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

ID	No	Affiliation	Place	Comments	Responses to Comments
1	1	Individuals		The content proposed by “Cyber Security Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry” clearly states that the proposal is to be made in “Japanese and English”. Since it is an issue in Japan, however, I think that it is not necessary to make the proposal in foreign language, including English, etc. More concretely, the English versions of “Invitation for public comments” and “The Cyber/Physical Security Framework(Draft)”, etc. are not necessary. In summary, it should be clearly stated for what purpose public documents in foreign language are prepared.	Security measures are not sufficient for efforts only in Japan, and it is necessary to proceed with the study while maintaining harmony with overseas systems. Therefore, we carried out public comments in English in order to seek opinions from not only domestic but also foreign countries.
1	2	Individuals		The term “Invitation” clearly stated by the Ministry of Economy, Trade and Industry means “to invite or to visit”, etc. in an active concept and has other passive meanings in the concept of public offering. It is a Japanese-English term created by Japanese who are not fluent in English. For example, when intending to publicly solicit proposals of opinions, I think that the term “Suggestion”, etc. is appropriate. The concept of “Comments” is also in the similar concept as “Suggestion”, etc. in terms of meaning. In conclusion, I think that the phrase “Suggestion for public comments”, etc. is appropriate.	We will use your comments as a reference in implementing public commnets in the future.
1	3	Individuals		In the structure of “Society6.0”, “space colony” is considered to be introduced. Therefore, I think the issue is in “freeze (operation stop)” in “storage” communication when connected to IoT devices, considering “sensor technologies, network technologies, and device technologies” consisting of “Cyber Physical System (CPS)” to be introduced in “5G (5th Generation)”. More concretely, I think that it is to integrate “IPS servers (Internet service provider)” using the Internet connection and “SIP servers (session Internet protocol)” using telephone lines and “Big Data (BG)” consisting of cloud computing in the area of “Information technology (IT)”. I think that it is to integrate “HTTP (HyperText Transfer Protocol)” using “API (Application Programming Interface)” consisting of edge computing in the area of “Artificial Intelligence (AI)”. In summary, I think that, for “HGW (Home GateWay)”, the installation of antenna tuners in the structure of “area (sector)” is necessary when “FTTH (optical fiber)” and “CATV (cable television)” using wired LAN are integrated to “Wi-Fi (wireless local network)” using wireless LAN by enabling them to support “satellite communication (satellite system)” in “GPS (Global Positioning System)” function for “GSM method and W-CDMA method” consisting of 3GPP. In conclusion, I think that it is necessary to describe the concept of structures in the areas of “general construction (civil engineering and construction), ships and vessels, aircrafts, railways, vehicles, industrial equipment, home electric appliances”, etc. For example, in “5G (5th Generation)”, “NR (New Radio)” using “satellite communication channel (satellite system), telephone lines (telecommunication), and the Internet connection (broadband)” is to be considered. In “6G (6th Generation)”, “NA (New Audio)” using “satellite communication channel (satellite system), telephone lines (telecommunication), the Internet connection (broadband), and television connection (broadcast)” is to be considered.	We will use your comments as a reference in advancing policies in the future.
1	4	Individuals		In the part concerning “Framework”, I think that cyber security measures are necessary for cloud computing using IT networks in the area of “Information technology (IT)” using “Cyber Physical System (CPS)”. I think that cyber security measures are necessary for edge computing using AI networks in the area of “Artificial Intelligence (AI)”. More concretely, I think that “sensors, networks, and devices” will be integrated, and therefore “API (Application Programming Interface)” on the Web can be a standard in “HTTP (HyperText Transfer Protocol)” communications for AI networks. For software, I think that cyber security measures that can support “applications, firmware, and database”, etc. are necessary. In summary, I think that networks can be considered as a structure consisting of “Big Data (BD)” in “database (DB)”.	We will use your comments as a reference in advancing policies in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
1	5	Individuals		In the area of “Artificial Intelligence (AI)”, I think that “separation” between approximately 1% of “geniuses (genies)” and approximately 99% of “ordinary people (ordinaries)” will become apparent. The definition of intelligence in plants and organisms, I think, is the “learning ability, cognitive ability, and judgment ability”. I think that the definition of intelligence in human is the “language capability, creativity, and judgment capability”. More concretely, I think that the structure using “data (numerical value)” “mechanisms” based on “answers” in AI consists of the structures of “statistical learning (probability learning)” and “machine learning”. (1) I think that the structure of statistics in statistical learning is the structure in which humans use the current data derived from the past data based on “statistical analysis (analyzer)” using “Bayesian theory (game theory)” with humans introducing the purpose to AI. In the answers derived by AI for the purpose, there is no “grounds (basis)”, etc. in this structure (2) The structure of “neural network (perceptron)” in machine learning consists of “deep learning” using “algorithms (information processing procedures)” in software. In hardware, it is the structure of “nodes (transistor circuits) and edges (bus wiring)” in the “input layer, hidden layer, and output layer”. For example, “convolutional neural network (CNN)” in learning with teachers, “recurrent neural network (RNN)” with teachers, and “generative adversarial network” without teachers, etc. I think that it is the structure for which turning tests are costly. In the answers derived by AI for the purpose, there is no “grounds (basis)”, etc. in this structure. In summary, unless humans are advanced to the level of approximately 1% of geniuses, advancement of the AI structure cannot be achieved. I think that, with the structure is highly advanced by approximately 1% of geniuses, even if the AI structure that is better than approximately 99% of ordinary people can be created, it cannot be made better than approximately 1% of geniuses. In conclusion, I think that, even if it is proposed to be human centered, approximately 99% of ordinary people will be overtaken by the AI structure through natural selection based on “heredity and environment” as defined in the theory of biologic evolution.	We will use your comments as a reference in advancing policies in the future.
2	1	Corporation	CPS.DS-5	It is not possible in some cases to “secure sufficient (complete) resources for so that no service activities will be suspended”, and therefore should be modified to read: “‘secure resources (people, goods, and systems) for protection or minimization of impacts’ under cyber attack (e.g., DoS attack)”. [Reason] As I believe that there are no complete protection measures against (D)Dos attacks, “securing sufficient resources” is unrealistic. In addition, “people” must also be secured for monitoring and making adjustments. (Reference) Completely eliminating DDos attacks is practically difficult https://japanese.engadget.com/2016/10/22/dns-ddos-twitter-spotify-psn/ (Reference 2) Cases in which Akamai withdrew https://japanese.engadget.com/2016/09/26/620gbps-ddos/ (Reference 3) In the case of botnet, whether the protection was effective cannot be determined https://japanese.engadget.com/2016/02/25/ddos-project-shield-google/	We revised the content, taking into account your comments. Relevant part : Part III 3.9 Data security CPS.DS-5
2	2	Corporation	CPS.DS-8	“Limiting access to the files” is considered to be a temporary measure to prevent spread of impact, and therefore it is deemed inappropriate to include this as an item representing “appropriate measures”. ⇒ When the organization detects the exposure of sensitive data to inappropriate entities, take appropriate measures such as “grasping the impact, preventing spread of impact, and measures to prevent recurrence”. [Reason] I initially read this sentence as “limiting access to the files” of the “data inappropriately exposed”. As for the description of “appropriate measures”, “grasping the impact, preventing spread of impact, and measures to prevent recurrence” listed in Appendix C (p.C-15) are considered more important than “limiting access to the files”, which is a temporary measure to prevent spread of impact.	As the response after information leak detection, including the original description and your comments, is considered appropriate in CPS.RP or later. Please refer to CPS.RP-1, CPS.AN-1 etc.
2	3	Corporation	CPS.PT-2	Various unnecessary ports should be “physically or logically blocked” rather than “physically blocked”. [Reason] Because the ports concerned include OS ports. In addition, commercially available dedicated devices used for physical blocking can be purchased at the prices anyone can afford, and, if possible, both “logical (software-based measure) and physical” measures should be discussed for port control.	We revised the content, taking into account your comments. Relevant part : Part III 3.12 Protective technology CPS.PT-2

ID	No	Affiliation	Place	Comments	Responses to Comments
3	1	Individuals		I am commenting on the assumption that what to do has already been decided even though the comments were said to be used as reference in making the final decision. Collecting these comments seems to be just a waste of time. It would just be worthless to do anything because, just like the fraudulent case of the Ministry of Health, Labour and Welfare, nobody takes responsibility when the officials commit fraudulent acts.	This framework has been modified based on the comments received from people in Japan and overseas as public comments.
4	1	Individuals	Table 2.1-4	The phrase listed in “Assumed security incidents in the first layer” (1) (d) must be a typo.	We revised the content as suggested in your comments. Relevant part : (Japanese) Table 2.1-4
5	1	Corporation	CPS.AC-8	It is listed in CPS.AC-8 to “Identify and authenticate the network connections and destinations when IoT devices and servers receive data from cyberspace or when IoT devices and servers transmit data to cyberspace”. I have read this a requirement for measures against the risk of information leakage or inclusion of false information resulting from the entity receiving the information or the entity transmitting the information being disguised. When “goods” that connect to network, which are covered by this framework, are considered, depending on the intended use, information may easily be obtained by malicious persons. In order for the goods to authenticate themselves, identification/authentication information must internally be stored, and, depending on the implementation methods, the information may be obtained by the method similar to Shack attack such as directly reading from ROM. Once the identification/authentication information is fraudulently obtained, the measures requirements listed in CPS.AC-8 will be ineffective. From these point of views, I would like to propose adding “safe storage of identification/authentication information” to the measure requirements.	In this framework, physical attacks against hardware are assumed and the measure requirements are described in CPS.DS-4, CPS.DS-7, CPS.DS-11, etc. Regarding your commnents, we leave the contents as original.
6	1	Individuals	CPS.RM-2	With regard to the content of CPS.RM, 3.5. CPS.RM – Risk management strategy Set priority, constraint, and risk tolerance assumptions for the organization and use it to judge investment risk. in particular, when comparing CPS.RM-2 Determine the organization’s risk tolerance level based on the result of the risk assessment and its role in the supply chain. with the following section 3.6. CPS.SC – Supply chain risk management Establish enterprise etc. priorities, constraints, risk tolerances, and assumptions and use them to assist in analysis of supply chain risk management. Establish and implement the process of identifying, evaluating and managing supply chain risks. the description “Determine the organization’s risk tolerance level based on ... its roles” seems to be in conflict from the point of view of consistency.	As stated in CPS.SC, "Risk tolerance of own organization" decided by“Organization's role in the supply chain” in CPS.RM is the important input to establishing a supply chain risk management process. Regarding your commnents, we leave the contents as original.
7	1	Individuals	p.3 etc.	In order for the general public to understand, the meanings, etc. of unfamiliar terms should be provided and the use of katakana terms should be avoided to the extent possible.	We used your comments as a reference in revising the content. Relevant part : Introduction 1.
7	2	Individuals	p.11 etc.	Add easy-to-understand explanation for the term “procedure” (first appears on p.12) On page 12, add a note: “For the definition of the term ‘procedure’, see Table 1.2-1 (p.17)” On page 17, in Table 1.2-1, the expression “a series of activities to archive defined purpose” is ambiguous. ⇒ “a system of operating procedures to achieve defined purpose”	We used your comments as a reference in revising the content. Relevant part :Part I 1. , Table 1.2-1

ID	No	Affiliation	Place	Comments	Responses to Comments
7	3	Individuals	p.14	The term “transcription function” is hard to understand, and therefore they should be replaced with “information transcription function” or “function of transcribing information”.	Regarding your commnents, we leave the contents as original.
7	4	Individuals	p.30	The term “hazard” should be added to the glossary. Hazard: Harm factor. Cause or source of accidents or disasters. The value obtained by multiplying the probability of encountering a hazard by the impact of accident or disaster is the risk.	We used your comments as a reference in revising the content. Relevant part : Appendix E
7	5	Individuals	Overall	I believe that in the world of Soriety5.0, consumers play important roles as stakeholders. The notations that take into consideration consumers should be used. The concrete locations and proposed amendments are as follows. (1) Figure i-2 (p.2): Add “Consumer” in the lowermost part. (2) Figure 1.3-1 (p.21): Add “Consumer” in the rightmost part. (3) Figure 2.1-5 (p.33): Add “Consumer” in the rightmost part. (4) Appendix A Use case #1: Add “Consumer” in the rightmost part.	We used your comments as a reference in revising the content. Relevant part : Figure i-2, Appendix A Use Case 1
7	6	Individuals	p.13	The phrase “the enterprise’s management” in the second paragraph of the description of the first layer should be replaced with “the enterprise’s information security management”, which is more accurate and easier to understand.	Corporate management, which is the basis of the reliability of the first layer, is a broad concept that includes not only information security management but also corporate governance. Regarding your commnents, we leave the contents as original.
7	7	Individuals		Since the relationship between risks and risk sources is not explained, it is difficult for people not familiar with ISO 31000 to understand. I suggest adding description of the relationship between risks and risk sources somewhere, for example, below the bulleted list on page 24. (I have in mind the description on page 251 of the Japanese edition of the “ISO/IEC 27017 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, Japanese Standards Association, dated Oct. 10, 2017)	We used your comments as a reference in revising the content. Relevant part : Part II
7	8	Individuals	p.29	In the second paragraph of ii., it is not clear what “the equipment that measure the dynamics of the physical space and transmit data to the cyberspace” exactly means. An example should be added. “Sensor”?	We revised the content, taking into account your comments. Relevant part : Part II 1.1.
7	9	Individuals	Figure 2.1-6	It is not clear what “hazard factor” means. Since “hazard” is defined to mean “harm factor”, “hazard factor” becomes “hazard factor factor” and does not make sense. Delete the annotation, etc. or replace it with “risk” or “risk source”.	Regarding your commnents, we leave the contents as original.
7	10	Individuals	Figure 2.1-6	The relationship with the three-layer is unclear, and therefore the description should be modified. The scenario such that “Attacks are performed from the third layer. The vulnerabilities of controllers in the second layer are targeted, and fraudulent instructions are generated and sent to the devices. Disaster will occur if malfunction preventing equipment in the devices is defective or insufficient.” should be illustrated in a figure. In this case, “attacks”, “vulnerabilities of controllers”, and “defectiveness or insufficiency of the devices” are the risk sources.	We used your comments as a reference in revising the content. Relevant part : Part II 1.1.
7	11	Individuals	p.25, 48	Cloud services are commonly used for processes related to IoT, etc. Cloud services belong to the third layer, but their management needs to be carried out in the same manner as that of physical devices in the first layer. It is desirable that this point be supplemented. (1) Insert the following sentence after the last paragraph on page 28: When using cloud services, however, although virtual machines (virtual servers, virtual networks, virtual switches, virtual storage, etc.) belong to the third layer, risk analysis on them should be conducted as devices in the first layer. (2) Add a note regarding cloud services at the end of the reference list on page 56. (Note) When using cloud services, it is desirable that the items of ISO/IEC 27017 conforming to the items of Annex A of ISO/IEC 27001 be referenced.	We used your comments as a reference in revising the content. Relevant part : Part II 1.1. , Part III 3.
7	13	Individuals		Reports should be created in character code specified by eGov to make it easier to refer to the text when writing comments.	We will use your comments as a reference in implementing public comments in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
8	1	Group	Figure 1.2-4	“Figure 1.2-4” illustrates the concept described in the preceding pages in a figure for the first time. For readers who have read the text of this framework from the beginning, however, it is not clear which case the figure illustrates. In addition, many components and layers overlap, making it difficult to understand. I suggest improving this figure by adding descriptions, etc. One option may be using the classifications in “Table 2.1-1” (p.28) to describe “Figure 1.2-4”.	We used your comments as a reference in revising the content. Relevant part : Part I 2.2.
8	2	Group	Table 2.1-1	With regard to “Targets of analysis” of “The Third Layer (Connections in cyberspace)”, the current description of the third layer seems to be focused on “connections across organizations”, but, considering the content of this framework, “data exchange (connection) within the organization” is also considered to fall under this layer. However, “data exchange within the organization” is currently organized as a component related to the first layer in this Table. It is therefore considered necessary to check the overall consistency and review the descriptions to avoid any misunderstanding. One option may be amending to read “across organizations and within the organization…”, etc.	We used your comments as a reference in revising the content. Relevant part : Table 2.1-1
8	3	Group	Appendix A	When compared to the use cases of other sectors and simplified model of “Figure 2.1-5” in the main text, it appears that for the building sector: ・[on page 8 of Use case] The approach used for placing the elements is different from that of other sectors ・[on page 9 of Use case] Classification of elements is different from what is in the figure on page 8 (For example, servers and integrated network as organized as components related to the third layer on page 9 of while they are mainly placed in the second layer in the figure on page 8) In this framework, elements are defined to have functions of multiple layers, and therefore it is understandable that a case can be different from the cases of other sectors depending on how the viewpoint is placed in each sector. However, since many readers refer to the use cases intending to get the concrete image, I suggest enhancing the figure by describing the characteristics and points of the case.	We used your comments as a reference in revising the content. Relevant part : Appendix A Use Case 5
9	1	Individuals	p.19	It seems better to add more roles and functions to be protected to each layer with an emphasis on connections between layers. More concretely, in the first layer, securing the trustworthiness of each organization itself has been necessary even in the past, and I would like to suggest adding generation of transcription source data to the functions. In the second layer, the functions should include, in addition to data transcription, proving/ensuring that the organization in the first layer and the data in the third layer point to the same object. In the third layer, since impersonation and fraudulent parties are considered as security incidents and risk sources, I believe that authenticating the communication destination or proving itself as communication source should also be considered as a function.	We used your comments as a reference in revising the content. Relevant part : Figure 1.3-1
10	1	Corporation	Appendix C	Declaration of "SECURITY ACTION" should be added in the selection and evaluation of business partners in the supply chain. ・Reason For small and medium-sized enterprises, implementing various types of authentications can be a great burden, and thus security action should also be utilized in CPS.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.SC-3 Basic

ID	No	Affiliation	Place	Comments	Responses to Comments
10	2	Corporation		In order to support the selection and evaluation of business partners in the supply chain as provided in the Cyber-physical Security Measures Framework (hereinafter referred to as “CPS”), examples of measures (BASIC) in CPS should be added to “Appendix 6 Information security related rules (sample)”. Of the examples of measures in “Appendix 6 Information security related rules (sample)”, measure requirement IDs to be considered are as follows. CPS.BE-1 (Basic) CPS.SC-5 (Basic) Add “SECURY ACTION declaration has been conducted” to the evaluation criteria In addition to the above, enterprises using IoT should provide the following measures in the security action declaration. (1) Requirements for IoT devices: CPS.AC-8 (2) Life cycle management of IoT devices: CPS.RA-4, RA-6, RP-1, SC-2, DS-12 • Reason Responding to the requirements and evaluation items for small and medium-sized business partners for each orderer can be a burden for the business partners. In addition, standardizing the evaluation criteria to a certain extent is also considered to be an advantage to orders.	We will use your comments as a reference in advancing security action in the future.
11	1	Group	Appendix A	The current use cases include examples of car, smart home, building, and electric power system, but no example of the distribution sector. Since the supply chain needs to be handled with distribution included, an example in the mail order (mainly e-commerce) sector, which is particularly dependent on the Internet, within the distribution sector should be added in “use cases” and “examples of security measures that meet the measure requirements”.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
11	2	Group		As illustrated in the following examples, the environment surrounding mail order is quite dynamic and closely related to the Internet, and thus cyber security is becoming more complex. • Transmission and use of information both from cyber and physical directions due to the advancement of omnichannel • Automation of e-commerce using IoT • Cases where information originated from third parties is provided in the cyberspace • Use of IoT in the fulfillment of logistics, etc. • Expansion of cross-border EC and responding to the EU General Data Protection Regulation • Transactions using virtual currency • Authentication using block chain • Emergence of platformers and regulations We have been making continued efforts, in cooperation with practitioners and specialists such as lawyers and consultants, etc., in studies on omnichannel (2014-2015) and studies on labeling risk management (2016-17), etc. We would like to request exchange of information on “The Cyber/Physical Security Framework (Draft)” that is considered to have a significant impact on the mail order sector. • Reason “The Cyber/Physical Security Framework (Draft)” surpasses the scope of security framework and covers the trustworthiness of the information provided in cyberspace and the information provided and shared between enterprises as well as the trustworthiness of the supply chain. For this reason, it is considered to provide the basic concept that will be the basis of various measures for communications and transactions in cyberspace and physical space. For information security management, many mail order companies refer to the privacy mark and the ISO 27000 family of standards, but they are expected to be required to respond to even broader matters with “The Cyber/Physical Security Framework (Draft)”. In order to enable many mail order companies, including small and medium-sized enterprises, to readily utilize “The Cyber/Physical Security	We would like to exchange information with various stakeholders when considering specific use cases and security measure requirements in each industrial field.

