws and regulations is indispensable.	We will use your comments as a reference in advancing further discussions on the framework. In addition, for the relationship with GDPR, we will consider appropriate responses while verifying its content.

No.		Affiliation	Place	Comments	Responses to Comments
	25-17	Corporation	Ch.3 L1.013	Emphasize the importance of training such incident handling is important	Regular training and education are described in L1.006.
	25-18	Corporation	Ch.3 L2.001	Both measures described come with a very different level of security: - We see that self confirmation is widely abused, e.g. CE mark / Self confirmation must be treated with care and needs a powerful market observation that it remains effective / not a good measure here	We will use your comments as a reference in advancing further discussions on the framework.
	25-19	Corporation	Ch.3 L2.002	Difficult to verify which processes a 3rd party observed. Requirement to have a very detailed and thorough security documentation for an IoT product may be a more realistic requirement	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.
	25-20	Corporation	Ch.3 L2.003	Has nothing to do with Security. Products without safety functionality just cannot applied in safety applications, that is violation of general laws and regulations. / Recommendation: Omit this requirement	We will consider revising the content, taking into account your comments.
	25-21	Corporation	Ch.3 L2.004	Recommendation to split this requirement into 2 requirements - one addressing a product manufacturer - one for their customers as the measures to be taken are different depending on their roles	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	25-22	Corporation	Ch.3 L2.012	Is a virus check on IoT devices feasible ? Many may not be checkable at all!	We will consider revising the content, such as adding the descriptions “where possible” or “it is desirable to” where implementation is desirable but measures cannot be implemented, taking into account your comments.
	25-23	Corporation	Ch.3 L2.014	That requirement should be separated in different requirements - for (component) product supplier - for product integrator - for end user as everyone has different duties to fulfill. Implemenation Example: **Starting remote updates can be dangerous, depending on the application. Must be used with extreme care ! / Should not be a general recommendation.**	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
26	26-1	Business Group	Overall	Overall, we support METI’s efforts to establish a voluntary, risk-management based framework. We strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring security. While the Chamber and USJBC broadly support the draft Framework, we suggest below certain ways that it could be further strengthened or would benefit from further clarification.	Your comments will be considered as positive feedback on this framework.
	26-2	Business Group	Overall	One consideration relates to how small and medium sized enterprises (“SMEs”) will utilize the framework. The level of detail in the proposed draft is high, making it less accessible for companies that do not have sophisticated internal cybersecurity capabilities. Many such companies will also outsource parts of security management to third parties. We encourage you to develop subsequent guidance which is more accessible for SMEs, as well as to provide greater clarity around their responsibilities when outsourcing cybersecurity functions to third parties.	This framework summarizes the key points of security measures and provides an overall framework for security measures, but does not set specific levels of security requirements. However, in order to facilitate the utilization of this framework when actually implementing security measures, we will revise the content to provide concrete examples of measures by considering the effects and costs of measures, etc. and taking into account your comments. For specific levels of security measure requirements, etc., we will advance efforts to identify measures common to all sectors, etc. by taking into account concrete discussions in each industrial sector and mutually feeding back inter-sectoral issues.

No.		Affiliation	Place	Comments	Responses to Comments
	26-3	Business Group	Overall	Second, there is broad consensus in industry that a multi-stakeholder framework is a sound baseline for businesses' cyber practices, including internationally. The Chamber has communicated this in the U.S. context to consecutive Presidential administrations, and we maintain that such an approach is the cornerstone for managing enterprise cybersecurity risks and threats globally. Beyond the benefits that interoperability brings from a trade perspective, it ensures that companies can scale best-in-class cybersecurity practices across borders, raising overall levels of cybersecurity. While we applaud the discussion of international alignment in the draft Framework, we encourage you to develop a more detailed strategy for how the Ministry will work with their international counterparts and industry to promote interoperability among cyber regulations.	We will consider revising the content, including overall structural review on multi-stakeholders, taking into account your comments.
	26-4	Business Group	Overall	Finally, we ask that coordination within the Japanese government on the Framework be prioritized. Too often companies face regulatory uncertainty around the world when different domestic agencies establish competing frameworks or regulatory schemes related to cybersecurity and the digital economy. While Japan has been a global leader in ensuring that companies do not face such uncertainties, we have noticed slightly different approaches in how METI and the Ministry of Communications are approaching industrial cybersecurity. Ensuring that the two are coordinated in their approaches will help to mitigate any risks or challenges to the ICT and cybersecurity industry's growth in Japan.	We will use your comments as a reference in advancing cyber security policies in the future.