ID	No	Affiliation	Place	Comments	Responses to Comments
12	1	Individuals		Thee layer model There seems to be an inconsistency when three layers are viewed in their entirety. The first layer is defined to be a layer in which security is ensured by ISMS of the organization such as companies, but there are some areas in the cyberspace in the third layer that are managed by the organization. Therefore, the third layer must contain the first layer. In other words, the first layer and the third layer are not separated. Since the second layer is defined to be a layer of the transcription function connecting physical space and cyberspace, the first layer is deemed to be physical space. Therefore, it is considered appropriate to define the first layer to be physical space, with the definitions of the second and third layers unchanged. Even in this case, each layer contains both areas that can and cannot be managed by the organization, and therefore the concept of the first layer of this document can be utilized. That is to say, it is considered appropriate to change the definition of the first layer, and reconfigure the model to have security management within the organization and responses to the areas not covered by the organization's security management in each layer. "Connections between organizations" on page 11, etc. should also be replaced with "connections between physical spaces".	In Society 5.0, supply chain is transforming from linear and fixed style to non-linear and flexible style. We defined this Society 5.0's new supply chain as "value creation process". Three layers' model would be useful to articulate and control complicated risks of the new supply chain, "value creation process". The first layer is "Connections between organizations". Regarding your commnents, we leave the contents as original.
12	2	Individuals	p.5, p.22, p.44	Of "concept", "policy", and "method", the meaning of "concept" can basically be understood. However, what "policy" and "method" refers to cannot be understood by even after reading the main text. Excluding the three terms listed above, the titles of Parts I through III can be understood. The meaning of "policy" in the title of Part II is unclear. The measure requirements can be considered to be a policy, but "Identification of risk sources and measure requirements" is not a policy. Part II can also be considered to be a method, and what "method" actually means is unclear. Proposed amendment: Delete "Concept", "Policy", and "Method" from the titles of Parts I through III.	We used your comments as a reference in revising the content. Relevant part : Introduction 5.
12	3	Individuals	p.6	iii. It realizes international harmonization The content here describes the state immediately prior to achieving international harmonization. Proposed amendment: It is considered appropriate to replace it with "It ensures consistency with standards in foreign countries".	We used your comments as a reference in revising the content. Relevant part : Introduction 6.
12	4	Individuals	7.(1)	(1) Identifying the risk sources The term "basis of trustworthiness" is defined in Glossary to be the established point to confirm that entity trustworthiness is ensured, but the meaning of "established point" is unclear. In the main text, management, functions, and data are listed as the basis of trustworthiness. In addition, it is questionable whether it is appropriate to limit the trustworthiness to entities. For example, process trustworthiness can also be considered to be covered by this document. Would this still be OK because the definition of entity includes software? In the definition, entity is regarded as goods that include software, but "process" mentioned above means an act, and therefore it is considered inadequate. However, if we were to consider that the trustworthiness of process itself does not matter because the trustworthiness of entity that executes the process includes the process trustworthiness, limiting to entity trustworthiness can be acceptable. Proposed amendment: Procedures, data, or collections thereof that will be the basis for determining the trustworthiness of entities and processes	We used your comments as a reference in revising the content. Relevant part : Appendix E
12	5	Individuals	7.(3)	(3) Building a trustworthy chain among each enterprise etc. and industry Unlike other parts of "7. How to use the Framework", this part describes future activities, not how to use. Proposed amendment: Add a new part "8. Future activities based on the Framework", or make this part a note within 7. Or add "(future activities)" to the end of the title for (3).	We used your comments as a reference in revising the content. Relevant part : Introduction 7.(3)
12	6	Individuals	Part I 1.	The meaning of "linear" is unclear. Proposed amendment: Delete it.	We used your comments as a reference in revising the content. Relevant part : Part I 1.

ID	No	Affiliation	Place	Comments	Responses to Comments
12	7	Individuals	Part I 1.	In the conventional supply chain trustworthiness, security management was also considered to some extent (e.g. cloud services and data center usage, software development outsourcing cases, etc.), but more emphasis was placed on ISO 9000. Although the scope of “the conventional supply chain” is unclear, in the cases of simply exchanging data, whether the partner company has obtained ISMS certification has not been an issue. Proposed amendment: Replace the first paragraph with the following. In conventional supply chain models, security measures are based on the idea that trustworthiness of the supply chain is ensured if the organizational governance and management of the participating entities is reliable. In cases where part of information processing in the supply chain is outsourced to data centers or cloud services, the overall process security can be ensured with outsourcing business partners that thoroughly take security measures such as ISMS and have obtained certification. This means that the basis for ensuring security was based on the trustworthiness of the organization’s management. Information processing mentioned above, however, did not include the latter cases but was limited to typical ones.	We used your comments as a reference in revising the content. Relevant part : Part I 1.
12	8	Individuals	Part I 2.	In the phrase “it is likely to miss essential points for the value creation process protection through the way to fixedly recognise risks on business assets”, the meanings of “fixedly recognise risks on business assets” and “essential points for the value creation process protection” are difficult to understand. Proposed amendment: assuming that business assets belong to fixed organizations does not enable appropriately response to risk sources and is likely to result in missing essential protection in each value creation process.	We used your comments as a reference in revising the content. Relevant part : Part I 2.
12	9	Individuals	Part I 2.1	2.1. Significance of the three-layer approach Approach is not presented, and significance is not described. This part only introduces the three-layer model and its elements. In addition, it is described at the end the first paragraph that “the three-layer approach presented here is a model for appropriately establishing the basis of trustworthiness”, but approach and model are different. I suppose that the approach is to take security measures based on the three-layer model, but cannot find such description. Proposed amendment: Replace the title of 2.1 with “Three-layer model and its elements”. If “three-layer approach” is to be used, the content of the approach must clearly be stated. Please consider how to deal with this for the entire document.	We used your comments as a reference in revising the content. Relevant part : Part I 2.1.
12	10	Individuals	Part I 2.1	In the description “the data exchange between both space, is required to have high accuracy. In other words, the trustworthiness of the value creation process is not ensured unless ensuring the accuracy of transcription and translation”, leaving aside “transcription”, “translation” does not necessarily involve “accuracy”. Therefore, the descriptions are incorrect. Proposed amendment: Replace it with “the trustworthiness of the value creation process is not ensured unless the data exchange between both space (hereinafter referred to as ‘transcription’) is ensured”.	We used your comments as a reference in revising the content. Relevant part : Part I 2.1.
12	11	Individuals	Table 1.2-1	Shouldn’t organizations that have different policies within the company or organization be treated as “organizations”? Both “procedures” implemented by system and by people are considered to exist. The scope is unclear. Proposed amendment: Clarify the definitions. For “organization”, if organizations such as those mentioned above need to be included, the definition should be “extents that share the same security policy in companies and organizations that compose value creation processes”.	We used your comments as a reference in revising the content. Relevant part : Table 1.2-1
12	12	Individuals	Part I 3.	The meaning of “using the three-layers and the six elements” is unclear. I believe that the approach is to “identify” and “develop”, but not to “use”. Proposed amendment: Replace it with “based on the three-layers and the six elements”.	We revised the content as suggested in your comments. Relevant part : Part I 3.
12	13	Individuals	Part I 3.	The meaning of multi-stakeholder approach is unclear. Proposed amendment: Replace “A multi-stakeholder approach is required” with “In this document, making efforts toward security measures by parties directly/indirectly involved as a whole is referred to as ‘multi-stakeholder approach’”.	We revised the content, taking into account your comments. Relevant part : Part I 3.

ID	No	Affiliation	Place	Comments	Responses to Comments
12	14	Individuals	Part I 4.	Despite the title “4. Concepts of securing trustworthiness in the Framework”, what is described in 4. is not included in the framework. Proposed amendment: Replace it with “Concept of securing trustworthiness based on the Framework” or “Future efforts”.	We revised the content, taking into account your comments. Relevant part : Part I 4.
12	15	Individuals	Part I 4.	Use a different notation for “Ex.”.	We used your comments as a reference in revising the content. Relevant part : (Japanese) Part I 4.
12	16	Individuals	Figure 1.4-1	The relationship between the figures on the right and the left is unknown. Proposed amendment: Add descriptions.	We revised the content, taking into account your comments. Relevant part : Figure 1.4-1
12	17	Individuals	Part II	In the first sentence of the first paragraph, “organized” should be “determined”.	We used your comments as a reference in revising the content. Relevant part : Part II
12	18	Individuals	Part II 1. ②	ii. The notation “and,” is uncommon. It is more common not to place a punctuation mark before and after “and”, or if a punctuation mark is to be placed, it should be placed before “and”. Proposed amendment: Remove the punctuation mark (comma).	We revised the content as suggested in your comments. Relevant part : (Japanese) Part II 1.②
12	19	Individuals	Part II 1.	In the second paragraph, the grounds for regarding i. through iv. as points to note are not described. The third sentence mentions “implementation” but that is not the grounds. The grounds seemed to be described on page 29 and beyond, and therefore those descriptions should also be used here. Proposed amendment: Add “The grounds that the following four points should be taken into consideration are described in 1.1 (2)” to the end of the first paragraph.	We revised the content, taking into account your comments. Relevant part : Part II 1.
12	20	Individuals	Part II 1. 1.(1)	In “characteristics and functions/roles of each layer”, the meaning of the term “functions” here seems to be different from that of functions in a general sense. For this reason, this sentence is difficult to correctly understand. The term is considered to mean functions to be performed for the characteristics of each layer. In “The scope of analysis and assets will be organized”, the meaning of “organized” is unclear. Proposed amendment: Replace “characteristics and functions/roles of each layer” with “characteristics and functions/roles to be performed/played for those characteristics of each layer”. Replace “The scope of analysis and assets will be organized” with “The scope of analysis will be determined and assets will be classified”.	We revised the content, taking into account your comments. Relevant part : Part II 1.1.(1)
12	21	Individuals	Part II 1. 1.(1)	In “All components to be managed are included in the first layer”, the expression “components to be managed” appears here for the first time. I believe this should be “components to be analyzed”. The expression “zone” also appears here, but seems to mean nothing special. The expression “it is appropriate” at the end should explicitly state the necessity. Proposed amendment: Replace the paragraph concerned with the following. All components to be analyzed are included in the first layer. However, those having functions of the second layer and the third layer need to be analyzed as components related to these layers. In addition, it must be noted that components having functions of both the second layer and the third layer need to be analyzed in both of these layers. When doing so, zones where components and systems are set and zones where people are required to follow certain procedures also need to be discussed, in light of functions, in risk assessment.	We revised the content, taking into account your comments. Relevant part : Part II 1.1.(1)

ID	No	Affiliation	Place	Comments	Responses to Comments
12	22	Individuals	Table 2.1-1	(1) In the “Concrete image of targets” column, “targets” here refer to targets of analysis. The indented descriptions in the column “Characteristics” are considered to describe sub-characteristics, but there is only one sub-characteristic in the first layer. Therefore, the characteristics here are not actually broken up, and the descriptions of the sub-characteristics are almost the same as the descriptions of the characteristics. (2) In the “Targets of analysis” column, it is desirable to have the definition of “transcription function”. (3) “Controlling components and displaying visualized data based on data received from cyberspace in accordance with certain rules” is considered to indicate inverse transformation of the transcription function. They are not corresponding, however, because the output of inverse transformation is larger than the input area of the transcription function (physical space) (data visualization is considered to be a closed process within the first layer). In addition, a name is needed or this inverse transformation, but “transcription function” should not be used in the name. (4) In the “Concrete image of targets” column, the images of both the transcription function and the inverse transformation function are mixed. 3D printer only has the inverse transformation function. Proposed amendment: (1) Replace “Concrete image of targets” with “Concrete image of targets of analysis”. Delete the sub-characteristic of the first layer. (2) For the second layer, replace “translating” in the first item of the “Targets of analysis” column with “translating (transcription function)”, and replace “transcribing function” in the “Concrete image of targets” column with “transcription function” (3) Replace “displaying visualized data” with an example of output to the physical space. When giving a name to inverse transformation, “materialization function” would be a candidate. With the addition of a new name, make necessary changes to the descriptions in the “Targets of analysis” column. (4) Separate the images for the transcription function and the inverse transformation function.	(1), (2) We used your comments as a reference in revising the content. Relevant part : Table 2.1-1 (3),(4) Regarding your commnents, we leave the contents as original since.
12	23	Individuals	Figure 2.1-3	The Figure is said to show “relationship of the target of analysis and assets in the first layer”, but how it is expressed is unclear.	We used your comments as a reference in revising the content. Relevant part : Figure 2.1-3, 2.1-4, 2.1-5
12	24	Individuals	Part II 1. 4.	Both IEC TR 63074 and IEC TR 63069 are mentioned, but, from the descriptions on page 45-46, security measures may affect safety, and therefore the latter is considered more appropriate. Proposed amendment: None.	Regarding your commnents, we leave the contents as original.
12	25	Individuals	Table 2.2-1	Without vulnerability, there will be no threat, and incidents occur when a threat is realized. Proposed amendment: Change the order of the columns in the table to: Vulnerability, Threat, and then Assumed Security incidents.	Regarding your commnents, we leave the contents as original.
12	26	Individuals	Part III 1.(1)	The sentence “For (i), …” is too long and hard to understand. Proposed amendment: Replacing it with the following. (1) For (i), security measures and measure requirements are summarized in Appendix C to help enterprises to decide on the level of security measures to be implemented. Examples of security measures are classified into three levels, namely High Advanced, Advanced, and Basic, so that enterprises can select security measures, after referring to various domestic/international guideline documents, etc., based on the classification on these documents, taking into consideration the viewpoints such as the scope of the measure (e.g., implementation only within the organization, or involving other relevant organizations) and relative costs for implementing/taking measures, etc.	We revised the content, taking into account your comments. Relevant part : Part III 1.

ID	No	Affiliation	Place	Comments	Responses to Comments
12	27	Individuals	Table 3.3-1	Category names can be improved, and life cycle is not considered in the ordering of categories. As a result, the relationship between “Risk Management Strategy” and “Supply Chain Risk Management” cannot be understood. The content of “Protection Technology” is unclear, and because of this, it seems to overlap with “Authentication, and Access Control” and “Data Security”. What “Communication” and “Mitigation” mean is unclear and vague. In addition, life cycle is not considered also in part of the ordering of measures requirements for each category as described later, making it difficult for readers to understand. Proposed amendment: Use the following ordering. “Asset Management”, “Business Environment”, “Governance”, “Risk Management Strategy”, “Risk Assessment”, “Supply Chain Risk Management”, “Awareness Improvement and Training”, “Identity Management, Authentication, and Access Control”, “Data Security”, “Protection Technology”, “Maintenance”, “Processes and Procedures to Protect Information”, “Continuous Monitoring of Security”, “Detection Process”, “Abnormal Activities and Events”, “Response Plan”, “Communication”, “Analysis”, “Mitigation”, and then “Improvement” List measure requirements for each category in the order with consideration given to life cycle.	The order of categories is considered in harmonization with NIST "Framework for Improving Critical Infrastructure Cybersecurity" as a reference. Therefore, about the order of categories, we leave the contents as origina. In addition, with regard to the order of measures requirements in the category, we used your comments as a reference in revising the content.
12	28	Individuals	CPS.AM-6	Who are relevant parties? Are they different from stakeholders? In addition, why do they need to be communicated? Depending on who relevant parties are, the description seems overly detailed. I believe that it suffices just to share (assuming that “share” means to inform of the existence and “communicate” means to inform of the existence and the content as well). Proposed amendment: Modify the description based on the points above.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-6
12	29	Individuals	CPS.RM-1	Replace “relevant parties” with “stakeholders” or “other relevant systems”.	We used your comments as a reference in revising the content. Relevant part : Part III 3.5. CPS.RM-1
12	30	Individuals	CPS.AT-2	The requirements may be too much for some “relevant parties”. Proposed amendment: Modify the description so that the requirements will not be too much.	We revised the content, taking into account your comments. Relevant part : Part III 3.8. CPS.AT-2
12	31	Individuals	CPS.IP-3	The measure requirements described here are meta level measure requirements, and are at the level different from other measure requirements. These requirements correspond to the entire measure requirements. Proposed amendment: Delete it.	We used your comments as a reference in revising the content. Relevant part : Part III 3.10.
12	32	Individuals	CPS.IP-4 CPS.IP-7 CPS.IP-9 CPS.AE-4	Change the wording at the end of the sentence in Japanese in CPS.IP-4, CPS.IP-7, CPS.AE-4. The same is applicable for CPS.IP-9.	We revised the content as suggested in your comments. Relevant part : Part III 3.10.
12	33	Individuals	CPS.IP-10	What is a "vulnerability management plan"? Proposed change: Add an explanation for "vulnerability management plan".	We revised the content, taking into account your comments. Relevant part : Part III 3.10. , Appendix E
12	34	Individuals	CPS.MA-2	It is not clearly defined whose "approval" is required.	We revised the content, taking into account your comments. Relevant part : Part III 3.11.
13	1	Corporation	Appendix B	With regard to "3_3 Functions to securely send and receive data", CPS.MA-1 appears two times in Measure Requirements for L3_3_a_SYS. The first MA-1 may be unnecessary. (MA-1 and MA-2 appear sequentially later.)	We revised the content as suggested in your comments. Relevant part : Appendix B
14	1	Individuals	CPS.SC-7	Change "with other relevant parties (omitting the rest)" to "with other relevant parties and individuals" to explicitly state the necessity of information disclosure to individuals. Besides the above, clearly define possible cases for individuals regarding data transfer between an organization and an individual. ・Reason As shown in Use case #4: Smart home in Appendix A, data transfer between an organization and an individual is also included in the scope of the framework.	We revised the content, taking into account your comments. Relevant part : Part III 3.6. CPS.SC-7

ID	No	Affiliation	Place	Comments	Responses to Comments
14	2	Individuals	CPS.RP	Add a suggestion for making a plan for disposal of data when business continuity is interrupted. ・Reason Interrupted business continuity makes subsequent analysis and improvement impossible, and after dissolution of the organization, data administrator may be absent, which differs from when the organization exists and also may lead to confusion and higher risk of information leakage.	Regarding your commnents, we leave the contents as original.
15	1	Corporation		Currently video and audio data is in a digital format and distributed over the network including the internet. Normally the copyright of media data including commercial video and audio data (e.g. movie and music) is owned by the copyright holder and has been protected by enabling such data to be viewed or listened only by specific consumers authorized by the copyright holder, using encryption and authentication technologies in addition to DRM(Digital Rights Management). According to technological progress like AI, however, completely different attacks from the previous ones have been increasing. One of these attacks is information falsification that is called Deepfake in some fields. (News for reference): http://www.niemanlab.org/2018/11/how-the-wall-street-journal-is-preparing-its-journalists-to-detect-deepfakes/ As the use of Deepfake spreads like this, it will become very difficult to figure out whether the media data is real or not. For a familiar example, currently photos and video data captured by security cameras can be used as evidence for crimes, due to developed Deepfake, however, it will become difficult to tell if the video or audio data is real or fake, and it will also become difficult to determine the value of such data as evidence in accordance with the development of AI. It is easily to imagine that the technology like this can facilitate media manipulation using fake news by means of images of the prime minister or president. Years ago the news sources were limited to terrestrial broadcasting but nowadays a wide variety of information is distributed via the network, which makes it more difficult to identify the information sources, leading to easier to spread fake news.	Securing the trustworthiness of the data itself is recognized as an important issue for the realization of "Society 5.0", and the framework also describes measure requirements (CPS.GV-3, CPS.SC-7, CPS.CM-4, etc.) . In order to promote the framework in actual industrial activities, security measures according to the classification of the data to be handled, and confirmation methods such as data integrity and authenticity are also required. We will use your comments as a reference in advancing security measures for data.