27	27-1	Corporation	Overall	Some Japanese Small & Medium Enterprise (SMEs) in the defense and aerospace industry have reportedly engaged some Original Equipment Manufacturers (OEMs) to explore how to avoid cybersecurity rules, thinking that working directly with OEMs will allow the SMEs to operate outside of NIST compliance (because these SMEs think incorrectly that METI and NIST rules are coming only from within Japan). The OEMs (Japanese and non-Japanese), however, recognize that operating outside of NIST rules for U.S. Government related procurement is not possible, and that Japanese SMEs in the defense and aerospace industry need better education on the source of NIST compliance. Even so, with or without knowledge on the source of NIST requirements, some Japanese SMEs can be expected to drop out of the defense and aerospace industry, leaving many SMEs that are better capable of acting on cyber security guidance. A similar situation with SMEs looking to avoid cyber and IT compliance took place in the Japanese banking industry around the year 2008. At that time, the last of Japan's investment banks switched regulators to the U.S. Government Federal Reserve and became subject to U.S. Federal Reserve information security requirements. There was a great deal of concern due to big Japanese banks outsourcing much of their critical IT functions, to include data centers. By 2010, the U.S. Federal Reserve mandated that all banks must have a supplier risk management program to address IT risks posed by suppliers and vendors. Similar to NIST 800-171, vendors could self-certify their own compliance. However, the self-assessment was 72 pages long and only in English. This assessment was developed by the U.S. Federal Reserve and became part of the Federal Reserve audit and inspection program. Out of many hundreds of banking suppliers at that time (800+), SMEs argued that they were not connected to any bank's systems and should not be required to comply with the IT requirements. This argument continued for about two years (2008-2010), and many Business Units and back office sections were reluctant to compel their suppliers to expend the resources (time and money) necessary to complete the self-assessment. In the end, the U.S. Federal Reserve informed all banks subject to its jurisdiction, to include Japanese banks operating within the U.S. and U.S. banks operating in Japan, that there would be no exceptions and placed the responsibility for ensuring compliance on the shoulders of those banks. Several SMEs were cut from the banking supplier base because they did not comply with the security requirements (either they were unable or unwilling to do so). Introduction of NIST 800-171 is beginning to reveal the same trend with SMEs in the Japanese defense and aerospace industry. The standard has been released (in English) and DoD will eventually require compliance through the OEMs. Without additional education and assistance, it will be challenging for many SMEs to answer the 110 areas on NIST 800-171. However, this will be the issue that determines whether they have contractual agreements with the U.S. Government and with OEMs (that also have contractual agreements with the U.S. Government).	We will use your comments as a reference in advancing cyber security policies in the future.
	28-1	Corporation	Overall	The area of the framework, or at least the description, that could be broadened is the second layer (cyber physical sysytems, wheret the componetns are IoT devices,). This layer is immensely complex. For example, the framework wants to certify IoT devices or classify IoT devices (e.g. official). Centerizd certification is necessary for cyber security, but it is difficult to understand how to even approach it, as ioT devices have such a broad range of functionality and capability (for example, extremey simple devices motion sensors to smartphones). Another example of difficulty due to this broad range is blocking physica; access, as buy their nature, IoT devices are expected to be ubiquitous. Therefore perhaps this section should at least mention that specific industries (e.g. automotive) would deal with these aspects differently.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
28	28-2	Corporation	Overall	Another examples of the difficulty brought on by widely differing IoT devices (even within industries) is continuous vulnerability updates. Again, is this practical with very simple IoT devices made by companies that don't have means or go out of business? This is a major concern of NIST, and we have already seen examples of devices that are old enought there is no will to update them, but they are still in active use.	We will consider revising the content, taking into account your comments.
	28-3	Corporation	Overall	Toward establishing trust: Trustworthy supply chain is an important and common practice, but in some ways is defensive and backwards looking. We feel that the "chain" security is also strongly dependent on innovatioin -- that is, innovating ahead of bad actors, and this gives a forward looking and offensive aspect in addition to workinig n a trustworthy chain. Perhaps the framework could make a mention of this.	Your comments will be considered as positive feedback on this framework.
	28-4	Corporation	Overall	In summary, the Framework is an impressive piece of work, and it is refreshing to see something this detailed, technical and well thought out. Given that standards, certification, etc, are likely to be set in individual industries, it would be good to see a "call to actioin" for those industries.	Your comments will be considered as positive feedback on this framework.
	29-1	Business Group	Overall	We have worked closely with governments around the world in relation to the development of national cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively deter and manage cybersecurity threats whilst still protecting the privacy and civil liberties of citizens. As a result of this experience, we have developed the International Cybersecurity Policy Framework, which sets out a recommended model for a comprehensive national cybersecurity policy. We have included a copy of the Framework with this letter. In summary, the Framework recommends six overarching principles that should guide the development of a successful national cybersecurity policy, namely that policies should: 1. be aligned with internationally recognized standards; 2. be risk-based, outcome-focused, and technology neutral; 3. rely on market-driven mechanisms where possible; 4. be flexible and encourage innovation; 5. be rooted in public-private collaboration; and 6. be oriented to protect privacy. While these principles are framed to guide overarching national cybersecurity policies, we believe they are also highly relevant to the Framework and should inform its approach. We appreciates METI's efforts to encourage society as a whole to improve cyber and physical security and to educate all kinds of industries in Japan, including small- and medium-sized enterprises (SMEs) which play such an important role in supply chains, job-creation, and society. We understand such efforts will be a basis to realize Japan's vision for a reliable Society 5.0 and Connected Industries. We are particularly grateful to METI for ensuring that the Framework addresses critical and emerging security topics, including the importance of supply chain security and discussing the concept of security by design and its increasing relevance for deployment of the Internet of Things ("IoT").	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
29	29-2	Business Group	Overall	To improve the draft Framework, we urge METI to place greater emphasis on existing international standards and private-sector efforts around cybersecurity. The global supply chain consists of companies located in many different countries and internationally-standardized policies and practices are highly beneficial for allowing global businesses to provide, and benefit from, the best globally available security solutions. Companies in the private sector are voluntarily collaborating to share best practices and strengthen cybersecurity throughout their supply chains and customer bases; the Framework should embrace these efforts as means to strengthen cyber and physical security throughout industry and society. We applaud the Framework's citation of several internationally recognized technical standards during its discussion of specific security considerations. However, the Framework would benefit from more clearly and strongly emphasizing the importance of aligning products, processes, and business practices with relevant internationally recognized standards conceptually throughout the document. Moreover, we note the draft Framework references internationally recognized standards for information security management systems (ISMS) (ISO/IEC 27001), cyber security management systems (CSMS) (ISO/IEC 62443-2-1), embedded device security assurance (EDSA) (ISO/IEC 62443-4-2), and information technology service management systems (ITSMS) (ISO/IEC 2000) as examples of measures at certain places. However, the draft Framework omits mentioning other important internationally recognized standards such as ISO/IEC 27103, which is the recently published ISO/IEC technical report on critical infrastructure cybersecurity that aligns with the Framework for Enhancing Critical Infrastructure Cybersecurity developed by the US National Institute for Standards and Technology, and ISO/IEC 27034 (concerning the secure development lifecycle).	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO/IEC 27103 and ISO/IEC 27034, etc., we will consider appropriate responses while verifying their content.
				It is important to ensure that the Framework is not interpreted as advocating for the development and implementation of local requirements for cybersecurity which may be inconsistent with internationally recognized standards and best practices. Not only would this result in additional compliance costs to companies doing, or seeking to do, business in Japan, but such an interpretation risks diminishing Japan's leadership in promoting seamless, interoperable standards regimes globally.	
	29-3	Business Group	Overall	We also observe that the recommended measures in the Framework appear targeted at different audiences — at consumers (purchasers of products) as well as suppliers (including producers or manufacturers of products). As such, there is ambiguity in terms of which recommended measures are applicable in a given scenario. For example, L1.008 and L1.009 would be more applicable to consumers, as they refer to a user organization needing to put in place a structure for detecting incidents and business continuity plans, respectively. However, L2.006 would be more applicable to suppliers, as it refers to the prevention of unauthorized logins through access control, something which is typically implemented by the supplier, and which a consumer would not be in a position to verify has been done by the supplier. L2.011 is another example of a recommendation that would be more applicable to suppliers — the countermeasures against counterfeit software would need to be built or implemented by the supplier and not a consumer.	We will consider revising the content, including overall structural review on the persons implementing measures, taking into account your comments. In addition, since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	29-4	Business Group	Overall	The requirements also do not factor in the possibility that different IoT devices have different capabilitites and not all IoT devices are able to implement the range of features and capability envisioned by the requirements. In relation to this, the various product features proposed by the Framework (e.g., identification of counterfeit software in L2.011, vulnerability countermeasures in L2.013, and having different fuctions accessible by different users) depend in how much computing power there is in the device to implement them; a 'dumb' IoT device would not be able to handle these requirements.	We will consider revising the content, such as adding the descriptions "where possible" or "it is desirable to" where implementation is desirable but measures cannot be implemented, taking into account your comments.