ID	No	Affiliation	Place	Comments	Responses to Comments
				If AI enables Deepfake, it is AI to detect it, which can be used as a measure but has some issues. First, every time AI algorithm for creating new Deepfakes is developed, fake detection AI needs to be adapted to it, causing a time lag until adaptation, which cannot prevent so-called zero-day attacks. Secondly the issue is when any data using Deepfake is delivered from various types of internet sources, how to completely check the data with AI before the data is seen or heard by viewers or listeners. This may be possible with AI by thoroughly checking all media data that can be found by crawling the internet, this, however, seems to be not realistic in consideration of the scale of the internet. From a possible different perspective, there is an approach to create a database for checking the authenticity of information, which provides viewers and listeners with a means to determine the authenticity of media data on their own by making inquiry to the database when they view or listen to the media data. Registering the person in charge of processing the media data, processing method and information of the output media into the database in a safe manner in different phases in which the media data is processed helps viewers and listeners determine the authenticity of the media data when they use it, for example, by clearly identifying the camera used for capturing the media data and then which image processing software was used for modifying the data. In order to create a database like this, taking the above as an example, it is required to securely receive data from the camera and image processing software and to store the received data in the database together with information on the date/time of receipt, and if any inquiry is made by a viewer/listener, to securely provide him/her with information immediately upon his/her inquiry. A very complex design and system scalability seem necessary to construct a large-scale system like this, actually, however, the blockchain mechanism can be used. That is, using blockchain instead of the above mentioned database can store the information input in it in a secure manner and strongly prevent the previous information from being falsified in a cryptographic manner because of the nature of Blockchain. In addition, as blockchain has a high scalability to encourage the development of virtual currency, its mechanism is useful. The blockchain mechanism developed and used based on various R&Ds on the back of the boom of cryptocurrencies can provide highly advanced features even in an environment where the authenticity of media data needs to be determined such as that where Deepfakes are becoming hard to distinguish from reality.	
16	1	Individuals	3.	As the description seems to be based on Stuxnet, it may be better to mention that the generalization/standardization of parts or communications for control systems is one of the factors. In this case, it is close to Charles Perrow's "Normal Accident" Theory. [Original] Because of the downsizing and higher functionality of IT devices, even if the system is recognized as "unnetworked and unconnected to the internet", all systems including electronic devices have grown in importance with increasing concerns about possible cyber attacks through the physical space; therefore we need to take necessary security measures based on recognition that electronic devices and systems owned can be included in the applicable scope of this framework. [Proposal for revision] Because of the generalization and standardization of proprietary electronic devices and communication protocols used in the system, even if the system is recognized as "unnetworked and unconnected to the internet", the devices seamlessly communicate with each other, leading to improved convenience while even a small incident can easily affect the entire system with increasing concerns about possible cyber attacks through the physical space; therefore we need to take necessary security measures based on recognition that electronic devices and systems owned can be included in the applicable scope of this framework.	We revised the content, taking into account your comments. Relevant part : Introduction 3.
16	2	Individuals	p.22	There is no problem with daring to use JIS Q 31000:2010, however the latest risk management standard is JIS Q 31000:2019 (ISO 31000:2018), while in the process diagram, "Establish the context" is changed to "Applicable scope, situations and standards" and "Preparing records and making reports" is newly added. The standard published nine years ago is too old to be referenced even though JIS Q 31000:2019 has been currently available.	We revised the content, taking into account your comments. Relevant part : Part II , Figure 2.1-1

ID	No	Affiliation	Place	Comments	Responses to Comments
16	3	Individuals	p.22~23	There is a large gap in relation between risk management process and steps. Describe both in the same manner. In addition, the description here is not sufficient because in “Risk Assessment Guide for Industrial Control Systems Version 2” (IPA), not only "imaginable attack scenarios“ (i.e. business damage-based risk analysis?) but also "asset-based risk analysis” are mentioned. There is no need, of course, to give a full description here, and giving an example of "imaginable attack scenarios“ (being aware of risk identification, analysis and evaluation combining Fault Tree with Attack Tree, if possible) can make improvements in this description. [Proposal for revision] The following shows an example of the process in security risk management: ■ "Establish the context" (or "Scope, situations and standards") 1 Specifying the target of analysis (1.1) - The original remains unchanged - 2 Defining assumed security incident and business damage level (1.2) - The original remains unchanged - ■Risk assessment [Risk identification; Risk analysis; Risk evaluation] 3 Analyzing risks (1.3) - The original remains unchanged - ■Risk management 4 Managing risks (1.4) - The original remains unchanged -	As described in Fig. 2.1-2, in part II of this framework, the risk analysis based on business damage is described as an example. Regarding asset-based methods as well, we believe that it is necessary to examine the way of analysis in Society 5.0 in which products and systems can be flexibly connected. We will revise the correspondence with the steps of ISO 31000 , taking into account your comments.
16	4	Individuals	p.36	"Risk aversion, reduction, transfer, or retention" in "1.4. Managing Risks" is the concept of JISQ2001:2001 that was published 18 years ago and is too old. The following seven risk management options are identified in JIS Q31000:2019. We propose to change the description here to either of the following: "Break seven options down into four categories, resulting in aversion, reduction, transfer, or retention" to show that the old concept is not directly used; or replace with the latest seven options. ・Avoid risks by determining not to start or engage in the activities that would produce the risk. ・Take or increase risks to pursue an opportunity. ・Reduce risk sources. ・Change the likelihood of the occurrence. ・Change consequences. ・Share risks (e.g. by entering into an agreement or buying insurance). ・Retain risks by making decisions based on information.	We revised the content, taking into account your comments. Relevant part : Part II 1. , 1.4.
16	5	Individuals	p.39	"IEC TR 63074 (Security measures for existing safety-related control systems/TC44)" for machinery safety (on the IEC side) and TR63069 (Safety and security analysis/treatment in general control systems/TC65)" for control system safety have yet to be published while "ISO TR22100-4:2018 (Guidance and consideration of related security aspects/TC199) for machinery safety (on the ISO side) has already been published, which may need to be mentioned.	We used your comments as a reference in revising the content. Relevant part : Part II 1. , 1.4. Figure 2.1-9
17	1	Government Agency	p.1-4	The need of an overall measure to achieve security is highlited very well.	Your comments are considered as positive feedback on this framework.
17	2	Government Agency	Part I: 2.	The data generated by automated analysis can also be used to optimize processes.	Automatic analysis of various data and process optimization based on the results is one of the forms of industrial activity in the ultra-smart society that Society 5.0 is aiming for.
17	3	Government Agency	Part I: 2.	Why is it likely to miss essential points due to a dynamical and flexible value creation process?	Because the value creation process is dynamic and flexible, the elements involved in the value creation process change according to the purpose and necessity of the current activity, and it is difficult to take security measures that capture the elements in a fixed manner.
17	4	Government Agency	Figure 1.3-1	How could this overview be applied to identify the risk sources?	Figure 1.3-1 shows the outline of security measures in each layer, and the identification of risk sources is described in Part II.

ID	No	Affiliation	Place	Comments	Responses to Comments
17	5	Government Agency	Figure 1.4-1	Is the creation of trust regarding the components somehow associated with the policy for a secure product development process?	As described in Part II 1.4. "Implementing risk response", in order to create and maintain trust in Components, security measures through the life cycle of Components from design, procurement, operation to disposal are important. We recognize that the secure product development process that you point out is an important part of it.
17	6	Government Agency	Part II	Are the interfaces to the environment also included regarding the scope of the analysis?	We recognize that it is included in the scope of analysis. We used your comments as a reference in revising the content.
17	7	Government Agency	Figure 2.1-9	There might be assets which are security relevant, but not safety relevant.	As you pointed out, there are assets that have little relation to the issue of safety. Therefore, risk assessment is carried out at the time of planning or procurement of equipment and system. Based on the results, we believe it is necessary to implement safety measures.
17	8	Government Agency	Part III	Part III is very helpful for the implementation of measures.	Your comments are considered as positive feedback on this framework.
18	1	Corporation	4.	The (smart) products produced are to be used by human end users. Representatives of their interest gropus should also be intended readers	We used your comments as a reference in revising the content. Relevant part : Introduction 4.
18	2	Corporation	Part I	The framework covers relationships between organizations. Data is however not only shared between organizations, there is/will be data exchange with consumer equipment installed at the customer premises. This challenges posed are only partly mentioned/addressed	In Society 5.0, data distribution among various organaizations and people are increasing. Therefore, in the third layer, the basis of trustworthiness is defined as data, and people who does not belong to an organization is also included in the scope, and the security requirements are described.
18	3	Corporation	Figure 1.4-2	This picture shows a “user”. Is this meant to be a consumer? Is he required to buy/rely on managed security services?	We revised the content, taking into account your comments. Relevant part : Figure 1.4-2
18	4	Corporation	Appndix. A #1	This picture depicts “Connections of components…” and seems to address end user equipment at least in the “smart home” application. How are these IoT-Devices addressed in the framework?	When viewed as a device that has a transcription function, it is the second layer, and when viewed as an end user-managed device, it is the first layer. Determine what should be dealt with from the security incidents assumed in each layer.
18	5	Corporation	Appndix. A #4	End user equipment (“Residents”) is shown. What concept shall apply for the security management at the end user/consumer premises?	End users are recognized as important stakeholders in this framework as well. However, because it is difficult for end users to demand sufficient security measures, it is important for stakeholders who provide components and services to end users to implement security measures.
19	1	Corporation	Part I: 2.1	(Editorial)Current sentence: ...it is necessary to introduce other types of the basis of trustworthiness and to secure the basises. Proposed edit: …it is necessary to introduce additional types of bases for trustworthiness and to secure them.	We revised the content as suggested in your comments. Relevant part : (English) Part I 2.1.
19	2	Corporation	Part I: 2.1	(Editorial)current sentence: In other words, the trustworthiness of the value creation process is not ensured unless ensureing the accuracy of transcription and translation. Proposed edit: In other words, the trustworthiness of the value creation process is not ensured unless the accuracy of transcription and translation is confirmed.	We revised the content as suggested in your comments. Relevant part : (English) Part I 2.1.
19	3	Corporation	Part I: 2.1	(Editorial) Include space between ‘thedata’	We revised the content as suggested in your comments. Relevant part : (English) Part I 2.1.
19	4	Corporation	Part I: 2.1	(Editorial)current sentence: …where cyber space and physical space become integrated one, security measures… Proposed edit: …where cyber space and physical space are highly integrated, security measures… (Suggestion) Rephrase the entire sentence to : In the value creation process of an industrial society, where cyber space and physical space are highly integrated, security measures corresponding to each of the three layers shall be taken into consideration.	We revised the content as suggested in your comments. Relevant part : (English) Part I 2.1.
19	5	Corporation	Table 1.2-1	Comment: Are ‘customer’ or ‘end consumer’ also considered as part of the value-added chain. In that case, include “customer” and “end consumer”.	The value creation process also includes "consumers" or "final consumers".

ID	No	Affiliation	Place	Comments	Responses to Comments
19	6	Corporation	Table 1.2-1	(Editorial) 1. Remove 'those' from the description of components 2. Within the explanation of 'procedure', archive should be replaced with achieve	We revised the content as suggested in your comments. Relevant part : (English) Table 1.2-1
19	7	Corporation	Part I: 2.2	(Editorial) 1. typing error: 'physcal machines'à 'physical machines' 2. Current sentence: … complexly related each other. Proposed edit: … complexly related to each other.	We revised the content as suggested in your comments. Relevant part : (English) Part I 2.2.
19	8	Corporation	Part I : 3	(Editorial) 1. typing error: 'developped'à 'developed'	We revised the content as suggested in your comments. Relevant part : (English) Part I 3.
19	9	Corporation	Figure 1.3-1	I cannot understand: Second Layer-security incident states 'operation with safety problems'. Additionally, 'unavailability of data' can also be a security incident. For example, a denial of service attack that blocks transmission of readings from the physical system to the cyberspace	Regarding your commnents, we leave the contents as original.
19	10	Corporation	Part I: 4	The concept of creation of trust, proof of trust and maintenance of chain of trust has been devised very clearly.	Your comments are considered as positive feedback on this framework.
19	11	Corporation	Part I: 4	(Editorial)current sentence: '…to preserve above records' Proposed edit: ' …to preserve previous records' or 'preserve historical data'. Comment: How is this part of creation of trust?	We used your comments as a reference in revising the content. Relevant part : (English) Part I 4.
19	12	Corporation	Part I: 4	(Editorial)current sentence: To create and managethe list for… Proposed edit: To create and manage the list for…	We revised the content as suggested in your comments. Relevant part : (English) Part I 4.(2)
19	13	Corporation	Part I: 4	(Editorial)Current sentence: 'To confirm of the trust of components/data by inquiring to the list for trustworthiness.' Proposed edit: 'To confirm the trust of components/data by inquiring to the list of trustworthy entities/assets.' Question: Does this imply that there's always a certifying authority that attests the trustworthiness of components? How will this be realized in the third layer, in which integrity of data is required as an element of trustworthiness?	We used your comments as a reference in revising the content. Relevant part : (English) Part I 4.
19	14	Corporation	Figure 2.1-2	In the first block, I would suggest to replace 'clarifying' with 'identifying' or 'determining'	We revised the content, taking into account your comments. Relevant part : (English) Figure.2.1-2
19	15	Corporation	Part II: 1.1	(Editorial) Typing error: 'implementin' → 'implementing' 'Tagets of analysis' → 'Targets of analysis'	We revised the content as suggested in your comments. Relevant part : (English) Part II 1.1.
19	16	Corporation	Part II	(Editorial) Typing error: 'exxchange' → 'exchange'	We revised the content as suggested in your comments. Relevant part : (English) Part II
19	17	Corporation	Figure 2.1-6	Affect of security breach on safety is depicted very well in the figure. I would suggest to remove 'problems' from the figure title	Regarding your commnents, we leave the contents as original.
19	18	Corporation	Part II	What is 'inappropriate data' referring to? Does it mean refer to illegal information leakage? Or is it inaccurate data, for e.g., via man in middle attack? Suggestion: replace by "unauthorized data"	'inappropriate data" is a file infected with malware, data that has been tampered with on the network, data sent from a spoofed IP address, etc. Regarding your commnents, we leave the contents as original.
19	19	Corporation	Table 2.1-6	Table presents a very comprehensive collection of security incidents in each layer. In 2nd layer, I would propose to add about leakage of data to unauthorized authority. For example, IoT device is corrupted to send data to malicious server, or a backdoor in the CPS system transmits confidential information to the attacker.	Regarding your commnents, we leave the contents as original.
19	20	Corporation	Part II	It is a good idea to mention about security-by-design in the procurement and testing phases of devices present in 2nd layer	Your comments are considered as positive feedback on this framework.
19	21	Corporation	Part II	(Editorial) Typing error: 'tsecurity' → 'security'	We revised the content as suggested in your comments. Relevant part : (English) Part II
19	22	Corporation	Part III	Is there a reason to use the terminology high advanced, advanced and basic instead of "advanced, medium and basic"?	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
19	23	Corporation	Part III	(Editorial)Current sentence: When the organization implements security measures classified as High Advanced, it should also implement the security measures classifed as Advanced and Basic. Message of the sentence is not quite clear. Does this mean that the organization shall have advanced and basic security measures in parallel to high advanced? Multiple security measures for one security risk? Proposed change: When the organization implements security measures classified as “high advanced”, this also should cover the security levels classified as “Advanced and Basic”. (Suggestion)Maybe, also replace classification by “advanced, medium and basic”	We used your comments as a reference in revising the content.
19	24	Corporation	Appendix A Use case #2	We do not understand the wording: “, and supplier pays products…”	We used your comments as a reference in revising the content. Relevant part : Appendix A
19	25	Corporation	Appendix A Use case #3	Use case 3 is a very good idea. And depiction of future connected cars as a value creation process is very impressive	Your comments are considered as positive feedback on this framework.
19	26	Corporation	Appendix D	Suggest to include IEC 62443 wherever it applies	We used your comments as a reference in revising the content. Relevant part : Appendix C
20	1	Corporation	Figure.i-1	In the figure i.1 the invented concept, Society5.0 just demonstrate the benefits of the human user. However it shall tell us, how the connected Industries creates new added value to Society5.0.	Your comments are considered as positive feedback on this framework.
20	2	Corporation	Introduction	compare the given definition of Society5.0 with the CEN/CLC JTC13 WP2019 definition, Digital Society	We will use your comments as a reference in advancing cyber security policies in the future.
20	3	Corporation	Figure.i-2	What kind of changes in the supply chain structure become necessary to create new value in the Society5.0?	Part 1 contains the concept of the new supply chain in Society 5.0.
20	4	Corporation	Table i.1	relate the IoT protection measures of table I.1 to the measures of the IEC 62443 standards series which goes beyond the NIST CRITIS Cyber Security measures. (It is noticed that the CPS FW is planned to be aligned with ISA 62443)	We used your comments as a reference in revising the content. Relevant part : Appendix C
20	5	Corporation		notice ,Supply Chain Risk Management for a global Digital Society is defined in the standard of ISO 27036-3	This framework has been formulating with reference to major international standards. In addition, since new international standards etc. are always established, we will constantly revise it appropriately with reference to various international standards etc. even after it is established, taking into account your comments.
20	6	Corporation	Appendix A	Use Cases of Society5.0 shall be considered more centered in the main sections of the CPS FW!figure i-1	As you stated, I have described it at the beginning of Appendix A Use case.
20	7	Corporation	Appendix D.1	The mapping of the CPS FW Cyber Security Controls shall not be restricted to the NIST Cyber Security Framework Subcategories but also to Digital Society Standards being focused by EU Standardization Organizations, such as CEN/CLC, ISO/IEC 270xx etc.	We will use your comments as a reference in advancing cyber security policies in the future.
20	8	Corporation	Appendix E	Harmonize the glossary definitions with various ISO/IEC Vocabularies from Cloud Computing, Big Data, AI, IoT, IACS etc.	We used your comments as a reference in revising the content.
21	1	Group		Overall, we support METI’s efforts to establish a voluntary, risk-management based framework, and we very much appreciate the willingness of the Government of Japan to consult with industry throughout the drafting process. As noted in our previous comments, we strongly believe that a multi-stakeholder approach to cybersecurity is the most effective way to encourage economic activity while ensuring security, and that effective cybersecurity is fundamental to the resiliency of digital infrastructure, digital trade, and the global value chain.	Your comments are considered as positive feedback on this framework.
21	2	Group		The proposed Framework provides a comprehensive view of the technical considerations for developers in creating secure IoT or cyber/physical solutions. However, as we strongly believe that risk management is foundational to effective cybersecurity, there is a demonstrated need for policies to reflect risk-based approaches and prioritize implementation of risk management processes. Thus, we recommend that the Japanese government endeavor to employ and encourage enterprises to use risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks to detect, respond to, and recover from cybersecurity events. To accomplish this, we believe that the Framework should focus on the assessment and identification of risk, methods for minimizing risk, and the maturity of companies in implementing international best practices.	As you stated, we recognize that the risk-based approach is important and we have adopted it in this framework.
21	3	Group		We also believe that privacy certification schemes play an important role in creating trust with consumers as they use and deploy IoT and cyber/physical systems. To this end, we hope that the framework can better promote a strong culture of protecting data, wherever it is stored, alongside the secure, technical solutions outlined in the framework.	In Soeicty 5.0, the importance of data protection is increasing, and the basis of trustworthiness in the third layer is defined as data, and the measure requirements and security measures are described.

ID	No	Affiliation	Place	Comments	Responses to Comments
21	4	Group		There is broad consensus in industry that a multi-stakeholder framework is a sound baseline for businesses' cyber practices, including in the international realm. We have communicated this to consecutive U.S. 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 also 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 METI to develop a more detailed strategy for how the Ministry will work with their international counterparts and industry to promote interoperability among cyber regulations.	As you stated, we recognize that the multi-stakeholder approach is important and is adopted in this framework. We will constantly revise the framework appropriately with reference to various international standards etc. even after it is established, taking into account your comments.
21	5	Group		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, the Ministry of Internal Affairs and Communications, and the National center of Incident readiness and Strategy for Cybersecurity are approaching industrial cybersecurity. Ensuring that the Government of Japan is coordinated in these approaches will help to mitigate any risks or challenges to the ICT and cybersecurity industry's growth, and help strengthen Japan's overall cyber resiliency.	We will use your comments as a reference in advancing cyber security policies in the future.
22	1	Corporation		The concept of the layers defined dividedly may be understood differently depending on reader's viewpoint, which may cause a gap that does not belong to any layer. Appropriate instruction manuals or guidelines for the definition of layers need to be prepared.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures. We intend to continue to explain such ideas in a more polite manner, and expect various activities to be expanded, such as commentary by those involved in the formulation of this framework.
22	2	Corporation		The requirements defined by the framework and requirements for the standards for reference are well compared with each other, which helps us have a good understanding of the corresponding relation. The framework becomes more easily applicable if differences among the requirements can be identified.	We will use your comments as a reference in advancing cyber security policies in the future.
22	3	Corporation		The content of the framework is a kind of difficult to understand, but new perspectives are added by applying the three-layer approach, while continuing to conform to US standards. We think that it is important how to run and use/develop this framework actually across all industry sectors.	Your comments are considered as positive feedback on this framework. We will use your comments as a reference in advancing cyber security policies in the future.
23	1	Group		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 grateful for METI's leadership in seeking to address security challenges facing industrial supply chains, which are daunting and an increasing focus of policy-makers around the world.	Your comments are considered as positive feedback on this framework.
23	2	Group		The updated draft Framework in 2019 represents a substantial improvement, and we were grateful to see many of our earlier comments taken into consideration. In general, the updated draft provides an important tool to help industry stakeholders assess, manage, and respond to risks across the systems and networks they manage and the supply chains they maintain. We welcome a risk management approach that METI has taken in the framework that would be more effective than a prescriptive regulation approach. It is all the more powerful thanks to its conscious alignment with existing internationally recognized best practices, such as key ISO standards. In our previous comments, we urged METI to align the Cyber/Physical Security Framework with the Framework for Enhancing Critical Infrastructure Cybersecurity, and we are grateful for the updated draft's substantial attention to harmonizing these frameworks. This alignment enables technology developers to adapt approaches to security across international markets, collaborate to address emerging security threats across national boundaries, and build a global workforce trained around common concepts.	Your comments are considered as positive feedback on this framework.
23	3	Group		We continue to caution against adopting a Japan-specific framework to Cyber/Physical Security. We recognize that METI is developing guidance that in some ways goes beyond the current internationally-recognized frameworks by focusing on the integration of IoT with cloud computing. Existing frameworks, such as ISO's work on ISO/IEC 30141:2018 and ISO/IEC 17789:2014 which establish a reference architecture to map the applicability of existing ISO standards to IoT and cloud computing, leave significant gaps in implementation guidance. As such, as the Government of Japan pursues the development and application of the Framework, we urge METI to continually revisit the document to ensure maximum alignment with emerging internationally-recognized standards to avoid inadvertently creating confusion in the industry and undermining the benefits of interoperability with other efforts (e.g. in the United States, the European Union, and elsewhere) to promote IoT security.	This framework has been formulating with reference to major international standards. In addition, since new international standards etc. are always established, we will constantly revise it appropriately with reference to various international standards etc. even after it is established, taking into account your comments.

ID	No	Affiliation	Place	Comments	Responses to Comments
23	4	Group		The model articulated by the draft Framework, identifying three layers (“connections between organizations,” “mutual connections between cyberspace and physical space,” and “connections in cyberspace”) and six elements (people, organizations, systems, components, data, and procedures) provides a useful concept for understanding key actors and relationships in the digital industrial ecosystem. It usefully illustrates where responsibilities and security considerations may overlap, and where they may diverge. Moreover, it prompts cybersecurity personnel to consider resources or relationships in relation to security planning that may not be obvious in the complex ecosystem of modern digital industrial supply chains. The three layers of the model translate usefully into an analytical tool to guide risk management activities, as Appendix A of the draft demonstrates. On the other hand, the six elements will be most useful as an illustrative concept rather than as an analytical tool. We are concerned that, as an analytical tool, the six elements may introduce too much complexity and ambiguity for straightforward application by many cybersecurity professionals. It may be worth considering whether, in Part II particularly, the model can be simplified to help cybersecurity professionals target their limited resources in developing organizational cybersecurity plans and policies.	Your comments are considered as positive feedback on this framework.
23	5	Group	Part III	The Framework is well aligned with internationally recognized best practices and provides broad coverage of considerations critical to securing digital industrial ecosystems and supply chains.	Your comments are considered as positive feedback on this framework.
23	6	Group	CPS.AM	The current draft section on Asset Management importantly includes guidance to maintain inventories of all hardware and software and to create records of information such as production date and condition. It should also include guidance that organizations adopt transparent and verifiable software asset management (SAM) practices to ensure that software is not only inventoried, but also confirmed to be appropriately licensed and up to date. Because unlicensed software is less likely to receive critical security updates that would otherwise mitigate the risks associated with malware exposure, its use heightens the risk of harmful cybersecurity incidents. Unlicensed technology from untrusted sources may also contain embedded malware inserted by malicious actors. We recommend including, after the current CPS.AM-4, a new ID statement: “CPS.AM-X. Apply transparent and verifiable software asset management practices to ensure software is appropriately licensed and up to date.”. The relevant internationally recognized standard is ISO 19770-1.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-1
23	7	Group	CPS.AM-5	The “Guidebook for using Cloud Security Guideline” (METI, 2013) is a useful reference regarding points to consider when stipulating contractual terms regarding the roles and responsibilities of users, especially in terms of using cloud services. The following internationally-recognized standards also useful for this purpose: ・ ISO/IEC 17789:2014, Information technology — Cloud computing — Reference architecture ・ ISO/IEC 19086-1: 2016, ISO/IEC 19086-1:2016, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts ・ ISO/IEC 19086-4: 2019, ISO/IEC 19086-4:2019, Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-7
23	8	Group	CPS.AM-6	While classifying assets according to function, importance, and business value is important to effective asset management, it may make less sense to classify people accordingly. Individuals within an organization can present similar security challenges (e.g., poor cyber hygiene, insider attack) regardless of their comparative importance of business value. We recommend your strike “people,” from the ID statement.	We revised the content, taking into account your comments. Relevant part : Part III 3.1 CPS.AM-6
23	9	Group	CPS.BE-3	This statement appears somewhat redundant of CPS.AM-2. We recommend that you delete CPS.AM-2.	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
23	10	Group	CPS.GV	An essential practice for achieving strong cybersecurity governance is to ensure that cybersecurity information is communicated to an organization's senior leadership, including its corporate officers and its Board of Directors, where relevant. We recommend you add, following CPS.GV-4, a new ID statement: "Establish a process for communicating key information on cybersecurity risk management policies and significant cybersecurity incidents to the organization's senior leadership."	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.GV-1、CPS.RM-1、CPS.RP-1
23	11	Group	CPS.RA-1	It is unclear whether this ID statement calls for a simple assessment and documentation of the aggregate vulnerability and an organization's assets, or if it would call for an assessment and documentation of the individual vulnerabilities. It is important that the recommendation is for the latter, that organizations should identify and document the individual vulnerabilities of their assets.	Regarding your commnents, we leave the contents as original.
23	12	Group	CPS.SC-2	For the purposes of clarity and ease of use, the ID statement should be broken out into several separate statements. Moreover, the draft statement currently provides guidance to use IoT devices certified by a third party or self-attested to be safe and secure; however, it does not link to any sort of standard or benchmark against which IoT devices should be assessed. Absent such a standard or benchmark, certifications or self-attestations may communicate wildly divergent information about the safety and security of an IoT device. We recommend that the draft language on use of certified IoT devices be deferred until future iterations (e.g. when more widely vetted IoT security standards exist), and that the ID statement be reorganized as follows: "CPS.SC-2. Identify, prioritize, and evaluate the relevant parties crucial to sustaining the operation of the organization." "CPS.SC-X. In services and system operations, select service suppliers who efficiently and effectively operate and manage services." "CPS.SC-X. When devices are procured, select suppliers of IoT devices whose management systems are properly established and operated and whose help desks and support systems are well prepared."	We used your comments as a reference in revising the content. Relevant part : Part III 3.6. CPS.SC-2 , Appendix C CPS.SC-2
23	13	Group	CPS.AC-6	We strongly support the use of multi-factor authentication to protect access to networks and other sensitive assets. Recent technological developments have enabled additional risk-based approaches to authentication (such as the use of contextual information like geolocation, device recognition, and pattern analysis), which can often be used in tandem with multi-factor or biometric identification. Therefore, we recommend the ID statement be edited as follows: "Adopt multi-factor authentication, combining more than two types of authentication and/or other risk-based authentication techniques, when logging in to the system over the network for the privileged user."	Regarding your commnents, we leave the contents as original.
23	14	Group	CPS.DS-6	Maintaining software with version upgrades and security patches is critical to both network and IoT security. As such, we recommend devoting a distinct ID statement to this important security measure, as follows: "CPS.DS-6: Carry out periodic quality checks, prepare standby devices and uninterruptible power supplies, provide redundancy, detect failures, and conduct replacement work, and update software for IoT devices, communication devices, circuits, etc. "CPS.DS-X: Ensure software assets, including IoT devices, are maintained with all current upgrades and security patches."	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
23	15	Group	Appendix E	It may be useful for the Framework to refer to the definitions and usage of the following terms found in the relevant ISO international standards. (1) “Actuator” to [SOURCE: ISO/IEC 20924:2018, 3.2.2] (23) “Hash value” to [SOURCE: ISO/IEC 27037:2012, 3.11] (24) “Identifier” to [SOURCE: ISO/IEC 20924:2018, 3.1.21] (28) “IoT(Internet of Things)” to [SOURCE: ISO/IEC 20924:2018, 3.2.1] (29) “IoT device” to [SOURCE: ISO/IEC 20924:2018, 3.2.4] (56) “Sensor” to [SOURCE: ISO/IEC 20924:2018, 3.2.9] (57) “Service” to [SOURCE: ISO/IEC TR 17028:2017, 3.1] (64) “Timestamp” to [SOURCE: ISO/IEC 18014-1:2008, 3.12] (65) “Trustworthiness” to [SOURCE: ISO/IEC 20924:2018, 3.1.32] Also, check “IoT Trustworthiness” to [SOURCE: ISO/IEC 20924:2018, 3.2.10]	We used your comments as a reference in revising the content. Relevant part : Appendix E
24	1	Group		The Internet of Things (IoT) is poised to transform economies and societies worldwide, and is a key building block for Japan’s Society 5.0. The challenges presented by IoT make a collaborative security approach more crucial than ever, and governments around the world have important choices to make to help shape the future of IoT security. We are pleased to see METI recognising the significance of the issue and taking actions to address it using a multistakeholder approach. Specifically, we would like to commend METI for embracing ‘security-by-design’ as a foundational principle to guide enterprises in formulating policies and implementing measures to bolster and reinforce trust in the IoT ecosystem.	Your comments are considered as positive feedback on this framework.
24	2	Group	CPS.AC-1 CPS.AC-4 CPS.AC-6 CPS.AC-8	Authenticate device software updates. The METI Framework directly addresses authentication of users, but does not seem to require authentication of “automatic” software updates for devices. Without this in place, attackers can hijack connections and download malicious software into the IoT devices. (OTA principles 1, 6)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.MA-2
24	3	Group	CPS.AC-1 CPS.AC-4 CPS.AC-6 CPS.AC-8	Authenticate device-to-device communication. Likewise, communication between devices should be authenticated, not just communication between users and devices or devices and servers. (OTA principle 13)	We used your comments as a reference in revising the content. Relevant part : Part III 3.7. CPS.AC-8
24	4	Group	CPS.DS-1 CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-6 CPS.DS-9 CPS.DS-12 CPS.DS-13 CPS.MA-1	Ensure that control software is secure, updated and encrypted. The METI Framework explicitly calls out software updates, audits, and encryption for devices, servers and their communication, but it does not appear to mention the device control software, which may be an application running on a mobile device or workstation, or via a web browser. Since a system is only as strong as its weakest link, it is important to consider these controlling applications in all scenarios. It is possible that application of these recommendations to the controlling software is implied, but we suggest that it be made explicit. (OTA principles 1, 2, 3, 6, 7, 8, 13)	Regarding your commnents, we leave the contents as original.
24	5	Group	CPS.IP-1	Specific requirement for strong, unique passwords. The METI Framework highlights an initialization process that would change the default settings, but we believe it is important to take that one step further and ensure that each device or service has a strong, unique password. If this is the case, even if a credential is revealed, the scope of impact is limited. We see that the Framework calls for multi-factor authentication where applicable and agree that this is also a best practice to recommend. (OTA principle 13)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-4、CPS.IP-1
24	6	Group	CPS.IP-1	Notification of password changes. This is a very specific issue, but it can help in the detection of attacks that take over a device, service or application. Users (or administrators) should be notified when a password is changed. (OTA principle 16)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.IP-1
24	7	Group	CPS.IP-1	Secure recovery of passwords. Likewise, if a password is forgotten, the supplier should provide a secure recovery mechanism to reset the password so that attackers cannot force a password change and then intercept the resulting interaction. (OTA principle 14)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.IP-1

ID	No	Affiliation	Place	Comments	Responses to Comments
24	8	Group	CPS.RA-1 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.DS-5	Understand behavior upon loss of connectivity. The METI Framework addresses DDoS resilience in several places but simple loss of connectivity (whether intentional or not) can also have a major impact on these systems and the cyber-physical interaction. Owners of these systems should understand the behavior of devices, servers and controlling applications in case of loss of connectivity and factor that into their risk assessment. (OTA principle 21)	Regarding your commnents, we leave the contents as original.
24	9	Group	CPS.RA-1 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.DS-5	Behavior during software updates. A related issue is understanding the behavior of devices during a software update. Some devices continue to operate as normal while the update is installed, whereas others undergo a long “pause” which can significantly impact operation. This can affect data collection and integrity and provide a potential opening for attackers, so the behavior needs to be factored into the risk assessment.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.MA-1
24	10	Group	CPS.AM-1 CPS.CM-6 CPS.SC-2 CPS.DS-4	Pre-purchase lifecycle issues. This is another issue that may be implied in the METI framework, but there are a few lifecycle issues that should be explicitly taken into account prior to purchase of devices or services. For example: Has the supplier committed to a certain timeframe for security patching and support? How will the device or service operate after that time (i.e., will all the same functionality still be available, or will it become limited)? (OTA principles 1, 6, 8, 19, 21)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-2, CPS.SC-4
24	11	Group	CPS.DS-5 CPS.AN-1 CPS.MI-1	Securing email interaction. Email is a major attack vector, and there have been reported cases of attackers sending fake email enticing users to download malicious device software. One way to protect against this is through use of email authentication technologies (SPF, DKIM, DMARC) and opportunistic TLS for email, which encrypts email between servers. Though this is “out of band” of the normal device, server, controlling application interaction, this vulnerability can also introduce significant risk. (OTA principles 34, 35, 36)	We revised the content, taking into account your comments. Relevant part : Appendix C
24	12	Group		Security is an ongoing process, and we would like to commend METI for this comprehensive work toward protecting IoT and Industrial Control Systems by supply chain management, and for its recognition of the importance of ensuring consistency with major international standards. Trust at all layers of the ecosystem is essential, and this framework will be an excellent resource to stakeholders working toward our common goals of improved security for the Internet overall, and for IoT and ICS in particular.	Your comments are considered as positive feedback on this framework.
24	13	Group		We also would like to direct your attention to some key pieces of work we have developed in this area, that can serve as either a foundation or a model for similar or complementary efforts to improve security-by-design: 1. The Internet Society’s Online Trust Alliance (OTA) IoT Trust Framework, a set of 40 principles addressing security, privacy and long-term sustainability (lifecycle) issues. Its development included more than one hundred stakeholders representing industry, government, and consumer advocates, who contributed to this recommended set of core actions. The Framework is available in Japanese: https://www.internetsociety.org/iot/trust-framework/ 2. The Internet Society is engaged in a number of multistakeholder processes to enhance IoT security globally. In Canada, we have partnered with the Canadian government (Innovation, Science and Economic Development, ISED), the Canadian Internet Policy and Public Interest Clinic, CANARIE, and The Canadian Internet Registration Authority (CIRA), to come up with recommendations and frameworks for consumer education, network resiliency, and labelling for IoT devices. Among the outcomes of this initiative is to support the efforts of CIRA to create an open-source, secure home gateway prototype, designed with the challenges of IoT devices in mind: https://iotsecurity2018.ca/	We will use your comments as a reference in advancing cyber security policies in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
				Other resources which may be relevant to the further development of the Framework include: 1. “Mapping Security & Privacy in the Internet of Things,” which was developed in conjunction with the UK’s “Code of Practice for Consumer IoT Security”: https://iotsecuritymapping.uk/ 2. ENISA’s “Baseline Security Recommendations for Internet of Things in the context of critical information infrastructures”: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot 3. For a snapshot of relevant standards work in the Internet Engineering Task Force (IETF) – the IETF IoT Rough Guide from the most recent IETF meeting in Bangkok last November. We publish these before every IETF meeting, as a resource to more easily monitor IETF work related to IoT: https://www.internetsociety.org/blog/2018/10/rough-guide-to-ietf-103-internet-of-things/ 4. The “Manufacturer Usage Description Specification“ (MUD), which would help provision IoT devices and automate network access control configuration, has been approved by the Internet Engineering Steering Group (IESG) as a proposed standard in 2018: https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/	
25	1	Individuals	Footnote 3	There is a mistake in the name of the organization in the footnote in Japanese version.	We revised the content as suggested in your comments. Relevant part : Footnote 3
25	2	Individuals	Part III 3.	Vertical ruled lines may be required in the title column so that it is easier to read. (like tables in Appendix C)	We revised the content as suggested in your comments. Relevant part : Part III 3.
25	3	Individuals	Part III 3.	"ver1.1" in the 18th line, "v1.1" in the title of the table on the same page and "Ver.1.1" in the "An Example of Corresponding Measure Requirement" column in the table on page 48 need to be unified.	We revised the content as suggested in your comments. Relevant part : Part III 3.
25	4	Individuals	Appendix C	"rev.4" in the title of the table needs to be appropriately changed to "Rev.4" as written in the main text.	We revised the content as suggested in your comments. Relevant part : Appendix C
26	1	Corporation	Appendix C CPS.IP-2	<High Advanced> in Example of Security Measures in Japanese version suggests the need to take two measures "together", i.e. restrictions on software and unpermitted installation of software. Taking both the measures together, however, is not realistic; therefore the description must be changed to take either of the two measures. ■ Reason Most of malware are executable software only by placing a file while most of measures using white- and black-lists take control of software when it actually runs upon being placed. In addition, as for software executable only by placing a file, the requirements to prohibit the installation of software (placement of files) are not realistically feasible; therefore it is preferable to change the description on the requirements to prohibit the installation using "or" or something, in order to prompt users to take either of the measures.	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.IP-2
26	2	Corporation	Appendix C CPS.CM-3	Whitelisting anti-malware measures are also effective and must be included in <High Advanced> in Example of Security Measures. ■ Reason Only behavioral detection measures are suggested here, the definition of behaviors for behavioral detection, however, can sometimes be updated, which is not necessarily optimal for mass-marketed IoT devices. Whitelisting measures must be included for IoT devices with limited functions.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.CM-3
26	3	Corporation	Appendix C CPS.CM-3	Whitelisting anti-malware measures are also effective and must be included in <Advanced> in Example of Security Measures. ■ Reason Only the installation of detection/restoration software using technologies of pattern matching is suggested here, however whitelisting measures must be included in consideration of IoT devices with limited functions and use in a narrow-bandwidth environment.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.CM-3
26	4	Corporation	Appendix C CPS.AM-1	Although asset management is fundamental for security requirements, responses should also be made on abnormal assets discovered as an example of <High Advanced> security measures. Therefore, it is better to change "The system implements and operates a mechanism which automatically detects unauthorized assets" to "The system implements and operates a mechanism which automatically detects unauthorized assets and eliminates them from management information, separate from the system, etc."	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-1

ID	No	Affiliation	Place	Comments	Responses to Comments
26	5	Corporation	Appendix C CPS.AM-5	It is unclear whether the security measure is restricting the connection and use of the organization's portable storage in an external system or using the organization's portable storage from an external system, or both. The applicable organization that will implement the usage restriction will change depending on whether the restriction applies to either or both. Thus, "Restrict a portable storage of the organization in an external system" described as an example of <Advanced> security measures needs elaboration. Furthermore, what does portable storage refer to? If it refers to portable storage devices, the security measures should apply to all storages (data storage devices) instead of only portable storage. Therefore, it is better to change "portable storage" in the <Advanced> security measure example to simply "storage (data storage devices)."	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-5
26	6	Corporation	Appendix C CPS.RA-3	Given crimes and issues pertaining to threat information disclosed to the product is frequent, the methods of obtaining information need to be more advanced. Therefore, the security measure requirement example for <High Advanced> needs to add the following example of security measures as it should also look at information on the dark web that are investigated and analyzed by professionals, and not just information disclosed to the general public. ・The organization utilizes services, etc. provided by professionals as necessary, obtain information that only some professionals have access to and identify threats based on the information.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.RA-3
26	7	Corporation	Appendix C CPS.SC-5	Because it is desirable to also strengthen identification features of CSF for other organizations including business partners, a regular demonstration to consigned parties that the company has low security risks through dark web investigations, etc. will increase consciousness towards security measures for both parties. In addition, making a list of reliable services will likely reduce the difference in levels between services used. Therefore, the addition of the following examples of security measures for <High Advanced> is requested: ・Important business partners and their reconsigned organizations will investigate for signs of attack or information leakage through dark web investigations, etc. and regularly report results to the organization. ・The investigation service to use needs to be a service listed.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-5
26	8	Corporation	Appendix C CPS.AC-5	In order to minimize damages from security incidents, systems administrators also need to be applicable in minimizing their authorization and be unable to suspend important services and protected processes. Therefore, the addition of the following examples of security measures for <High Advanced> is requested: ・The organization may minimize the authorization of the systems administrator in order to minimize damages from security incidents. ・The organization may restrict even systems administrators from suspending the server's important services or protected processes in order to minimize damages from security incidents.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-5
26	9	Corporation	Appendix C CPS.AT-2	The phrase "appropriate training and security education appropriate to the execution of the roles assigned" is repeated between measure requirements and examples security measures, making actions to take difficult to understand. Implementing measures will be easier if there are examples of training presented for "appropriate training and security education appropriate to the execution of the roles assigned." Therefore, it would be better to specify, such as "simulations that assume an actual accident occurred."	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.AT-2
26	10	Corporation	Appendix C CPS.DS-3	According to the revision made in FY2018 on the government's common standards for information security measures, it is standard that all data transmitted with external parties are encrypted. It is not appropriate to narrow the scope of verification in the example of security measures regardless of describing something similar in the security requirement. Therefore, for the example for <High Advanced> security measures required, all data sent and received needs to be encrypted regardless of their level of importance, and have all transmitted data be encrypted at appropriate levels. In addition, there would be no issue if the phrase "from a high apparatus of the importance." is deleted.	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.DS-3

ID	No	Affiliation	Place	Comments	Responses to Comments
26	11	Corporation	Appendix C CPS.DS-9	The security requirement mentions "prevent unauthorized software from launching" while the examples of security measures only touches on notifying and detecting, and lacks clarity in terms of preventing launching as described in the requirement. Because a clearer description is needed on the prevention of launching unauthorized software (software irrelevant to work), the addition of the following measure for <High Advanced> is requested: ・The organization uses a tool that will prevent the launching of applicable software in the event an unauthorized software is detected. A measure to limit software that can be launched should also be included in addition to preventing the launch of unauthorized software. Therefore, the addition of the following measure for <Advanced> is requested: ・The system suspends the launch of unregistered software by registering (identifying) software that will launch	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.DS-9
26	12	Corporation	Appendix C CPS.IP-7	Dark web investigation should be added as a way to assess attacks from external parties. Therefore, the addition of the following measure for <Basic> is requested: ・The organization regularly makes assessments that it is not subject to attacks and reports results to the systems administrator.	Please refer to Appendix C CPS.RA-3 High-Advanced for the point you pointed out.
26	13	Corporation	Appendix C CPS.PT-1	Details should also be added given that O/S logs alone will not be able to respond to all needs that differ by situation. Therefore, the addition of the following measure for <High Advanced> is requested: ・Detailed logs (O/S command level) that don't remain in the O/S function will also be collected because they are effective in subsequently tracking the causes of security incidents and unauthorized actions, as well as detecting security incidents.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.PT-1
27	1	Group		Although the security measure guidelines presented individually can be perceived as measures that need to be implemented, the description of "this framework" is inconsistent throughout the document (and particularly pointed out in "Reason" below). It is unclear what "framework" refers to. Does the framework: ・Refer to the structure of the new industrial society (three layers) and the six elements? ・Or the structuring of this document (i.e. Parts I, II and III)? ・Or the set of security measure guidelines? ・Or the set of common measures? ・Or the set of approaches that will clarify the subjects of analysis? In addition, the framework is compared to NIST Cybersecurity Framework v1.1 and considered "harmonizing" with it, but currently, the proposal for consideration guidelines for the three layers are only being classified according to the NIST framework. It's difficult to perceive that the concept for a new framework is being indicated. ■Reason The descriptions of "the framework" are diverse as indicated below. ① (P. 1) Executive Summary, line 24 (5th paragraph) "The Cyber/Physical Security Framework will guide the implementation of the Connected Industries program to reduce the risk of cyberattack" ②(P. 4) 3. Intention of developing the Framework and its scope of application "The Framework grasps the overall picture of the new industrial society"	This framework provides an overall framework for security measures and has been formulating with reference to major international standards. We used your comments as a reference in revising the content. Relevant part : Introduction