	29-5	Business Group	Overall	Given the rapid advancement of technology, and the corresponding evolution of the cyber threat environment, **we applaud METI for developing a robust, voluntary Framework informed by internationally recognized technical standards and best practices, and we look forward to working with METI to further strengthen the Framework and urge its widespread use and continuing evolution.** While we believe it would be counterproductive for the Framework to be applied as a rigid prescriptive measure, it has great value as a set of best practices. The recommendations we provide herein are intended to strengthen its impact and facilitate its broad adoption.	Your comments will be considered as positive feedback on this framework.
	29-6	Business Group	Ch.3	We recommendthat the Framework address the following considerations in the first layer: • Traceability: As a supply chain risk management best practice, companies should ensure they can trace all component parts to their original source. • Data security: All supply chain data and sensitive product data should be protected at rest and in transit using encryption or other security tools.	We will consider revising the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
	29-7	Business Group	Ch.3 L2.002	We applaud METI for including “security-by-design” into the draft Framework. Building software according to security-by-design principles generates safer, less vulnerable, better functioning software, and encouraging adoption of secure-by-design software can help drive adherence to such principles throughout the software sector. The section could be further enhanced with a more robust description of what “security-by-design” means. To that end, the section should cite ISO/IEC 27034 (Application Security), which provides guidance to assist organizations in integrating security into the processes used for developing and managing software applications.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO/IEC 27034, etc., we will consider appropriate responses while verifying their content.
	29-8	Business Group	Ch.3 L2.010	We recommends this section not only discuss how to dispose of IoT devices, but also include guidance for proactively replacing IoT devices as necessary to maintain currency or when they are no longer supported by the manufacturer.	We will consider revising the content, taking into account your comments.
	29-9	Business Group	Ch.3 L2.013	We recommends specifying that organizations should consider “patchability” in IoT device acquisition decisions as devices should be patchable absent exceptional circumstances. The guidance should also recommend “immediate” or “as quickly as possible, rather than “periodic,” application of patches since security patches should be applied as quickly as possible upon release, with priority given to those patches addressing high-risk vulnerabilities.	We will consider revising the content, taking into account your comments.
	29-10	Business Group	Ch.3 L3.014	BSA urges METI not to promote physical separation of networks in general, since physical separation will jeopardize Japan’s vision of “Society 5.0” and “Connected Industries” and often will not enhance security. Physically separated networks should be reserved to specific cases of highly sensitive data where, in addition to physical separation, other important features to mitigate the security risks introduced by physical separation are included.	We will consider revising the content, taking into account your comments.
	29-11	Business Group	Overall	There are other important international standards that the Framework should draw upon and refer to. We therefore recommend listing other important ISO/IEC standards such as ISO/IEC 27103, which provides guidance on how to leverage existing standards in applying a cybersecurity risk management framework, and ISO/IEC 27034, described above, in this section of the Framework. It would also be helpful to reference the NIST Interagency Report 7622 on supply chain risk management.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO/IEC 27103 and ISO/IEC 27034, etc., we will consider appropriate responses while verifying their content.
	30-1	Corporation	Overall	Our perspective on the draft Framework is based on our experiences managing direct and third-party cybersecurity risks to our products, services, and enterprise environment. We’ve learned that an effective approach is: risk based, helping organizations apply resources in a prioritized way; outcomes focused, enabling organizations to be agile and adaptive as the threat and technology landscape rapidly evolve; translatable, bridging risk management understanding across horizontal and vertical boundaries and facilitating meaningful executive-level engagement; and international standards based, supporting interoperability across sectors and regions in an increasingly interdependent ecosystem. Overall, an effective approach helps to establish a holistic program that drives continuous assessment and improvement in addition to compliance with relevant requirements. METI’s draft Framework includes numerous concepts and measures that are consistent with such an approach. It advocates for a risk-based, flexible, and interoperable approach, providing a helpful mapping of its security measures to controls within leading international standards and best practices. In addition, the draft Framework helpfully frames and describes how the information and communication technology (ICT) supply chain, or “value creation process,” is changing in “Society5.0”—by becoming more dynamic and less linear, with more fluid and fewer obvious start and end points (e.g., at page 7).	Your comments will be considered as positive feedback on this framework.