ID	No	Affiliation	Place	Comments	Responses to Comments
				④ (P. 8) 7. How to use the Framework "In order to accurately... build the entire framework as follows" (1) Part I (Concept)... (2) Part II (Policy)... (3) Part III (Method)... ... In this way, by using three part structure, the Framework can catch up with any changes of security requirements continually and flexible." ④ (P. 8) 7. How to use the Framework "By referring to the three-layer approach shown in the Framework..." ⑤ (P. 10) Line 11 "The Framework provides a guide for security measures required by Society5.0 and Connected Industries extended supply chain models." ⑥ (P.10) Last line "Part I of the Framework...describes policies to deal with risk sources in each of its elements." ⑦ (P.12) Line 7 "The basic structure of the Framework is to identify the risk source of the value creation process in three layers, present policy and security measures for each risk source for the six elements, and present specific examples of the measures." ⑧ (P.23) Line 12 The Framework presents security measures common among all industries..." ⑨ (P.25) Part II (Policy): Identification of risk sources and measure requirements "In Part II, the risk source of the value creation process in the new industrial society is organized based on the three-layer approach, presented in the Framework"	
27	2	Group		Because the first layer is better presented by discussing systems and product life cycles, the text should be revised to focus on life cycles. ■Reason Based on the relationship between individuals and organizations, there are limits to discussing through three layers/ Given all positions from the top to bottom of supply chains and systems involve people and organizations, it would be difficult to discuss those elements alone by categorizing them into layers. For example, security risks pertaining to physical access also involve internal crime. Residents and guests may potentially attack the system of smart homes. Discussions based on layers would be insufficient in this case. As such, the second and third layers would also involve people during the operation and maintenance processes, and thus require security measures that take this into account. Layer-based discussions won't cover this aspect enough.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
27	3	Group	6. (2) ③	Specific explanation is needed on the table comparing the relationship with international standards. ■Reason The table of comparison here is assumed to refer to Appendix D. The appendix would be more effectively referred to if there is an explanation on Appendix D (standards compared, comparison method, etc.).	We used your comments as a reference in revising the content. Relevant part : Part III 1.(1)
27	4	Group	6. (2) ③	A plan should be developed based on complementing the system and discussing with Europe in order to compare the Japanese and European systems pertaining to trust services and achieve interoperability. ■Reason There is no legal basis equivalent to EU's trust framework for time stamp stations that provide the time and electronic signatures that verify identity. Furthermore, there is no legislation in Japan for certification serving as a basis to verify components (IoT), companies and organizations that corresponds to EU's e-Seal. The following reference material, a workshop held as part of MIC's research survey, is recommended for comparison: (http://www.soumu.go.jp/main_content/000597573.pdf) Comparison of Japanese and EU trust service systems: (https://nosurrender.jp/trust_ws/docs/download/s05.pdf)	We will use your comments as a reference in advancing cyber security policies in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
27	5	Group	Part I 2.1 4.	① The development of a trust framework through legislating a Japanese version of the EU e-Seal with interoperability in which certifications similar to those for individuals can be issued to companies and mutually trusted is requested. ② The development of a system that issues certifications for organizations, people and components out of the six elements and enables trusted ID-based interactions is proposed. This would be exactly like EU's system. ③ A system in which a trusted institution grants certifications to organizations, people and components out of the six elements and issues certifications to information from each element is suggested. Adding interoperability with EU's eIDAS is also suggested. ④ A system to monitor institutions that issue certifications is recommended as a procedure within the six elements. Adding interoperability with the auditing structure of EU's eIDAS in order to ensure reliability is also suggested. ■Reason The trustworthy relationship intended will be achieved by granting IDs and certifications to each of the organization, people and components within the six elements classified in P. 11 and building a trust framework in which each element can trust one another. EU and the US are completely taking the lead if companies are connected only within Japan and do not have interoperability for trustworthiness with EU and the US. A system for connecting companies should be defined in a manner that actively emulates standards from EU that is more advanced in its e-Seal definition and other projects in order to recover some leadership. A known example is Estonia, which established the landscape of providing certificates to organizations and people for interaction through an information exchange infrastructure named X-Road and IDs for its citizens and now offers many services. X-Road is covered on P. 14 in the reference material provided by member Shibata on January 31, 2019 during the Trust Service Study Working Group (1st session) of MIC's Platform Service Workshop (As of Jan 2019: https://www.x-tee.ee/factsheets/EE/#eng) (http://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02cyber01_04000001_00016.html) Its spreading of services is demonstrated through statistics as follows, for example: *Connection services: 2,691 *Queries: 100,231,584/month *Connection providers: Private: 651; Public institutions: 504 I do not know much about how ID assignments to components are being considered in EU and the US. Or maybe this matter should be initiated by Japan.	We will use your comments as a reference in advancing cyber security policies in the future.
27	6	Group	p.19	The trustworthiness of data within the six elements need to be defined in advance. I predict the system will be designed to not excessively ensure trust towards data. ■Reason The trustworthiness of data is speculated to only be limited to proving the trustworthiness of data sources based on certification from the data provider. This would generate a system that won't question the authenticity of the contents. For example, the trustworthiness of the publisher can be ensured but its contents cannot be completely trusted (fake news) for news published by Newspaper A. News can also be unintentionally incorrect or intentionally misleading as well.	Securing the trustworthiness of the data itself is recognized as an important issue for the realization of "Society 5.0", and the framework also describes measure requirements (CPS.GV-3, CPS.SC-7, CPS.CM-4, etc.) . In order to promote the framework in actual industrial activities, security measures according to the classification of the data to be handled, and confirmation methods such as data integrity and authenticity are also required. We will use your comments as a reference in advancing security measures for data.
27	7	Group	p.21	An example profile should be added after "...please use the Framework in order to adopt appropriate security measures internally.“ (There is no mention of adopting security measures internally afterwards) ■Reason Measures (for security) are normally developed based on analysis of threats and past incidents. However, the Framework will be easier to utilize if there was an example easily understandable because it involves processes in the supply chain and thus extensive.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
27	8	Group	Table 2.1-1	Should be defined together with examples of physical phenomenon in the physical space. ■Reason Even when only considering behaviors of people, there are infinite physical phenomenon that occur in physical space such as eating, going to the bathroom and blinking. There are also phenomenon that only the person engaging in it could determine, such as meditating, thinking and sleeping. It would likely be very difficult to convert all physical phenomenon to digital information.	We used your comments as a reference in revising the content. Relevant part : Part I 1.

ID	No	Affiliation	Place	Comments	Responses to Comments
27	9	Group	p.29	The definition for IoT should be defined by units that communicate with external parties, etc. ■Reason IoT devices are also composed through a combination of IoT devices, and their units vary greatly, starting from those measures by HEMS through cars, trains and airplanes. What is important here is to be able to exchange proof that information is coming from a certain device based on certifications when transmitting data with external parties. However, because certifications will become necessary for smaller devices in order to prevent hacking to internal parts of devices, I predict the units that should be developed at the moment and the units that should be developed in detail in the future will be defined on a separated basis.	Regarding your commnents, we leave the contents as original.
27	10	Group	Figure 2.1-8	"Acquirer" (in Figure 2.1-8) should be in Japanese (for the Japanese version) ■Reason Given there is no other mentioning of the term "Acquirer," there is no solid reason as to why the term has to be used in the figure.	We revised the content as suggested in your comments. Relevant part : Part II 1.4. , Table 2.1-8
27	11	Group	Part II 1.4.	"The organization should take measures such as adopting security-by design at the design and procurement stages…" ⇒ "Planning" is also necessary in addition to "design" and "procurement" ■Reason What needs to be protected should be thought out during the planning phase.	We revised the content as suggested in your comments. Relevant part : Part II 1.4.
27	12	Group	Part II 1.4.	Change to "needs to" instead of "should." ■Reason Needs to be a stronger requirement.	We used your comments as a reference in revising the content. Relevant part : Part II 1.4.
27	13	Group	Part II 1.4.	A suggestion to change the following: "(e.g. production, transportation)" ⇒(e.g. design of software, production involving implementation, transportation) ■Reason The procedures and product quality are important for the "design and implementation of software for contractors"	We revised the content as suggested in your comments. Relevant part : Part II 1.4.
27	14	Group	p.41	A suggestion to change the following: "Specifically, the data should be checked to determine whether it has been falsified,…" ⇒Specifically, connections should be checked if they are connected with the correct devices, the data should be checked to determine whether it has been falsified,... ■Reason Checks need to be made if the correct devices are being connected	Regarding your commnents, we leave the contents as original.
27	15	Group	Part III	High Advanced ⇒ Highly Advanced ■Reason Grammar error; may also be revised to "Very Advanced."	We used your comments as a reference in revising the content. Relevant part : Part III , Appendix C
27	16	Group	CPS.RA-4	Key concept 4 of IoT Security Guidelines should be added to key concepts 10 and 12. ■Reason Key concept 4 mentions conducting risk analysis from the planning process in IoT Security Guidelines.	We revised the content as suggested in your comments. Relevant part : Part III 3.4. CPS.RA-4
27	17	Group	CPS.RA-5	Add key concepts 4 and 7 of IoT Security Guidelines ■Reason Key concepts 4 and 7 of IoT Security Guidelines will help determine risks.	We revised the content as suggested in your comments. Relevant part : Part III 3.4. CPS.RA-5
27	18	Group	Appendix D.3 A.12.1.1	The implementation of human-centered design (ISO9241-210 and other HCD processes) is recommended to make "available" as described in Controls. ■Reason The operating procedures that will be made available will be completed and developed by incorporating ISO9241-210 HCD processes.	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
27	19	Group	Appendix D.3 A.12.2.1	The implementation of human-centered design (ISO9241-210 and other HCD processes, together with control of product quality "usability" and "quality during usage" of ISO25010) is recommended to achieve "appropriate user awareness" as described in Controls. ■Reason An easily recognizable user interface can be completed and developed by incorporating ISO9241-210 HCD processes and enhancing qualities for ISO 25010.	Regarding your commnents, we leave the contents as original.
28	1	Corporation	Appendix D.2	Appendix D.2 compares NIST SP 800-171 and the Cyber/Physical Security Framework. And while the level of security measures exemplified in the Framework are categorized into three levels of "Basic," "Advanced" and "High Advanced," they will be more useful if there is a table that compiles example security measures by level that can be performed by a reverse lookup. ■Reason The abovementioned feature will be beneficial for industries and companies when referring to this Framework to develop security measures that match with their fields and products.	Regarding your commnents, we leave the contents as original.
28	2	Corporation	Part III 3.9 3.11	NIST SP 800-193 and Platform Firmware Resiliency Guidelines can be added onto "Informative References" for the following measurement requirement IDs: CPS.DS-11, CPS DS-12, CPS MA-1, CPS MA-2 ■Reason Reference of these guidelines will be beneficial to specifications pertaining to measures countering risks of firmware falsification of IoT devices, etc.	Regarding your commnents, we leave the contents as original.
29	1	Group	p.4-5	The outcome of Connected Industries referred to as the Fourth Industrial Revolution will greatly impact the future of Japan. I agree with the report on the need to integrate cyberspace and physical space, the necessity of cooperation between companies and the importance of cyber security. When implementing the necessary security measures according to company conditions through using this Framework, I believe the IoT Security Check Sheet published on 2/28/2019 from our section meeting would be helpful. I hope such collaboration with private sector activities will also be promoted.	Your comments are considered as positive feedback on this framework.
29	2	Group	p.7	From the perspective of a private sector company, it is more realistic to start with the utilization of the core IoT technology and then move on to the Connected Industries initiative after deepening understanding and knowledge. Whether or not IoT will spread among companies depends on the "knowledge of utilizing IoT safely and with peace of mind," or simply put, security. In this sense, I believe the IoT Security Check Sheet published on 2/28/2019 from our section meeting would be helpful for companies to carry out specific actions. I hope such collaboration with private sector activities will also be promoted.	We will use your comments as a reference in advancing cyber security policies in the future.
29	3	Group	4.	As a person assumed to read this Framework, I believe departments involved in the purchasing decisions of the supply chain should be added because in practice, decisions on selecting vendors and parts also consider the perceptions mentioned in this Framework.	Regarding your commnents, we leave the contents as original.
29	4	Group	Part I	It is mentioned that "information that once would have been stored on paper documents can be digitized and stored in large quantities in cyberspace," but readers would better understand if there is an example on what kind of physical information would specifically apply. A summarization of the contents on the second layer described in "Appendix A. Use Case" would be sufficient.	We used your comments as a reference in revising the content. Relevant part : Part I 1.
29	5	Group	Table 2.1-4	In addition to DoS attacks as mentioned in (1) C of the first layer, destructions through ransom ware should also be added given there are information devices of organizations destructed through destructive malware and ransom ware such as WannaCry.	We used your comments as a reference in revising the content. Relevant part : Part II 1. , 1.2. , Table 2.1-4

ID	No	Affiliation	Place	Comments	Responses to Comments
30	1	Corporation		In a system as complex as the Society 5.0, it is practically impossible to assure the trustworthiness of all participants. Rather, it is important to limit the trust needed in (external parties), and assure that some level of untrustworthy components cannot cause critical damage. The two main vehicles for that are in some forms tried and tested. In the MILS (Multiple Independent Levels of Security/Safety) architectures, trust is concentrated on key elements, and large parts of the system are deliberately left untrusted. For example, a measurement device can authenticate and encrypt its values before handing it over to the modem; a compromised modem is thus reduced to being able to drop messages, but cannot alter messages anymore. If the communication between the measurement device and the modem is protected by a data diode, the modem also cannot be used to try and compromise the measurement device. While a thorough architecture analysis with a systematic approach would be preferable, the reality in many existing control systems is that the security of end devices is very weak or non-existing. A quick win solution would be to identify parts of the system that are impossible to bring to an adequate security level within a reasonable time and, if it is not possible to leave them disconnected, isolate them with a dedicated security gateway from the larger network, as well as implement strong monitoring to detect potential problems. The second approach is distribution of trust; examples here are blockchain like technologies which limit the required trustworthiness of individual participants, or intelligent comparison of related sensor readings to identify readings that do not make sense.	We will use your comments as a reference in advancing cyber security policies in the future.
30	2	Corporation	Part I 4.	Page 21: It is important to distinguish between trust and trustworthiness. Trust is essentially a state of mind – I can trust my 9-year-old to not steal sweets (though I might be foolish to do so). Trustworthiness is something that can be created by security measures (e.g., a lock on the cookie jar). We recommend to clearly state the difference of those two terms.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	3	Corporation	Part I:4.(2)	Page22 (2) The proof of trust paragraph is hard to understand in the English version. We highly recommend revising the translation.	We used your comments as a reference in revising the content. Relevant part : (English) Part I 4.(2)
30	4	Corporation	Part I 4.(3)	(3) The trustworthiness chain also needs to be clear on assumptions and expectations. It is perfectly fine if a communication system does not encrypt its data, as long as all applications that use that system are aware of this fact and – if needed – encrypt data themselves. It is thus vital that at all points where systems interact with each other, it is documented what the assumptions are and what guarantees a system can deliver.	We used your comments as a reference in revising the content. Relevant part : (English) Part I 4.(3)
30	5	Corporation		While Risk analysis is vital, one should also require a level; of risk-independent security hygiene – like one doesn't ask which bacteria are concretely mitigated by washing ones hands, some good practices should be mandatory for every component and subsystem (e.g., if data is encrypted, it should be done with a government approved cipher such as AES(Advanced Encryption Standard), and not with a self made one). [See: Smart Meter Req] http://www.gridsec.org/docs/20150614%20E2E-Sicherheit-Anforderungskatalog-EN.PDF] Also, requirements should come with a specification of testability – if a requirement is not verified, there is a high likelihood it will not be satisfied everywhere in the chain.	We will use your comments as a reference in advancing cyber security policies in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
30	6	Corporation		The Risk analysis focuses on analyzing risks for the business and for information systems; this approach (which is the basis for ISO 27000) is not sufficient for a connected society, where the risks for the overall society can massively exceed the risks for the business (a company that manufactures a vulnerable component used in the Olympic games can at worst go bankrupt; the national embarrassment over a cyber incident at the Olympics is far beyond that), and where the cyber and the physical domain can interact closely. This also needs to play into the mitigation, as the effort to mitigate a risk need to match the society value, not just the business value. Example: The heartbleed bug had no business impact on the people who produced it (as this was open source), but caused millions in damage in a large number of systems. Similarly, it might be invisible to a business if all their suppliers use the same sub supplier, and thus a single incident can affect a large part of their supply chain. Similarly, the focus of ISO 27000 on information security can distract from physical risks – again taking the Olympic games as an example, an attacker that focuses on physical damage – turning off the lights in the stadium, turning off the fridges in the doping control center, or closing all stadium fire doors can cause massively more damage and embarrassment that a purely information-centric attack. Overall, while ISO 27000 is a good Information security standard, it can be misleading for the Society 5.0 project. Other standards and frameworks that are more process-system, oriented, such as the STAMP framework and ISA/IEC 62443 should get more focus in this setting. Thus, we would strongly recommend to get more domain experts from the ICS/SCADA world involved in this framework. Also, it is important to have a healthy mix of government, academic, and various industry experts.	We will use your comments as a reference in advancing cyber security policies in the future.
30	7	Corporation		The risk assessment does not seem to focus much on privacy. Given the wealth of data created also by consumers, it would be important to also analyze the risk this poses for the consumers. This is especially vital in a global supply chain containing European partners, as free-flowing data would require all participants to follow the guidelines of the GDPR (General Data Protection Regulation)	We will use your comments as a reference in advancing cyber security policies in the future.
30	8	Corporation	第 II 部 1.1.(2) ③	I like that approach however, labelling all data with origin and trust level imposes an information architecture that few companies will be able to implement. An additional challenge is the handling of this data in an AI system. Due to their nature, those systems make it very hard to determine what input data had what impact on the output, and thus reliably determine how trustworthy the end result is if the input data has mixed levels of trustworthiness.	We will use your comments as a reference in advancing cyber security policies in the future.
30	9	Corporation	Overall	In overall, many international references are heavily US focused. Considering a global supply chain may include European partners, we recommend to include more European standards and guidelines such as GDPR and NIS directive.	This framework has been formulating with reference to major international standards. In addition, since new international standards etc. are always established, we will constantly revise it appropriately with reference to various international standards etc. even after it is established, taking into account your comments.
30	10	Corporation	Appendix E	(23) The definition of a hash-value misses some features; for example, it should be hard to derive any useful information about the original values knowing only the Hash value, it should be hard to find two input values that result in the same hash value, and a small change in the input value should lead to a totally different hash value.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	11	Corporation	Appendix E	(39) In Cyber-Physical systems such as industrial control systems, a process can also be the physical process. ISO 27000 is mispleading here, as it focuses on information security, and does originally not take control systems into account.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	12	Corporation	Appendix E	(41) Public key also can be used authentication (e.g., through digital signatures), key establishment and other functions; the definition given in the text only focuses on encryption.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	13	Corporation	Appendix E	(65) While Trustworthiness is defined, Trust is not. We would recommend the classic definition: A trusted system is a system whose failure can violate the security policy.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	14	Corporation	Appendix E	(42) Redundancy can also cover non-computer systems, such as a redundant power supply, and even people.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	15	Corporation	Appendix E	(47) Safety traditionally focuses on accidental risks, while security focuses on deliberate, malicious action.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	16	Corporation	Appendix E	(48) This includes steps such as a use-case analysis, risk analysis, threat analysis, asset inventory, security architecture, external requirement analysis, privacy impact assessment, etc.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	17	Corporation	Appendix E	(50) In a Cyber-Physical system, security incidents can also move from information security to physical or process security.	Regarding your commnents, we leave the contents as original.
30	18	Corporation	Appendix E	(53) Security policies are not restricted to priorities by top management; there can be a hierarchy that can go into quite some low level detail (e.g., a safe must delay an attacker for at least 5 hours is a security policy that likely does not come from top management).	We used your comments as a reference in revising the content. Relevant part : Appendix E

ID	No	Affiliation	Place	Comments	Responses to Comments
30	19	Corporation	Appendix E	(54) Security risk is defined as “Possibility of some effects on the management of the organization caused by the malfunctions related to security.” It should be added (especially for Society 5.0) that there are also effects to society and other organizations; it is also unclear why the definition focuses on the management (If patients in a hospital die due to a security problem, the main effect is on the patients, not the management of the organization.	We used your comments as a reference in revising the content. Relevant part : Appendix E
30	20	Corporation	Appendix E	(55) This is also more commonly known as a security control.	Regarding your commnents, we leave the contents as original.
30	21	Corporation		While we applaud the provision of an English version to reach out to a wider community, a straight translation is a difficult task – the same wording has subtly different meanings or provides a different context in another language (for example, many languages cannot differ between security and safety). Having had the opportunity to have a team of experts that had to rely only on the English version as well as Japanese native speakers, we found various places where the English version alone was ambiguous, unclear, or insufficient, which could be explained easily with the original version. We would recommend a quality control of the next version to be performed by a team of domain experts that comprises both bi-lingual (ideally both Japanese and non Japanese native speakers) and foreign experts to assure the Japanese context is correctly transferred into the English version.	We will use your comments as a reference in translating the framework.
31	1	Group		・ Explanations using metaphors and analogies It would be better if there are explanatory materials that use analogy such as, "If referred in terms of food,..." in order to deepen understanding on the Framework. Although a briefing was held at JNSA and provided us with deepened understanding, rhetoric that would further facilitate understanding without direct explanations will also be useful.	We will use your comments as a reference in advancing cyber security policies in the future.
31	2	Group		・Change the wording for "three layers" Additional explanation is required because the word "layer" is used. Furthermore, in Japanese context and the illustrative figures combined make readers imagine hierarchy that "sequentially overlaps vertically." Meanwhile, because the basis of definitions for the three-layer structure differ, each of the definitions are not exclusive and cannot be uniformly classified. It would be better for readers and organizations that will use this Framework to understand if the term is changed to something like "three perspectives," "three standpoints" or "three angles."	We have discussed the point you pointed out in the cross-sectoral SWG. When we say “layer” in English, we have the opinion that it is appropriate to express the three-layer approach of this framework. Regarding your commnents, we leave the contents as original.
31	3	Group		・Appendixes B, C, D and E Appendixes B, C and D refer to multiple documents that ISOG-J, the lower branch of JNSA, has prepared and published. In addition the glossary in Appendix E explains on the terms SOC, CSIRT and security measure organization. Because ISOG-J positions security measure organizations as including SOC and CSIRT, it would be preferable if explanations such as those provided below would be added: Example) A security measure organization includes organizations and functions such as SOC and CSIRT. ['5W1H' to Share Cyber Security Information to Strengthen Security Measure Organizations (SOC, CSIRT) v1.0 (ISOG-J, 2017); The Security Measure Organization Textbook v2.1 (ISOG-J, 2018); The Textbook Handbook on Security Measure Organizations v1.0 (ISOG-J, 2018); The Security Measure Organization Textbook: Self-Check Sheet for Maturity Level v2.2 (ISOG-J, 2019)]	We used your comments as a reference in revising the content. Relevant part : Appendix E
32	1	Individuals		Specific examples of responses are listed on Appendix B as risk-countering measures against individuals of malicious intent. The examples cover what relevant personnel can do under current laws and legislations. However, cyber crimes cannot be completely covered through the current Act on the Protection of Personal Information, Fair Competition Code or Act on the Protection of Specially Designated Secrets. Would new laws be necessary (such as a spy prevention law applicable to private-sector information) based on current conditions (and eyeing the future)? Otherwise, the government will be unable to respond to cyber crimes with superficial responses. We look forward to your ministry leading the way towards legislation.	We will use your comments as a reference in advancing cyber security policies in the future.