No.		Affiliation	Place	Comments	Responses to Comments
30	30-2	Corporation	Overall	**Focus on operationalizing the Framework within an enterprise risk management program** While the draft Framework appropriately reflects complexity and dynamism in the value creation process, METI's stated goal is for the document to be utilized at the operational level, which is best accomplished by enterprise risk management (ERM) professionals. Integrating a cyber/physical framework within an ERM program, which is responsible for managing risk horizontally across organizational silos and reporting risk posture vertically to senior management, helps not only to ensure a risk-based approach but also to facilitate meaningful executive engagement on security decisions and investments. In most organizations, an ERM program includes a few critical steps: identify assets and assess risks, considering likelihood, consequence, and prioritization; manage risks and protect assets (i.e., avoiding, transferring, mitigating, or accepting risks); detect and respond to continuously evolving threats; and review the effectiveness of risk management steps and adjust as needed. These steps contribute to a risk management lifecycle, or a consistent set of processes that ERM professionals can use to strengthen risk posture as their operating environment changes. Even as, for example, supply chains become increasingly complex, these steps remain relevant to evaluating and managing risks and responding to threats. A few approaches exist for framing a cybersecurity program and integrating it within an ERM program. Microsoft has traditionally used a "protect, detect, respond" framework; ISO/IEC 27103 and the Framework for Improving Critical Infrastructure Cybersecurity (i.e., Cybersecurity Framework Versions 1.0 and 1.1) use five "outcomes" or "functions"— identify, protect, detect, respond, and recover—as the framework for a set of security activities. Both approaches are consistent with the risk management lifecycle used by most ERM programs, making operationalizing the frameworks more straightforward. METI should further develop its draft Framework to create a bridge between its three-layered approach and cybersecurity frameworks that organizations are using in their ERM programs. Specifically, METI should not only complete a mapping of its security measures to controls within international standards or best practices but also consider interoperability and integration at the level of an ERM program. ERM professionals benefit from guidance that improves their understanding of the Society5.0 value creation process, but security measures should be framed in way that facilitates operationalizing them.	We will use your comments as a reference in advancing cyber security policies in the future.
	30-3	Corporation	Overall	**Strengthen and enhance the Framework's outcomes-focused approach** An outcomes-focused approach to a cyber/physical security framework is critical because it ensures that organizations have sufficient flexibility, determining the processes and technologies that most effectively manage risks in their environments today and evolving those processes and technologies along with the changing ecosystem and threat environment. While METI's draft Framework is grounded in a flexible approach, it could go further in strengthening and enhancing an outcomes-focused approach. For example, Security measure L1.013, "Appropriate information sharing of the security incident," calls for organizations to exchange security incident information with JPCERT/CC. While some organizations may strengthen their risk posture by doing so, others may more effectively leverage alternative information sharing forums, including global, private sector forums such as the Industry Consortium for Advancement of Security on the Internet (ICASI) and the Cyber Threat Alliance or public-private forums such as the sector-specific ISACs based in Japan. Rather than prescribing that organizations leverage JPCERT/CC, the draft Framework should highlight diverse information sharing forums that may be relevant for organizations to consider, including if they operate at a global scale or in a particular sector. Likewise, within the second and third layer (L2 and L3), METI outlines a number security measures related to the lifecycle of IoT devices. Many of these considerations can be consolidated into a principles-based approach rooted in recent research published by us, *The Seven Properties of Highly Secure Devices*. Security measure L2.001, "Introduction of secure IoT devices," calls for organizations to select IoT devices certified by a third party or for which there is self-attestation for safe and secure use. However, just one example of a third-party certification is provided (IEC 62443-4-2); there are others that are worth listing in this context to further encourage organizations to pursue third-party assessments. Here are two examples:	We will use your comments as a reference in advancing further discussions on the framework.

No.		Affiliation	Place	Comments	Responses to Comments
				OPC Foundation. In the manufacturing sector, the OPC Foundation developed the OPC Standard that companies can follow to help enable the secure exchange of data in automated industrial settings.8 After performing a check of the OPC Unified Architecture's (UA) security functions, the German Federal Office for Information Security confirmed that it was designed with security in mind and that no systemic security vulnerabilities were found. Trusted Computing Group (TCG). The Trusted Computing Group (TCG), which is an organization dedicated to creating standards for interoperable trusted computing platforms, is developing the Device Identity Composition Engine (DICE) Architectures for device identification and attestation. This enables manufacturers to use silicon gates to create device identification based in hardware, making security hardware part of the DNA of IoT devices from the ground up. Consistent with Microsoft's comments that METI's framework should be considered in the context of an ERM program, We welcomes further engagement with METI and Japanese industry as security measures for IoT continue to mature and take root in principles, products, and services as well as standards that can be leveraged to strengthen the IoT ecosystem. Ultimately, IoT will become less of an emerging or exotic new technology and blend into the fabric of organizational operations. This evolution will require organizations to consider IoT as part of their mainline ERM program.	
	30-4	Corporation	Overall	**Drive global interoperability by leveraging and mapping security measures to ISO/IEC 27103** While METI's intention to develop a framework that is globally interoperable is clear and appreciated, leveraging and mapping security measures to ISO/IEC 27103 would represent an important further step toward driving greater global interoperability. ISO/IEC 27103 integrates standards developed not only in JTC 1 SC 27 but also in other ISO and IEC subcommittees, leveraging broader risk management guidance and supporting cross-sector relevancy (e.g., ISO/IEC 20243, ISO 31000, and IEC 62443 among others). Moreover, ISO/IEC 27103 demonstrates how these standards help to fulfill not only the functions, categories, and subcategories introduced through the Cybersecurity Framework but also the principles and essentials introduced by METI's Cybersecurity Management Guidelines.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO/IEC 27103, etc., we will consider appropriate responses while verifying their content.
31	31-1	Corporation	Overall	We do very much appreciate the division between security for IT and IoT systems, as in the past a lot of issues have arisen from using requirements from IT on IoT. In this, the framework is a great first step towards harmonizing safety and security, a well as the different operational conditions between It and IoT, and will be a great help to increase the security while achieving the 'Society 5.0'. Our experience with auditing and testing such systems has shown a great need to provide more guidance to the industry, so this it s a most welcome step.	Your comments will be considered as positive feedback on this framework.
	31-2	Corporation	Overall	Some care needs to be taken with the scope of IoT though. The range of IoT devices is rather vast, covering for example home entertainment, healthcare implants, public lighting, up to smart grids and nuclear power plants. In this, any general guideline for IoT devices has to necessarily stay rather broad, and cannot give vendors and operators in a specific sector the amount of guidance they need. In this, we are looking forward towards companion documents that dwell into more detail both on the technology and on sector specific security requirements, and would be very happy if we could be of assistance.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	31-3	Corporation	Overall	The coordination with international standards (NIST CSF, NIST SP 800- 171 and ISO27001) is well intended, the idea this framework can contribute in increasing the market value of	Your comments will be considered as positive feedback on this framework.
	32-1	Business Group	Overall	**Scope and Impementation** The Framework clearly addresses how companies may use the framework; however, it is unclear what type of entities are covered or whether only specific sectors of the economy are covered. If the intent of the Framework is to be sector-specific, we recommend including specific requirements for each sector and addressing whether they will become mandatory. We would also recommend that METI specify the timeline for adoption of the framework as well as implementation. The Framework may provide more useful guidance to companies by focusing on key high-level principles as for each of the Three Layers, referencing existing standards for guidance and implementation in place of the three sections of measures from the draft framework. In this way, users and organizations will have the flexibility to align their needs according to the principles without being confined to the prescribed measures in the framework.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.

No.		Affiliation	Place	Comments	Responses to Comments
	32-2	Business Group	Overall	**Alignment with International Standards** We notes that numerous cybersecurity recommendations in the Framework conflict with or are redundant with current international standards. The parallel existence of local and international standards could lead to various security and interoperability problems as well as high compliance costs. Industry would benefit more from global standards and consolidation than from having to reconcile numerous individual frameworks from local regulators. The potential conflicts between international and local frameworks can be overcome either by adopting global standards or by making sure that local frameworks are fully aligned with international standards and with each other. Many of the Framework's measures focus on Internet of Things (IoT) security and incident response/management requirements. We propose that specific guidance on IoT security and incident response/management be provided or adopted from international standards bodies to address those concerns and requirements, better focusing and providing more directed guidance on the issues involved. The Framework should cover all systems that are considered part of cyberspace and not exclusively focus on IoT systems, as doing so could give a false sense of security.	Conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards, we will consider appropriate responses while verifying their content.
	32-3	Business Group	Overall	In order to make the Framework more helpful for companies, we suggest that METI include a register of risks or security concerns for the Three Layers (Figure 4, page 8). Such a risk register would help organizations align their risk assessments to METI's Cybersecurity Framework and ensuring they are addressed as part of their existing practices, rather than requiring prescriptive security measures that stifle security innovation. Additionally, implementation and practice of existing standards such as ISO 27001 Information Security Management Systems (ISMS) will result in implementing similar measures based on the risk identified and assessed.	We will use your comments as a reference in advancing cyber security policies in the future.
	32-4	Business Group	Ch.3 L1.001 L1.002	Regarding L1.001 "development of security policies and preparation of the structures," We note that the risk impact is not necessarily related to the risk factor specified. For example, the cause for delay in countermeasures against security incidents could be due to lack of preparation, insufficient resources, an unanticipated incident, and many others. Similarly, the risk factor in L1.002 is similar to what is outlined in L1.001 though phrased differently. Again, the causes of the risk impact in this section may not necessary be due to the security measures taken or not taken. We encourage METI to review existing standards such as ISO 27001 to ensure alignment and clarity of guidance.	We will consider revising the content, taking into account your comments.