ID	No	Affiliation	Place	Comments	Responses to Comments
33	1	Corporation		We aims to support METI's efforts to articulate risk and take measures to address key strategic challenges to identifying and managing risk associated with the global ICT supply chain. It is critical to demonstrate that both the government and industry are taking the necessary steps to increase the security posture of their products and systems. In support of METI's second draft of the Cyber/Physical Framework, we recommends the following: (1) Support industry and government collaboration and stakeholder learning environments to promote sharing of cybersecurity lessons learned and best practices; (2) Address and reduce the security risks associated with ICT product supply chains; a. Offering the possibility to suppliers of having a conformity assessment program to build trust, credibility and value to society. b. Leverage the most effective and cost efficient methodologies to improve the security posture of products and systems. i. If actors in the supply chain want to demonstrate compliance, they can accomplish this through utilizing conformity assessment practices, such as evaluation, certification, verification. (3) Develop and utilize appropriate metrics and evaluation techniques for cybersecurity assurance of ICT products and supporting IT infrastructure; a. Industry and government need to establish internationally accepted & harmonized standard(s) on cybersecurity with a risk-based approaches.	We will use your comments as a reference in advancing cyber security policies in the future.
33	2	Corporation		To mitigate product level supply chain risks for connected technologies throughout the life cycle of the product and to restore trust in regards to the security of devices, services, systems and companies, supply chain risk management policies should include the following elements: • Demonstrated and ongoing employee training to raise and maintain awareness of effective supply chain security practices, including identification of risks, sourcing of third-party software and components, roles and responsibilities, and coordinated disclosure of potential vulnerabilities; • Due diligence assessment of the entire supply chain with process integrity validation to determine whether adequate safeguards are in place to minimize cybersecurity risk associated with the use of their software or components, with regular follow-up audits; • Clear technical criteria and requirements, including legal requirements or prohibitions, for all third-party software products and components used throughout the life cycle of ICT products; • Sufficient protection against security flaws and weaknesses for all software applications to identify potential vulnerabilities that may result in a compromise; • Consideration of periodic risk assessments, including risks to information security relating to ICT products; • Independent verification of the steps taken to validate security of third-party software; • Formal process for identifying and regularly updating software applications and applying patch releases as appropriate to help ensure continued protection against newly identified threats; and • Implementation of "track and trade" programs to establish and monitor sources of all software, components, and code to facilitate efficient access to software updates and security patches and to help ensure ongoing support for legacy products.	We will use your comments as a reference in advancing cyber security policies in the future.
33	3	Corporation		Vehicles including smart cars, their software and wireless digital systems; connected & electric cars and autonomous cars are extremely vulnerable to security threats. This should be of concern to government agencies such as vehicle licensing, vehicle registration, traffic management and law enforcement agencies. We are are also developing safety standards to address the needs of autonomous vehicles and the desire to test highly automated vehicles with safety drivers. New programs and certification efforts will enable the market to develop new and innovative technologies while reducing the risk to their consumers and alleviate the concerns of local and federal government agencies. We are currently supporting the U.S. Department of Transportation to demonstrate the current automotive cybersecurity risks, as well as UNECE type approval in Europe. The result is an independent third-party validation that can help mitigate risk and support the automotive industry navigate the growing complexities across the supply chain – from compliance and regulatory issues to trade challenges and market access.	We will use your comments as a reference in advancing cyber security policies in the future.
33	4	Corporation		We applauds the METI's leadership, coordination, and collaboration, with the private sector to strengthen cybersecurity. Cybersecurity provides an ideal opportunity for strong public-private partnerships. Collaborating with both the public and private sectors, we has developed several cybersecurity/risk management standards and programs to address critical infrastructure protection and cybersecurity risk by developing solutions that are voluntary, rely on market driven mechanisms, and are risk-management based and internationally aligned. We look forward to further engaging METI in support of its Cyber Supply Chain Risk Management goals.	Your comments are considered as positive feedback on this framework.

ID	No	Affiliation	Place	Comments	Responses to Comments
34	1	Group	Appendix B L1_1_a_PEO	[People] Do not fully recognize the security risks that they may become involved in ・In addition to training and education, reviews should also be made on whether access to manuals, contacts, procedures and public Wi-Fi are okay (because forgetting IoT devices out in the public is possible given their increase in count, exemplary cases should be presented on where to contact, together with where to contact when a suspicious email has been opened)	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AT-1
34	2	Group	Appendix B L1_1_a_SYS	[System] A structure that promptly detects and responds to abnormalities in security has not been implemented in the system ・No security of logs (assuming internal crime, operation logs for important data and files, etc.) ・Definition of the scope of acceptable closing of communications when considering the shutting down of communication and adoption, preparation and availability of white lists ・Malware should be quarantined but not deleted (if deleted, the malware functions and connections cannot be analyzed) ・Are logical extensions of interpreting intrusions and infringements not included?	We revised the content, taking into account your comments. Relevant part : Appendix B L1_1_a_SYS
34	3	Group	Appendix B 1st layer	The following threats should be added as applicable to "data that needs protection from the field the organization manages is leaked," one of expected security incidents listed: ・Falsification of website pages following an external attack (uploading of unauthorized files, XSS) ・Data falsification following an internal crime (crime committed by an employee with writing authorization) ・Falsification of sensor information (attack by physical destruction or jamming) ・Falsification of data through malware	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	4	Group	Appendix B 1st layer	Data vulnerability is not considered in "business cannot be continued in an appropriate manner following a security incident in the organization," one of expected security incidents listed.	We revised the content, taking into account your comments. Relevant part : Appendix B
34	5	Group	Appendix B 1st layer	Confirmation of whether the organization and the externally-affiliated company have certification such as ISO/IEC 27001 should be conducted in responding to "a security incident occurred in a product or service distribution channel and caused unintended quality deterioration such as device damage," one of expected security incidents listed.	Regarding your commnents, we leave the contents as original.
34	6	Group	Appendix B 2nd layer	Responses that use switching devices that monitor the network are missing in the following threats: ・Network connection through IoT devices illegally tampered with through theft, etc. ・Unauthorized falsification by people inside or outside the organization with malicious intent	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	7	Group	Appendix B L2_3_c_SYS	Responses by the system only contain radio.	We used your comments as a reference in revising the content. Relevant part : Appendix B L2_3_c_SYS
34	8	Group	Appendix B L3_4_b_DAT	It is difficult to determine responses for the vulnerability of "data being scattered" based on risk management. There is probably no company that does not disperse data, and is hence unrealistic.	Regarding your commnents, we leave the contents as original.
34	9	Group	Appendix B 3rd layer	The threat of having illegal components connected is missing in "identity fraud to a legitimate entity through unauthorized organization, people, component or system," one of expected security incidents listed.	Regarding your commnents, we leave the contents as original.
34	10	Group	Appendix B 3rd layer	The authentication security level is low for the response for "inappropriate data is received from (fraudulent) organizations, people, components, etc.," one of expected security incidents listed, because only ID is mentioned as means of authentication and identification in cyberspace. (There are also possibilities of reply attacks)	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	11	Group	Appendix B 3rd layer	Responses for intermediary attacks are insufficient for the response for "inappropriate data is received from (fraudulent) organizations, people, components, etc.," one of expected security incidents listed, in terms of authenticating wireless access points (users, IoT devices, servers, etc.)	We revised the content, taking into account your comments. Relevant part : Appendix B
34	12	Group	Appendix C CPS.BE-1	Supply chain should also be defined (such as the scope; for example, is electricity or water included?).	Regarding your commnents, we leave the contents as original.
34	13	Group	Appendix C CPS.BE-1	Since the contents of <Advanced> and <Basic> are similar, I think they should be merged.	Regarding your commnents, we leave the contents as original.
34	14	Group	Appendix C CPS.BE-2 CPS.AM-6	Since the contents of CPS-AM-6 and CPS-BE-2 are similar, I think they should be merged.	Regarding your commnents, we leave the contents as original.
34	15	Group	Appendix C	Please clarify the implementation timing of the examples. (Is it once a year or when changes are made to the contents?)	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
34	16	Group		Some aspects of the three layers are redundant, and categorization of many are unclear when one tries to categorize them. For example, the first layer mentions physical elements, and we can understand that elements such as “people” and “organization” match the first layer and that elements such as “data” and “procedure” match the third layer. However, all elements are relevant to all layers when we look at Appendix B, etc., so many aspects invite unclear understanding. (Reference: Similar opinion) Since layer separation does not create “MECE” relationships, readers may be confused and have difficulty understanding. Therefore, it may be better to categorize layers without overlaps. The NIST Cybersecurity Framework makes separations by process (identification, protection, detection, response, and recovery), so it is easy to understand. Because of overlaps in layers, discussions in Appendix B create confusion. There are a number of similar response requirements, so it seems tedious.	The three-layer model is a model that captures a new society "Society 5.0", and is not a model that clearly separates the objects included in each layer. In order to ensure the trustworthiness of corporate (organization) management, it is also required to secure the trustworthiness of objects in cyber space managed by the corporate (organization) and the transcription function of IoT devices. This three-layer model is a key concept of the framework, so I will continue to explain it carefully.
34	17	Group		Each layer mentions similar risk sources, but aren’t risk sources completely different in each layer? When we consider imaginary cases, questions arise when applying. It may be better to utilize the existing framework when performing risk analysis. (Attack tree, for example)	When we capture the value creation process based on a three-layer model, we do not believe that the risk sources are completely different in each layer, as there are six elements in each layer.
34	18	Group	Appendix B 3rd layer	Shouldn’t the function include the categorization of “function to process data”? In response to this, risks such as “falsification” exist.	Regarding your commnents, we leave the contents as original.
34	19	Group	Appendix B 3rd layer	I think “denial-of-service attack” refers to DoS attack, but the first layer and second layer used the description “DoS”. If terminology is not standardized, it will cause confusion.	We revised the content as suggested in your comments. Relevant part : Appendix B
34	20	Group	Appendix B 3rd layer	In the assumed security incident “The system that handles the organization’s data in a related organization stops due to a denial-of-service attack”, the DoS attack is assigned to “organization”. However, isn’t it the “system” that responds to this?	It is assumed that other organizations will be asked to carry out the system response from own organization. Regarding your commnents, we leave the contents as original.
34	21	Group	Appendix B 3rd layer	I don’t see the aspects of wireless devices and radio waves. Example: Damage is received due to unauthorized operation of equipment from a physical distance using wireless devices. Example: External interference of radio waves affects the service, etc.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	22	Group	Appendix B 3rd layer	“People” and “data” of the assumed security incident “The organization’s protected data is leaked from a data processing area managed by a related organization” do not mention risks and response to data extraction.	It is assumed that other organizations will be asked to carry out the response for people or data from own organization. Regarding your commnents, we leave the contents as original.
34	23	Group		I felt that this is trying to systematically guarantee the comprehensiveness of risk sources through the three-layer approach. However, companies that have not been promoting Society5.0 must apply it to their own companies when actually checking the security using this guideline. Due to this, I felt that the security guideline for each industry would become very important.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	24	Group		Since there are many descriptions that are difficult to understand as well as vague expressions, I felt that it would be difficult for companies to evaluate/take measures by using this framework at this point. Please continue to make adjustments/considerations with the Ministry of Economy, Trade and Industry and various companies and formulate a framework with utility values.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	25	Group		Regarding the appendix, I felt that the interpretation may differ depending on the reader and that the burden to check the contents is heavy because there are many items with similar descriptions. I felt that efforts to divide the section written by SE and the section written by the management and to link the configuration diagram and items would be good to lighten the burden.	We will use your comments as a reference in advancing cyber security policies in the future.
34	26	Group		There are a number of vague expressions, such as “safety”, “hazard”, and “appropriate”. Due to this, it is necessary to clarify the definitions so that there is no discrepancy between each industrial area. The writing seems to be on the CIA side of IT systems. What if you write from the perspective of SAIC (safety, availability, integrity, and confidentiality) of OT systems (divide depending on the case to be operated in the field). AI and cloud-type, which are the latest technologies, need to be mentioned.	We used your comments as a reference in revising the content. Relevant part : Appendix E
34	27	Group		It draws a parallel with materials of the level of international standards, such as NIST framework, and I think it is very good in the aspect of ensuring comprehensiveness.	Your comments are considered as positive feedback on this framework.
34	28	Group	Appendix B	Extraction of functions/security incidents does not seem thorough. (What if you utilize frameworks, such as CIA and STRIDE?)	Regarding your commnents, we leave the contents as original.
34	29	Group	L1_1_a_COM	This says "The security status of components and the status of network connections are not managed appropriately". However, isn't checking of the first layer impossible to begin with unless asset inventory is taken?	We revised the content, taking into account your comments. Relevant part : Appendix B

ID	No	Affiliation	Place	Comments	Responses to Comments
34	30	Group	Appendix B 1st layer	The assumed security incident “Data that must be protected is leaked from an area managed by the organization” does not mention perspectives of physical intrusion and protection.	We revised the content, taking into account your comments. Relevant part : Appendix B
34	31	Group	Appendix B 1st layer	The fact that the assumed security incident "The system dealing with the data of its own organization stops due to a denial of service attack" only limits the attacks and incidents that damage availability to denial of service attack gives me a sense of wrongness. Aren't there other cases? (Zero-day, etc.)	We revised the content, taking into account your comments. Relevant part : Appendix B
34	32	Group	Appendix B 1st layer	Regarding the assumed security incident "Security measures that satisfy the legal requirements for a system cannot be implemented", the fact that security measures that satisfy the legal requirements for a system cannot be implemented does not seem to be a security incident. Isn’t it vulnerability that should be mentioned? Compliance with laws and restrictions stipulated in each industry is not a measure requirement but a rule involving punishment. It gives me a sense of wrongness to mention it here.	The security incidents you pointed out are considered to be important. Regarding your commnents, we leave the contents as original.
34	33	Group	Appendix B 2nd layer	The policy in case the transcription and transfer functions malfunction does not incorporate the perspective of "only safely stopping data transcription and transfer or detaching it". This is due to the facts: Third layer: Data is not corrupted First layer: There is no issue with the company, supply chain, or physical matters. Don't we also need the perspective to use physical functions (such as people) instead when only transcription and transfer function in an unexpected manner, rather than just recovery?	We revised the content, taking into account your comments. Relevant part : Appendix B
34	34	Group	CPS.IP-8	The criteria for "appropriate partners" are vague. Don't we need specific criteria, such as government certification?	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	35	Group	CPS.MA-1	The words “where applicable” seem unnecessary. Whether or not to perform it and granularity can be stipulated in Appendix C.	The need for remote maintenance is considered to be very high. On the other hand, there are cases where it is practically difficult to introduce such a mechanism. Regarding your commnents, we leave the contents as original.
34	36	Group	Appendix B L2_1_a_PRO	It says “There is no procedure, at the time of procurement, for checking whether the goods have appropriate levels of security functions”. Isn’t checking necessary not only at the time of procurement but also at the time of operation?	Regarding your commnents, we leave the contents as original.
34	37	Group	Appendix B 2nd layer	The vulnerability of the system under the assumed security incident “Unexpected behavior of the IoT device due to unauthorized access to its controls by impersonation of an authorized user” does not include “vulnerable protocol is used”. Measure requirements for this are missing. In addition, isn’t use of same ID/password part of people’s vulnerabilities?	Regarding your commnents, we leave the contents as original.
34	38	Group	Appendix B 2nd layer	The assumed security incident “Behavior that threatens safety, regardless of the behavior being normal or abnormal” is missing the perspective of safety instrumentation for the system. In case of a building, separation of the fire alarm system network and emergency elevator stop are assumed.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	39	Group	Appendix B 2nd layer	In the assumed security incident “Data (created by a device that does not support a tampering detection function such as MAC) is tampered with in the communication path between the IoT device and cyberspace”, the MAC address falsification detection function is one of the measure requirements, and there are attacks to falsify part of the payload. Due to this, “such as MAC” is not necessary.	We revised the content as suggested in your comments. Relevant part : Appendix B
34	40	Group	Appendix B 2nd layer	In the assumed security incident “Inappropriate measurement occurs due to physical interference with measurement”, threats and vulnerability/measure requirements are not linked. Isn’t the measure to control people’s unauthorized actions? It makes more sense to include this as an incident/threat against the center part of the first layer.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	41	Group	Appendix B 3rd layer	In the assumed security incident “The security requirements for highly confidential data to be shared only among authorized parties have not been set or met” does not include the item to divide from the perspective of the system. If utilizing with a building, segmentation of highly confidential data is one of the possibilities.	We revised the content, taking into account your comments. Relevant part : Appendix B
34	42	Group	Appendix C CPS.AM-2	Regarding the “common numbering rules” under <High Advanced>, numbering rules applicable to different industries seem excessive. Are there such industries? (Reference: Same opinion) Is “in accordance with the rules applicable to different industries such as cross - industry common numbering rules” under <High Advanced> realistically possible? Are there cases in which this has already been introduced? If this is introduced, the effect in case of changes to the supply chain due to changes to the business partner, etc. would be great.	It is considered effective for securing traceability when collaboration beyond the existing industry is activated in the future. Regarding your commnents, we leave the contents as original.
34	43	Group	Appendix C CPS.AM-3	Shouldn’t convenience of search be added to <High Advanced>?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-3