	32-5	Business Group	Ch.3 L1.003	Regarding L1.003 "clarification on security incident responses," effectiveness in security incident response depends not solely on having related documentation and security measures in place. We suggest that METI reference and adopt ISO 27031 (ICT Readiness for Business Continuity) to ensure adequate preparation against known and emerging security incidents, and ISO 27001 to ensure adequate ISMS is in practice to address known risk issues in organizations.	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27031, etc., we will consider appropriate responses while verifying their content.
	32-6	Business Group	Ch.3 L1.004	**Security Risk Factors vs. Weaknesses** Regarding L1.004 "maintenance contracts with suppliers," the risk factor and impact are general and do not directly relate to contracts and suppliers in a way that would motivate the adoption of the security measures recommended in this section. Without identifying the related threat, what is listed as a risk factor in L1.004 is too attenuated, and should not be classified as a risk factor as such. ISO 27001 addresses third party security, and the ISO 27036 series focuses on information security suppliers. In addition, ISO 27017 and 27018 address the additional security and privacy controls required for cloud computing. These standards in combination address the risks involved in using third party providers.	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27017 and 27018, etc., we will consider appropriate responses while verifying their content.

No.		Affiliation	Place	Comments	Responses to Comments
32	32-7	Business Group	Ch.3 L1.005	With respect to L1.005 “implement PDCA cycle for security measures,” PDCA is one of the many management systems approaches that organizations may use. ISO/JTC1 have recognized this and therefore removed PDCA as the prescribed management system approach in all management systems standards, including ISO 27001 and 9001. Concerns over incident preparedness and response capabilities are addressed in existing ISO standards 27031 and 27035, respectively. The contents in this section are very general and should reference the relevant standards directly.	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27031 and ISO 27035, etc., we will consider appropriate responses while verifying their content.
	32-8	Business Group	Ch.3 L1.007 L1.008	L1.007 outlines “management of components, systems, and other assets.” We note that asset management is part of ISO 27001 ISMS. The risk factor cited in this example would be addressed if the organization were to implement ISO 27001 ISMS. Further, these factors should be classified as a potential weakness, not a risk factor, if no related threat is identified. The risk impact described is a potential risk, but unmanaged devices are not the only source of malware infection. Similarly, in L1.008 “implementation of functions and procedures for appropriate detection and analysis of security” the risk factor described is a potential weakness in a given environment; however, without identifying the related threat, it should not be classified as a risk factor. The risk impact described could potentially result from a delay in discovering a security incident, which is not the same as the inability to correctly identify security incidents. An effective incident detection and response system encompasses more than the function and procedures alone, as the title of the recommendation suggests. While the examples of measures for each element include the systems element, they do not cover the components, data (e.g., event logs) and procedures involved, which are all important in holistically addressing concerns regarding an organization’s capability in identifying security incidents. In order to more effectively address this issue, we suggest adoption of ISO 27035 standard for incident management and handling guidance.	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27035, etc., we will consider appropriate responses while verifying their content.
	32-9	Business Group	Ch.3 L1.009	Regarding L1.009 “inclusion in the business continuity plan and contingency plan,” the risk factor described is a deficiency or weakness (i.e., “cannot make proper business continuity decisions”) which may result from other weaknesses – for example, lack of a business continuity plan (BCP), inadequate testing of the BCP, indecisiveness of the decision maker, or lack of knowledge. The risk impact noted refers to a scenario in which “the organization cannot determine the impacts of the security incident,” which is not mentioned in the risk factor reference. We recommend that the concerns and measures outlined in this section be addressed through adoption of ISO 27031 “ICT Readiness for Business Continuity,” and ISO 27035 “Information Security Incident Management.”	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27031 and ISO 27035, etc., we will consider appropriate responses while verifying their content.
	32-10	Business Group	Ch.3 L1.011	Regarding L1.011 “management of records on produced components,” the risk factor described is likely the result of other issues, which can relate to many other factors. What is articulated as the L1.011 risk factor is thus too generic to be classified as a risk factor as such. The measures recommended in this section are unlikely to ensure that the root cause would be discovered to improve assurance of the supply chain. Alternatively, we suggests referencing ISO 27036 to address supply chain security concerns.	We will consider revising the content, taking into account your comments. In addition, conforming to international standards, etc. is important in achieving international harmonization. We will therefore make a comparison with NIST SP 800-53 and revise the content, in addition to comparisons with ISO/IEC 27001, NIST CSF, and NIST SP 800-171, the results of which we have already provided to you. In addition, for comparisons with other international standards such as ISO 27036, etc., we will consider appropriate responses while verifying their content.

No.		Affiliation	Place	Comments	Responses to Comments
	32-11	Business Group	Ch.3 L1.013	**Information Sharing** In L1.013 “appropriate information sharing of the security incident,” the risk factor does not connect with the title and the risk impact described. The risk factor described should not be considered a risk; rather, it is a deficiency in the system that can result in a risk under certain threat conditions. Effective cybersecurity threat information sharing requires more than creating a security operation manual and sharing with JPCERT/CC. It requires establishing mutual trust or a trust ecosystem that will facilitate sharing amongst entities with the capacity to act upon actionable threat information. In addition, any such systems must ensure adequate protection of information shared, including understanding what types of information to share, and how shared information may be used without compromising the proprietary or sensitive data of the sharing entities (e.g., personal data). We also recommends that METI review existing trust systems, such as the use of independent third-party audits and attestation, as in the case of ISO 27001 certification and the Systems and Organizational Controls (SOC) continuous assurance (SOC I and II) schemes that have been widely adopted and recognized by governments and industries in many countries, including Japan. Existing schemes should be adopted and further promulgated instead of creating new certification systems that will cause additional costs to businesses, increase barriers to market access, and negatively impact innovation and business efficacy.	We will consider revising the content, taking into account your comments.
	32-12	Business Group	Ch.3	**Inclusion of Internet of Things (IoT) Security** Section 3.2 focuses on IoT security; however, it does not fully address different IoT systems models and the adoption of related protection approaches specific to those models. For example, IoT systems for Smart Homes, Smart Offices, Smart Buildings, Smart Vehicles, and Industrial Control Systems (ICS) will all require different security approaches given the different types of risk scenarios, the cost of IoT end points, and the data and network systems involved. Generally, the measures proposed in this section appear too narrow and high level so that they may not be useful for actual implementation. For example, in L2.008 on physical security measures for IoT devices, the measures suggest considering only surveillance cameras and the use of locks and entrance/exit controls without considering the physical environment where the devices are installed, and physical access for maintenance purposes. Regarding L3.014, “separation of networks,” ITI recommends that physical isolation be limited to cases where systems are used for highly sensitive and local purposes. The use of physical isolation results in disconnection from the networks of other systems. We suggest that METI consider adopting available IoT security standards or working with ISO standards committees to develop suitable guidance for different IoT systems models.	This framework provides an overall framework for security measures and describes the approaches and measures common to all industrial sectors. Since it is assumed that the content of security measures required for each industrial sector may vary, we henceforth intend to make the measures specific when they are taken, taking into account the efforts to formulate specific guidelines for each industrial sector, etc.
	32-13	Business Group	Ch.3	While Section 3.3 “security measures for connections in cyberspace,” focuses on “connections,” the measures are broad and high-level, focusing more on supply chain and IoT security. The recommended measures also focus on IoT device connections-related issues rather than more comprehensive connection issues impacting all systems, devices, and people, all of whom will connect in different ways and affect the security of IoT systems and cybersecurity more broadly. Further, we note L3.006 overlaps with the physical security measures in L2.008. Additionally, L3.008 on “maintaining the availability of cyberspace” also may represent a broad requirement, depending on how “cyberspace” is defined. For organizations and users, the issue of business continuity and systems availability are covered in Layer 1, and measures are also provided in ISO 27001 and ISO 27031.	We will use your comments as a reference in advancing further discussions on the framework.
	32-14	Business Group	Ch.3 L1.010	**Compliance with Laws and Regulations** With respect to L1.010, we note that a violation is an outcome of one or more unlawful activities. As such it should not be classified as a risk factor. Compliance with laws and regulations is expected of all organizations, not only in relation to the context of this Framework. We respectfully suggest removing this section.	We will use your comments as a reference in revising the content.
	32-15	Business Group	Ch.3 L1.012	**Protection of Privacy** The risk factor in L1.012 is focused on a narrow aspect of personal data collection and use. In the context of cyberspace, personal data may be collected not only by devices, but also from other online systems, social networks, etc. It is important to consider the OECD privacy principles as part of a set of principles that the Framework should promote rather than considering them as a measure for privacy protection.	We will consider revising the content, taking into account your comments.

No.		Affiliation	Place	Comments	Responses to Comments
33	33-1	Corporation	Preface	I feel strongly that the introduction of security capabilities to Industrial IoT systems of all kinds needs to be carefully focused so that security has an appropriate and proper place with respect to safety, reliability, resilience, and privacy. In light of that I would like to offer a proposal that you consider recasting the framework as "The Cyber/Physical Trustworthiness Framework". I stand ready to discuss this change in scope but believe it would be a good change and bring your framework efforts closer to the work in the Industrial Internet Consortium, Industrie Platform 4.0, and the work ISO's new IoT working group as well as the work on Cyber/Physical systems at NIST.	We will use your comments as a reference in advancing further discussions on the framework.