ID	No	Affiliation	Place	Comments	Responses to Comments
34	44	Group	Appendix C CPS.GV-1	The difference between <High Advanced> and <Advanced> is not very clear.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.GV-1
34	45	Group	Appendix C CPS.RA-4	The definition of "hazard" is vague.	We revised the content, taking into account your comments. Relevant part : Appendix E
34	46	Group		While IoT is comprehended as a sensor in some locations, there is a mention of control with IoT, giving me a sense of wrongness.	In this framework, IoT devices are regarded as devices that may have functions such as sensors and actuators. Regarding your commnents, we leave the contents as original.
34	47	Group	Appendix B 1st layer	Shouldn't the description be “availability”, “integrity”, and “confidentiality” in the order of importance for material composition? (Examples) 1. Shutdown of facility/function, loss of control 2. Falsification of control data and product information 3. Leak of authorization information	The objective situation of the user changes which of confidentiality, integrity, and availability is to be emphasized. Regarding your commnents, we leave the contents as original.
34	48	Group	Appendix B 1st layer	Isn't asset management for all OT environment facilities necessary? Too much focus is given to PC.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-1
34	49	Group	Appendix B 1st layer	Value of “people” is described from the perspective of IT. Descriptions are needed based on the understanding of the gap that IT can be replaced limitlessly and OT has higher perspective on safety. Perspectives of people conservation, labor conservation, and automation should be incorporated.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	50	Group	Appendix B 2nd layer	Transmission of illicit commands and service disability (DoS) are not included.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	51	Group	Appendix B 2nd layer	It does not mention risks of data transmitted to unexpected recipients (Example: C2 server).	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	52	Group	Appendix B 2nd layer 3rd layer	It does not consider internal threats, such as inside job and human error.	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	53	Group	Appendix B 2nd layer 3rd layer	It contains measures not relevant to security, such as CPS.IP-5.	Regarding your commnents, we leave the contents as original.
34	54	Group	Appendix B 3rd layer	Doesn't collaboration with other organizations that are concerned require SLO or SLA conclusion?	Regarding your commnents, we leave the contents as original.
34	55	Group	Appendix B 3rd layer	Shouldn't the locus of responsibility (by the unit of division) be clarified for data protection?	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	56	Group	Appendix B 3rd layer	Isn't the definition of confidentiality level necessary before the level of encryption strength for data encryption?	We revised the content, taking into account your comments. Relevant part : Appendix B
34	57	Group	Appendix B 3rd layer	Aren't restrictions on OS and software update necessary?	Regarding your commnents, we leave the contents as original.
34	58	Group	Appendix C	Isn't it better to clarify the determination criteria for <High Advanced>, <Advanced>, and <Basic>? For example, <Basic> is documentation, <Advanced> is the fact operation is thoroughly performed, and <High Advanced> is the facts that automation is being promoted and that periodical audits and improvements are performed.	We used your comments as a reference in revising the content. Relevant part : Appendix C
34	59	Group	Appendix C CPS.GV-2	I think it is cleaner to define the measure requirement as "internal rules according to laws/guidelines are formulated" and define "review and revise the rules on a continuing and timely basis", etc. as examples of security measures for <High Advanced> .	We revised the content as suggested in your comments. Relevant part : Part III CPS.GV-2 , Appendix C CPS.GV-2
34	60	Group	Appendix C CPS.RA-6	The connection between <High Advanced> and <Advanced> is unclear.	Unlike <Advanced>, <High Advanced> states that safety risk assessment and security risk assessment are integrated and implemented.
34	61	Group	Appendix C CPS.RM-1	It is not clear what the management reviews.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.RM-1
34	62	Group	Appendix C CPS.RM-2	What defines “important business partners”? In addition, what will be the interview frequency and contents of questions? Aren't the objectives to recognize, tolerate, and share risks instead of interviewing?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.RM-2

ID	No	Affiliation	Place	Comments	Responses to Comments
34	63	Group	Appendix C CPS.SC-1	The “security measure criteria regarding supply chain” is unclear.	It refers to security measures of business partners, or security measures applied to products and services provided.
34	64	Group	Appendix C CPS.SC-2	The directions of the 2 examples of security measures under <High Advanced> are not consistent.	The first measures are to prioritize the business of the organization and resources.The second measures are to estimate how much security incidents at a business partner affect business and resources, and how likely it is. Regarding your commnents, we leave the contents as original.
34	65	Group	Appendix C CPS.SC-2	I think specific standards are required when implementing the examples of security measures under <Basic>.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-2
34	66	Group	Appendix C CPS.SC-2	The writing of the below example of security measures is too long and unclear: “When the organization selects a business partner (service provider), it is desirable to select a service provider who has obtained an ITSMS certification based on JIS Q 20000 or is found to have implemented the equivalent measures based on self declaration of conformity and who operates and manages IT services it offers efficiently and effectively.”	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.SC-2
34	67	Group	Appendix C CPS.AC-1	Does automation of management of their system account really exist?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-2
34	68	Group	Appendix C CPS.DS-14	Shouldn’t the example of security measures “Whether or not it has tolerance against physical attacks” be moved to <Basic>?	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.DS-14
34	69	Group	Appendix C CPS.AE-1	Doesn’t the OT domain require monitoring other than the means of mechanism or application of a policy in place of monitoring?	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.AE-2
34	70	Group	Appendix C CPS.AE-2	The examples of security measures of <Advanced> should add the note to include the data linkage aspect not only within the organization but also between organizations.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.AE-2
34	71	Group	Appendix C CPS.AE-3	Shouldn’t there be a note saying that “sensors” here refer to those (previously mentioned), such as IDS, IPS, and SIEM, in terms of security measures (to be safe)?	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.AE-3
34	72	Group	Appendix C CPS.AE-3	Shouldn’t the examples of security measures of <Advanced> mention logging into edge devices, such as IoT?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AE-3
34	73	Group	Appendix C CPS.CM-1	Why is only VoIP regarded specially?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.CM-1
34	74	Group	Appendix C CPS.CM-1	Shouldn’t there be a note regarding the fact that networks are not limited to computers, such as attacks on composite devices via fax lines?	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.CM-1
34	75	Group	Appendix C CPS.CM-2	Is setting of physical access control not included because it’s obvious?	Please refer to CPS.AC-2.
34	76	Group	Appendix C CPS.CM-3	The meaning of “real-time scanning of files from external sources” seem unclear.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.CM-3
34	77	Group	Appendix C CPS.RP-1	Shouldn’t actions, such as shutting down in case of abnormality, included in <High Advanced> be taken in <Basic>?	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.RP-1
34	78	Group	Appendix C CPS.RP-1	Regarding the examples of security measures under <Basic>, wouldn’t the decision of whether or not measures are required require the decision-making criteria mentioned in <Advanced>? Measures under <Basic> alone are not possible, so this fails.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.RP-1
34	79	Group	Appendix C CPS.CO-2	The meaning of “Remain aware of the positive side” is unclear.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.CO-2
34	80	Group	Appendix B L1_1_b_DAT	Shouldn’t it include consideration of the fact security devices to detect man-in-the-middle attacks have not been introduced as a vulnerability and its measure requirement to implement security devices that can detect man-in-the-middle attacks in the communication network?	We revised the content, taking into account your comments. Relevant part : Appendix B L1_1_b_DAT
34	81	Group	Appendix B L1_1_c_SYS	Shouldn’t the response of physical devices in case of communication shutdown be stipulated?	Please refer to L1_3_a “Your organization can not continue business properly due to your own security incident”.
34	82	Group	CPS.GV-4	Shouldn’t we also consider risks not only in cyber space but also in physical space?	We revised the content, taking into account your comments. Relevant part : Part III CPS.GV-4
34	83	Group	Appendix B 1st layer	Regarding the assumed security incident “Security measures that satisfy the legal requirements for a system cannot be implemented”, since the METI and IPA have issued various guidelines, shouldn’t this section at least include reference to relevant guidelines?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.GV-2

ID	No	Affiliation	Place	Comments	Responses to Comments
34	84	Group	Appendix B L1_3_a_SYS	Since IIoT devices can bypass its own organization's network, wouldn't monitoring be insufficient?	We used your comments as a reference in revising the content. Relevant part : Appendix B L1_3_a_SYS
34	85	Group	Appendix B L1_3_c_PEO	Wouldn't a security incident causing damage to components (products) and/or services also be a vulnerability? In addition, wouldn't it be necessary to take appropriate measures, such as collection, for components (products) that are assumed to possess some sort of quality fault by paying off the facilities that were damaged in a security incident, as a measure requirement?	Regarding your commnents, we leave the contents as original.
34	86	Group	Appendix B L2_3_a_ORG	It's not possible for the introducer side to check the implementation of the tampering detection function. This would not work unless the introduction decision is made based on those guaranteed through a certification, etc. by special external organizations in the same manner as quality, etc.	The point you pointed out is considered as one of the ways to implement CPS.SC-4. Regarding your commnents, we leave the contents as original.
34	87	Group	Appendix B 3rd layer	Aren't "unable to transmit/receive data" as part of the assumed security incident and "data transmission/reception shutdown by device takeover" and "interference radio wave transmission" as risk sources required?	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	88	Group	Appendix C CPS.AM-2	The meaning of "The organization identifies the conditions of outputs related to the requirements for monitoring and measuring throughout the processes of manufacturing and providing services" under <Advanced>/<Basic> is unclear. I would like more detailed explanations.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-2
34	89	Group	Appendix C CPS.BE-1	Regarding the examples of security measures under <Basic>, it is important to recognize business connections, but mandating sharing them may cause confusion in case of updates to business partners, etc. or may cause some people to miss the updates.	This measure is not intended to oblige business relationship reporting. Regarding your commnents, we leave the contents as original.
34	90	Group	Appendix C CPS.GV-4	Regarding "The organization tries to include necessary resources for implementing security-related risk management to all capital plans and investment management processes, and documents exceptions to this requirement" under <Advanced>, is it realistic to implement this on everything?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.GV-4
34	91	Group	Appendix C CPS.RA-1	Regarding the examples of security measures under <High Advanced>/<Advanced>, isn't it difficult for most companies to implement vulnerability tests on control systems?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.RA-1
34	92	Group	CPS.RA-2	With control systems, most companies are outside of the scope of SOC/CSIRT. I think many companies decide that this item is satisfied because of SOC/CSIRT for information systems.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.RA-2
34	93	Group	CPS.RA-4	The description of the measure requirements is unclear as to if the target systems only include information systems, only systems including IoT, or also control systems.	We used your comments as a reference in revising the content.
34	94	Group	Appendix C CPS.RA-4	What is the scope of risk assessment? (Does it include everything from control systems to information systems?) If "Risk Assessment Guide for Industrial Control Systems" is to be applied to everything, I think this will be a great burden to many companies even if it's only once a year. I want the sense of levels included here.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.RA-4
34	95	Group	CPS.RA-5	The difference between this and the CPS.RA-4 item is unclear.	CPS.RA-4 simply requires performing a risk assessment, and CPS.RA-5 should consider threats, vulnerabilities, possibilities, effects when actually evaluating risk in the assessment.
34	96	Group	Appendix C CPS.RM-1	Shouldn't <Basic> include "the organization clarifies the scope of responsibility and responsible people for cyber security risks"?	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.RM-1
34	97	Group	Appendix C CPS.SC-6	Shouldn't the examples of security measures of <Basic> include "the organization is able to recognize the risk for its own organization due to the occurred malfunction in case nonconformity is found in an audit or test for a business partner"?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-6
34	98	Group	Appendix C CPS.SC-9	Shouldn't the examples of security measures of <Basic> include "the organization is able to recognize incidents that may occur in its own organization"?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-9
34	99	Group	Appendix C CPS.SC-10	Shouldn't the examples of security measures of <Basic> include "the organization is always able to recognize the completion of contracts with other relevant organizations, such as business partners"?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-10
34	100	Group	Appendix C CPS.AC-5	Under <Basic>, there is a description "If the separation of duties is difficult to implement due to the shortage of human resources, etc.,". However, why don't you describe this as the minimum level instead of dividing by case?	Regarding your commnents, we leave the contents as original.
34	101	Group	Appendix C CPS.AC-7	The example of security measures under <Basic> says "establishes a data flow regulation policy", but shouldn't rules, such as data flow regulation policies, be included in the main text on the summary level?	We used your comments as a reference in revising the content. Relevant part : Part III
34	102	Group	Appendix C CPS.RA-1 CPS.DS-9 CPS.DS-10	Introduction of "vulnerability diagnosis tool" and "penetration test", which are included in the examples of security measures for CPS.RA-1, to the OT field is difficult. In the same manner, introduction of "automated tool", which is mentioned as an example of security measures under <High Advanced> for CPS.DS-9, and "integrity verification tool", which is mentioned as an example of security measures under <Advanced> for CPS.DS-10, to the OT field is difficult.	We used your comments as a reference in revising the content. Relevant part : Appendix C

ID	No	Affiliation	Place	Comments	Responses to Comments
34	103	Group	Appendix C CPS.DS-12	In order to regularly check that the IoT devices and the installed software are genuine products by using the serial number and hash of the device, why not propose introduction of asset management tools?	We revised the content, taking into account your comments. Relevant part : CPS.DS-12
34	104	Group	Appendix C CPS.IP-9	Aren't the examples of security measures under <High Advanced> on the <Advanced> level? In addition, isn't review of "staff members" mentioned in <Basic> on the <Advanced> or <High Advanced> level, depending on the contents of the review?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.IP-9
34	105	Group	Appendix C CPS.IP-10	Regarding the reference mentioned in <Basic>, it is more difficult to carry out application of patches to control devices than IoT devices.	We revised the content, taking into account your comments. Relevant part : CPS.IP-10
34	106	Group	Appendix C CPS.MA-1	I think the example of security measures "The organization inspects the devices and/or tools for maintenance brought in by the staff members who update its IoT devices and servers in order to make sure that no inappropriate or unauthorized changes will be made" under <High Advanced> can be under <Advanced>, depending on the contents of the inspection.	Regarding your commnents, we leave the contents as original.
34	107	Group	Appendix C CPS.MA-2	I think the example of security measures under <High Advanced> can be under <Advanced>. I think the example of security measures under <Advanced> can be under <Basic>.	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.MA-1
34	108	Group	Appendix C CPS.PT-3	The example of security measures under <High Advanced> says "intrinsic safe designing", but I think the discussions of intrinsic safe designing and efforts of Connected Industries/ Smart Factory are completely different. I think intrinsic safe designing is something that should be considered at the time of new establishment or complete update of a plant, and I do not think intrinsic safe designing is something that should be reviewed according to IIoT and data utilization. I think it is welcome to hold discussions to reduce the frequency of unstable conditions due to security incidents and the level of impact in case of such incidents, but I think the point of discussion is different for intrinsic safe designing.	Regarding your commnents, we leave the contents as original.
34	109	Group	Appendix B	This does not mention risk analysis results and process to tolerate risks.	We revised the content, taking into account your comments. Relevant part : Part II
34	110	Group	Appendix B 1st layer	This does not mention wiretapping (man-in-the-middle attacks) as a risk source for data leakage.	We revised the content, taking into account your comments. Relevant part : Part II
34	111	Group	Appendix B 2nd layer	Shouldn't maintenance personnel be mandated to come along?	Maintenance personnel is described in CPS.AC-2, CPS.CM-2. Regarding your commnents, we leave the contents as original.
34	112	Group	Appendix B L2_3_b_ORG	The measure requirement in response to the vulnerability of being unclear about the status of devices says "Document and save the list of those composing the system", but shouldn't there be inventory-taking and updates periodically?	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-1 , Appendix C CPS.AM-1
34	113	Group	Appendix B 3rd layer	Only "DoS" is mentioned as a threat, but aren't there other attack methods/threats?	We revised the content, taking into account your comments. Relevant part : Appendix B
34	114	Group	Appendix B 3rd layer	While this includes security requirements for confidential information and measures in response to attacks, this does not mention human errors (such as setting mistake).	We used your comments as a reference in revising the content. Relevant part : Appendix B
34	115	Group	Appendix C	While these are not specific policy examples or something that provides a guarantee that "you are safe as long as you do this!" (expectation of users), they are effective as tools to give readers the triggers to consider security measures.	Your comments are considered as positive feedback on this framework.
34	116	Group		Comprehensiveness of risk sources and response requirements is high, and it seems that they included items that are effective in a wide range of industries. They are very effective to be used as a checklist to consider security measures. It is very helpful to companies to have some sort of foundation. On the other hand, I did have the impression that it was unclear from which section I should start referring to, due to the high level of comprehensiveness.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	117	Group		I think it would be an even better framework if measures with greater effect (those with overlapping measure requirements in Appendix B) are clarified.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	118	Group	Appendix C	The categorization standard of <Basic>, <Advanced>, and <High Advanced> for examples of security measures is vague. I think it would be difficult to determine how far they should go if a company is to operate the framework in their organization. Also, aren't <Basic>, <Advanced>, and <High Advanced> for examples of security measures in the order of difficulty? Shouldn't they be in the order of priority?	The categorization standard of <Basic>, <Advanced>, and <High Advanced> for examples of security measures is judged comprehensively by referring to the operation level of the measure, the scope of application of the measure, priority, and other guidelines. We would like to continuously consider appropriate the categorization standard. Relevant part : Appendix C

ID	No	Affiliation	Place	Comments	Responses to Comments
34	119	Group		Wouldn't it be difficult to operate this framework based on the power relationship between the contractor and contractee?	We will consider efforts to implement the framework in society regardless of the relationship between companies and organizations.
34	120	Group	Appendix B 1st layer	While intrusion is expected as an expected threat, physical destruction does not exist.	We revised the content, taking into account your comments. Relevant part : Appendix B
34	121	Group	Appendix B 1st layer	Since IoT is a field that has just started, shouldn't we need the process to comprehend the soundness of companies that provide the corresponding devices first?	Regarding your commnents, we leave the contents as original.
34	122	Group	Appendix B 2nd layer	Shouldn't the concept of standards for products themselves be established? If we should introduce products that satisfy standards in order to prevent poor quality products, followings guides would not be able to support.	Please refer to CPS.SC-4 <Advanced> which gives an example of certification for a product that implements a specific security function.
34	123	Group	Appendix C	Considering the order of reading as well as the implementation order, it is easier for this to be written in the order of Basic -> Advanced -> High Advanced. This is due to the fact that those implementing Advanced would take such measures after implementing Basic.	Regarding your commnents, we leave the contents as original.
34	124	Group	Appendix C CPS.AM-1	Isn't the main objective management itself, rather than documentation? In addition, maybe a little more focus should be given to introduction of management systems.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-1 , Appendix C CPS.AM-1
34	125	Group	CPS.AM-2	It seems that the main objective is to ensure traceability of products, but it is not very clear from the measure requirements. In addition, the differentiation of words, such as "identify" and "specify", is unclear.	We revised the content, taking into account your comments. Relevant part : CPS.AM-2
34	126	Group	Appendix C CPS.AM-5	The measure requirements and examples of security measures after <Advanced> do not match. If it's necessary to manage the external information systems to be utilized, this should be included in the requirement.	We revised the content, taking into account your comments. Relevant part : Part III 3.1. CPS,AM-5
34	127	Group	Appendix C CPS.AM-6	Shouldn't the contents of examples of security measures under <High Advanced> really be performed in <Basic>? The examples of security measures under <Basic> lean too much toward information systems.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-6
34	128	Group	Appendix C CPS.AM-7	This leans too much toward elements, such as compensation for damages and disclaimer, and lacks descriptions on decisions regarding security requirements, which should really be considered.	Regarding your commnents, we leave the contents as original.
34	129	Group	Appendix C CPS.BE-2	Shouldn't the examples of security measures under <High Advanced> and <Basic> be the other way around? Prioritization of the organization should be performed in <Basic>.	We revised the content, taking into account your comments. Relevant part : Part III 3.1. CPS,BE-2
34	130	Group	CPS.BE-3	The reason to differentiate CPS.BE-1 and CPS.BE-2 is unclear.	CPS.BE-3 itself does not directly recall security measures, but it is stated as a separate measure requirement with the intention of being an input to CPS.BE-1 and CPS.BE-2.
34	131	Group	Appendix C	There are 3 steps in the measures of Appendix C, and I feel that ingenuity has been practiced to enable businesses of various security levels to utilize the framework. However, I feel that <Basic> compromises with the minimum measures that can realistically be performed by businesses, and I wondered if they are truly effective measures.	We would like to continuously improve the contents, taking into account your comments.
34	132	Group		There are some parts without correspondence between threat and measure, and there are many descriptions on overlapping threats and measures. In addition, the contents of descriptions in general are unclear with some parts that are difficult to understand. Due to this, it is hard to picture practical utilization for businesses to directly utilize it.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	133	Group	CPS.AM-2	This says "identifying dependencies … by the organization's supply chain", but isn't the scope too large?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AM-2
34	134	Group	Appendix B L2_1_a_COM	Aren't "devices" mentioned for vulnerability for "components" "IoT devices"?	We revised the content as suggested in your comments. Relevant part : Appendix B L2_1_a_COM
34	135	Group	Appendix B L2_1_b_SYS	Isn't authentication insufficient as vulnerability of "system"?	Regarding your commnents, we leave the contents as original.
34	136	Group	Appendix B L2_1_b_COM	I feel a sense of wrongness with a fact that physical blocking is a measure requirement in response to the fact "settings are not robust enough".	We used your comments as a reference in revising the content. Relevant part : Part III 3.10. CPS.IP-2
34	137	Group	CPS.AE-1	Aren't "baseline of network operations" and "identify and manage… the expected data flows between people, goods, and systems" different measures? It is unclear when they are next to each other.	Regarding your commnents, we leave the contents as original.
34	138	Group	Appendix B L2_1_b_ORG	[Organization] Regarding the vulnerability "the organization has no mechanism for regularly checking proper use of its network", a measure requirement of permanent monitoring to conduct network and access monitoring. The vulnerability and measure do not match.	We used your comments as a reference in revising the content. Relevant part : Appendix B L2_1_b_ORG
34	139	Group	Appendix B 2nd layer	Shouldn't the assumed security incident "Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices" be "Unauthorized input to the IoT device due to unauthorized access to the system that remotely manages the IoT devices, causing the devices to behave in previously unexpected ways"?	We revised the content as suggested in your comments. Relevant part : Appendix B

ID	No	Affiliation	Place	Comments	Responses to Comments
34	140	Group	Appendix B 2nd layer	Isn't "being infected with malware falsifying control signals" a threat for the assumed security incident "Behavior that threatens safety, regardless of the behavior being normal or abnormal"?	We used your comments as a reference in revising the content. Relevant part : Appendix B L2_2_a
34	141	Group	Appendix B L2_3_a_ORG	This should be "tampering detection function and tampering prevention function" instead of "tampering detection function".	We revised the content as suggested in your comments. Relevant part : Appendix B L2_3_a_ORG
34	142	Group	Appendix B 2nd layer	Isn't "sensor's read values are falsified" also a threat for the assumed security incident "An unauthorized or tampered-with IoT device connects to the network and transmits incorrect data"?	We used your comments as a reference in revising the content. Relevant part : Appendix B L2_3_b
34	143	Group	Appendix B 3rd layer	The descriptions between "receives…data" under the assumed security incident and "data transmission/reception" under the risk source don't match.	We revised the content, taking into account your comments. Relevant part : Part III 3.1. CPS,BE-2
34	144	Group	Appendix C 3rd layer	Shouldn't the example of security measures "use a vulnerability diagnosis tool that can immediately update the vulnerability of the system to be diagnosed" under <High Advanced> be corrected to "use a vulnerability diagnosis tool that can immediately update the vulnerability database of the system to be diagnosed"?	We revised the content as suggested in your comments. Relevant part : Appendix C CPS.CM-7
34	145	Group	CPS.RM-1	Who are "relevant parties"?	We revised the content, taking into account your comments. Relevant part : Part III 3.1. CPS,RM-1
34	146	Group	Appendix C CPS.RM-2	It seems that "…performed in CPS.BE-1" is included in both <High Advanced> and <Advanced>.	We revised the content, taking into account your comments. Relevant part : Part III 3.1. CPS,RM-2
34	147	Group	Appendix C	Descriptions on risk assessment and risk management are excessively included in detail over multiple pages.	Risk assessment and risk management are recognized as very important and fundamental responses in implementing security measures. Regarding your commnents, we leave the contents as original.
34	148	Group	Appendix C CPS.AC-9 CPS.DS	Measures from the IT side are excessively included in detail regarding password authentication and encryption.	We used your comments as a reference in revising the content. Relevant part : Appendix C AC-9, CPS.DS
34	149	Group	Appendix C CPS.CM-2	Too much is written regarding entry control in the examples of security measures under <Advanced>, and the granularity is different from <High Advanced> and <Basic>.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.CM-2
34	150	Group	Appendix C CPS.RA-2	Regarding external sources, it lacks descriptions on cyber intelligence.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.RA-2
34	151	Group	Appendix C CPS.AC-3	In OT, all of the handled information is expected to have high confidentiality.	It is assumed that the importance of information, including confidentiality, will be defined at the discretion of the company actually managing the information.
34	152	Group	Appendix C CPS.AC-4	In OT, critical infrastructure services would be affected if re-login is blocked for a certain period.	We used your comments as a reference in revising the content. Relevant part : Appendix C AC-4
34	153	Group	Appendix C CPS.AC-7	There is no description on physical network separation.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.AC-7
34	154	Group	Appendix C CPS.DS-5	While resources for DoS attacks, etc. are mentioned, there is no mention regarding detection.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.CM-1
34	155	Group	Appendix C CPS.CM-3	Validation that data handled by IoT devices and server devices is within the permissible range should be included under <Basic>.	We revised the content, taking into account your comments. Relevant part : Appendix C CPS.CM-3
34	156	Group		While the focus is on threats of and measures against data leakage and data falsification, the description granularity for fraudulent operation of devices, etc. is too rough, making it difficult to be utilized for actual threat analysis, etc. (Reference: Similar opinion) - There are many descriptions about data leakage and falsification, there are few descriptions regarding threats related to component control (unexpected operation, function shutdown, etc.)	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
34	157	Group	Appendix C	In examples of security measures, the lower-level description of "to do …" and higher-level description of "specific measure to do…" are difficult to understand.	There was no corresponding statement.
34	158	Group		Compared to the fact that the descriptions of the main text are progressive, specific theories in Appendix B and later are on the ISMS basis in principle, not responding to IoT and leading technologies.	We will use your comments as a reference in advancing cyber security policies in the future.
34	159	Group	Appendix B	Terminology is for IT engineers, so it might be better to use simple terminology. For example, shouldn't "contingency plan" in CPS.IM-2 be replaced with another expression?	We used your comments as a reference in revising the content. Relevant part : Appendix B

ID	No	Affiliation	Place	Comments	Responses to Comments
34	160	Group	Appendix C	IT, OT, and IoT are mixed in examples of security measures, so please categorize them.	We revised the content, taking into account your comments. Relevant part : Appendix C
34	161	Group	Appendix C	The difficulty level may differ in some cases, depending on the scope of application. Due to this, it may be good to have a column for the scope of application.	We used your comments as a reference in revising the content. Relevant part : Appendix C
34	162	Group		I would like to edit and utilize this, so please also disclose this in the Excel format.	We will consider the publication method, taking into account your comments.
34	163	Group	CPS.AM-1 CPS.RA-1	IIoT devices should be included in the management information as devices requiring security management and vulnerability management.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-1 , 3.4. CPS.RA-1
34	164	Group	CPS.DS-8 CPS.SC-11	This uses “entity” and “procedure” in IT terms, but these words should be replaced for OT users.	We used your comments as a reference in revising the content. Relevant part : Appendix E
34	165	Group	CPS.RA-1	It is unclear from the writing if this is referring to identifying vulnerabilities and preparing a list of tolerated assets.	We used your comments as a reference in revising the content. Relevant part : Part III 3.4. CPS.RA-1
34	166	Group	Appendix C CPS.AM-1	What is the scope and granularity of asset inventory to be performed under <Basic>? In addition, how is the level of importance under <Basic> determined? For example, the reality is that only the vendors know about sensors and controllers. Since the number of sensors and controllers is great, it requires an impossible level of physical endurance to position them under the <Basic> level. It also requires physical endurance to determine the level of importance.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1 Asset Management CPS. AM-1
34	167	Group	Appendix C	Is it ok that <Advance> and <Basic> are common? I don’t understand the difference from where it says “<Basic> N/A”. Shouldn’t the style of description be unified?	We used your comments as a reference in revising the content. Relevant part : Appendix C
34	168	Group	Appendix C CPS.AM-2	The contents are too vague and not clear as to what needs to be done. Isn’t it impossible to expect “throughout the processes” under examples of security measures under <Basic>?	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-2
34	169	Group	Appendix C CPS.AM-3	The example of security measures that are common for <Advance> and <Basic> seems to only describe the measure requirement using different words and is not an example of security measures.	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-3
34	170	Group	Appendix C CPS.AM-4	Rollback of firmware for IoT devices and OT devices is not possible. Due to this, in order to satisfy the rollback requirement, don’t we need to possess spare controllers and IoT devices themselves?	We used your comments as a reference in revising the content. Relevant part : Part III 3.1. CPS.AM-4
34	171	Group	Appendix C CPS.AM-4	What is the unit of organization to identify system configurations under <Basic>? I think it is difficult to identify system configurations of all companies.	It is desirable to cover all systems in the organization, but if it is difficult due to problems of labor, budget etc., we recognize that it is important to prioritize the configuration of systems with a certain level of importance or more with reference to the level of importance defined in CPS.AM-5. We used your comments as a reference in revising the content. Relevant part : Part III 3.1 Asset Management CPS. AM-4
34	172	Group	Appendix C CPS.BE-1	Customers are ones that consider the supply chain. Isn’t it enough for small and medium enterprises to represent the overview according to the customers?	Companies in the supply chain upstream (including SMEs) are assumed to be dealing with multiple downstream companies within an industry or across industries, so the impact of the company's incidents may be propagate. Therefore, it is not the case that the supplier should consider measures that take into consideration the supply chain, but it is desirable that management be implemented appropriately from the perspective of supply chain risk management, including upstream companies.
34	173	Group	Appendix C CPS.BE-2	Shouldn’t “the organization also considers whether there is a harmful effect on health, safety, and environment (HSE) caused by an inappropriate operation of the organization’s business activities when classifying and giving priorities to resources” under <High Advanced> be categorized under <Basic>?	We revised the content, taking into account your comments. Relevant part : Part III 3.2. CPS.BE-2
34	174	Group	Appendix C CPS.BE-3	“The organization identifies suppliers which have important dependence relationships for the continuation of its business” under <High Advanced> is something that is conducted in the course of business plan formulation, so shouldn’t it be under <Basic>? I have the impression there is an overlap with other items, and so if you apply it in order from the beginning, there is the possibility that you'll be conducting the same thing twice.	We revised the content, taking into account your comments. Relevant part : Part III 3.2. CPS.BE-3
34	175	Group	Appendix C CPS.GV-1	Is it ok to understand that control systems do not need to respond to <Basic> and <Advanced>?	We think that it is difficult to apply to the industrial control system the security policy with some contents detailed, which was formulated mainly for the information system. On the other hand, we think that it is necessary to respond as much as possible about the security policy of more abstract description.

ID	No	Affiliation	Place	Comments	Responses to Comments
34	176	Group	Appendix C CPS.GV-2	Is it ok that the same examples of security measures are used in all of <High Advanced>, <Advanced>, and <Basic>?	Since compliance with laws and regulations is considered to be a basic requirement to conduct business, <High Advanced>, <Advanced> and <Basic> are described in common. Regarding your commnents, we leave the contents as original.
34	177	Group	Appendix C CPS.GV-4	This should also mention that a long-term perspective should be included for management strategy. Short-term perspective should be under <Advanced> or <Basic>.	We used your comments as a reference in revising the content. Relevant part : Part III 3.3. CPS.GV-4
34	178	Group	Appendix C CPS.RA-2	Obtaining the latest security information also in the OT field should be required under <High Advanced>.	We revised the content, taking into account your comments. Relevant part : Part III 3.4. CPS.RA-2
34	179	Group	Appendix C CPS.RA-4	The example of security measures “the organization analyzes a situation where a hazard leads to damage and clarifies the possibility of occurrence and the severity of the damage to estimate a possible risk. At the time, it is desirable to check whether there is any hazard caused by a security issue” under <High Advanced> should be conducted under <Basic>. Otherwise, the scope of application will be unclear.	Implementation of security measures considering safety is described in CPS.RA-6 <High-Advanced>. Regarding your commnents, we leave the contents as original.
34	180	Group	Appendix C CPS.RA-5	Shouldn’t automating risk assessment and sharing threats and vulnerabilities with stakeholders of the supply chain be included as an example of security measures under <High Advanced>?	We used your comments as a reference in revising the content. Relevant part : Part III 3.4. CPS.RA-5
34	181	Group	Appendix C CPS.RA-6	Which items are the example of security measures under <Basic> referring to by “the following items”?	We used your comments as a reference in revising the content. Relevant part : Part III 3.4. CPS.RA-6
34	182	Group	Appendix C CPS.SC-1	Shouldn’t the example of security measures “the organization makes clear to business partners (external information system service providers) of necessary functions, ports, and protocols for the use of the services, along with other services” under <High Advanced> be categorized under <Basic>? This is especially the case if they are using external services.	We used your comments as a reference in revising the content. Relevant part : Part III 3.6. CPS.SC-1
34	183	Group	Appendix C CPS.SC-3	Shouldn’t <High Advanced> require satisfaction by all relevant parties in the supply chain (including sub-contractors, sub-sub-contractors, and following contractors)?	We used your comments as a reference in revising the content. Relevant part : Part III 3.6. CPS.SC-3
34	184	Group	Appendix C CPS.SC-3	What are “potential risks in terms of legal regulations that may arise due to difference of applicable laws”?	As an example, there may be cases where different legal systems are applied depending on the location of the data center in using the cloud service. We used your comments as a reference in revising the content. Relevant part : Appendix C CPS. SC-3
34	185	Group	Appendix C CPS.SC-3	Vendors and SIer seem to have extreme disadvantages. Since this contradicts other contract-related laws, it doesn’t seem to possess effectiveness.	We used your comments as a reference in revising the content. Relevant part : Part III 3.6. CPS.SC-3
35	1	Corporation		We appreciate METI’s public consultation process, including the extended review time allowed for this updated draft, as well as its interest in receiving comments from and engaging with global stakeholders. We are encouraged by the Government of Japan’s vision for “Society5.0” as well as METI’s intention to support this vision through its Connected Industries program. As described in the draft Framework’s introduction, Internet of Things (IoT) and Artificial Intelligence (AI) technologies have the power to transform our lives and societies, creating “new value” in a “human-centered society.” Likewise, from our perspective, “AI will enable humans to harness vast amounts of data and make breakthrough advances in areas like healthcare, agriculture, education and transportation. We’re already seeing how AI-bolstered computing can help doctors reduce medical mistakes, farmers improve yields, teachers customize instruction and researchers unlock solutions to protect our planet.” However, as METI has recognized in providing context for the draft Framework, a more digitally connected society in which “cyberspace and physical space” are more significantly integrated will impact cybersecurity risk exposure.3 As a result, the implementation of effective approaches to cybersecurity risk management is increasingly important, both to support organizations’ operations and continuity and to strengthen an interconnected ecosystem. Without foundational cybersecurity risk management practices in place, organizations may also struggle to sustainably integrate the advanced technology that will contribute to a realization of Society5.0. Moreover, without interoperability of foundational cybersecurity risk management approaches across sectors and regions, the potential benefits of global value chains and more dynamic, less linear “value creation processes” may be limited or undermined.	Your comments are considered as positive feedback on this framework.

ID	No	Affiliation	Place	Comments	Responses to Comments
35	2	Corporation		Our perspective on the draft Framework is based on our enterprise risk management experience as well as our recognition of the benefits of cybersecurity policies and requirements that are interoperable across sectors and regions. In the draft Framework, METI has given considerable attention to the interoperability of its proposed security measures with those articulated in international standards and best practices, including ISO/IEC 27001:2013, ISA 62443, the Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (the "Cybersecurity Framework"), and the Council on CyberSecurity "Critical Security Controls." In particular, we find value in METI's effort to utilize the Cybersecurity Framework Categories, which provide a helpful framing for cybersecurity risk management activities that have relevance for organizations across various sectors and regions. Likewise, efforts to demonstrate alignment with – and including a mapping of measures to – the Cybersecurity Framework Subcategories and ISO/IEC 27001 controls increase the draft Framework's utility for more organizations.	Your comments are considered as positive feedback on this framework.
35	3	Corporation		To further advance the considerable investment that METI has made toward ensuring organizations understand how its proposed security measures are interoperable with international standards and best practices, we encourage METI to consider adding ISO/IEC 27103 to its list of references and Part III or Appendix D mapping efforts. ISO/IEC 27103 brings together numerous references already incorporated in the draft Framework, including ISO/IEC 27001 and the Cybersecurity Framework, along with a number of other ISO and IEC standards relevant for cybersecurity risk management (e.g., to include ISO 31000, which is also referenced in the draft Framework). Furthermore, in including a mapping to IEC standards, ISO/IEC 27103 is particularly relevant for a broader set of sectors, helping to demonstrate alignment of cybersecurity risk management practices across various connected industries. Moreover, as a significant contributor to the development of ISO/IEC 27103, METI is well positioned to articulate and demonstrate its value to both local and global stakeholders tracking and leveraging its guidance.	This framework has been formulating with reference to major international standards. In addition, since new international standards etc. are always established, we will constantly revise it appropriately with reference to various international standards etc. even after it is established, taking into account your comments.
35	4	Corporation		Complement the draft Framework's comprehensive approach by offering simplified guidance tailored to particular stakeholders, such as executives, directors of enterprise risk management, or managers of groups focused on supply chain security or IoT deployment As a comprehensive document that describes not only on the conceptual underpinnings of its structure but also an assessment of risk sources, a set of proposed security measures, and mapping to multiple international standards and best practices, the draft Framework represents a significant undertaking and body of work. While there is likely value in having all of that content combined in one document for some organizations and stakeholders, others may find it challenging to recognize what content is most relevant for them based on their role and ability to operationalize the draft Framework's guidance.	This framework provides an overall framework for security measures. We will consider approaches to more effective cyber security measures according to the scale of industrial activities and the position of stakeholders.
35	5	Corporation	Appendix C	Foster operational agility and appropriate focus through risk-based and outcomes-focused approaches Risk-based and outcomes-focused approaches to cybersecurity risk management help organizations apply resources in a prioritized way and ensure sufficient agility and adaptability as organizational missions change and the technology and threat landscapes evolve.6 Many areas of the draft Framework include guidance that is consistent with a risk-based and outcomes-focused approach, but there are also opportunities to further embed both principles. For instance, CPS.AC-6, "Adopt multi-factor authentication, combining more than two types of authentication when logging in to the system over the network for the privileged user," helpfully advocates for the use of an important security technology, but it does not account for other advanced technology or potential future developments (e.g., biometrics). We encourage METI to consider more outcomes-focused and risk-based language, such as: "Access permissions and authorizations are managed, incorporating the principles of least privilege, separation of duties, and high confidence methods of authentication where appropriate based on risk." In addition, within Appendix C, we encourage METI to reflect that varying degrees of investment in security measures may not necessarily correlate with levels of advancement but rather with appropriate investments based on business objectives and priorities as well as risk assessments and broader mitigation strategies.	We used your comments as a reference in revising the content. Relevant part : Part III 3.7. CPS.AC-6

ID	No	Affiliation	Place	Comments	Responses to Comments
35	6	Corporation		Contribute to, raise awareness of, and integrate learnings from global collaborative efforts to address IoT security where appropriate The draft Framework helpfully acknowledges that risk profiles for connected devices will vary to some extent based on their use case and respective implementation. Electrical girds, healthcare devices, transportation, and factories might share certain capabilities and device classes, but their security profiles and adequate threat protection capabilities will not always be identical. The diversity of use cases and risk profiles for IoT creates more complexity for policymakers focused on this space. Still, while global best practices for baseline IoT security measures may not be as well defined or broadly recognized as in the context of cybersecurity risk management, there are numerous efforts that METI may consider, both in the context of IoT in general and in the context of more specific use cases. In the context of Industry 4.0, for example, the Industrial Internet Consortium's (IIC) Industrial Internet Security Framework7 describes necessary measures to secure IoT not just in the context of cyberspace but also in the physical realm (i.e., the security mechanisms needed for considering potential impacts on safety, resilience, and reliability). In addition, IIC's IoT Security Maturity Model builds on the concepts of their Internet Security Framework and defines different levels of security investments for organizations to achieve based on their business objectives and priorities as well as risks. This not only enables them to invest in security mechanisms that meet their specific use cases but also provides a mapping of how organizations that are facing resource constraints can evaluate their investments and continuously improve their management of cyber-physical systems as determined appropriate. To address the security of consumer IoT devices, the UK Government has published a Code of Practice for consumer IoT security. It sets out thirteen security guidelines that manufacturers of consumer IoT devices are encouraged to implement. The practices were mapped against published standards, recommendations, and guidelines from nearly 100 documents and 50 organizations. Due to this mapping, manufacturers are able to better understand the relationship between the Code of Practice and already existing material – from both industry and government – focused on consumer IoT. This makes it easier for developers to leverage existing and industry-acknowledged guidelines when implementing various practices. Moreover, instead of being prescriptive, the outcome-focused nature of these principles provides manufacturers sufficient flexibility to improve the security of their devices based on current best practices and then to evolve as better methods become available. Both manufacturers of IoT devices and customers using them will likely operate in international environments. Taking that into account, we encourage METI to contribute to and help raise awareness of global collaborative efforts and international standards that are growing in recognition within the marketplace – much like it has in the context of cybersecurity risk management. As a further reference, the U.S. National Institute of Standards and Technology (NIST) has also published a draft report that summarizes international efforts to standardize IoT cybersecurity. It provides a functional description of IoT based on use cases and describes different core cybersecurity areas, such as cryptography, incident management, or physical security, and maps them to international standards in each area. Leveraging international standards to secure their cyber-physical systems will help organizations operate in a global landscape and benefit from industry-supported practices and implementation guidelines.	Your comments are considered as positive feedback on this framework. Since new international standards etc. are always established, we will constantly revise this framework appropriately with reference to various international standards etc. even after it is established, taking into account your comments.
36	1	Corporation	0	Industrial structure by platformers are not assumed. 【Reason】 ・ Platforms represented by GAFA and BAT are the basis of economic activities (including transactions) of many companies and individuals, but in this framework, security risks (and credit risk) in the case of such industrial and business structures is not considered? ・ In the ecosystem deployed on the platform, various businesses (corporations and individuals) operate on the platform. These are businesses (such as Ad-hoc operators, individuals in cyberspace, operators of data sales, or automated transactions by AI) that are different from the old companies that are aiming for long-term survival and scale accumulation, and it is expected that business entities different from conventional companies will be more and more. ・ In this case, the security measures for platformers and businesses using the platforms should be described. ・ This is also necessary for the economic activity in the "place" of CPS between companies that exchange industrial data.	We understand that your comments are included in the third layer of this framework, the connection in cyber space. In Part II, measures can be organized by analyzing what to protect, security incidents, threats, and risk sources in each layer. We will use your comments as a reference in discussing security measures in each sector-specific or cross-sectoral SWG.

ID	No	Affiliation	Place	Comments	Responses to Comments
36	2	Corporation	0	There is a lack of consideration of security or trust in the new economic and social framework. 【Reason】 ・ In the conventional money economy, credit collateral such as money and banking system by “country” was one “root” of economic activity, but with decentralization, sharing, boundaryless economic activity now taking place, The framework of mutual trust on a decentralized basis represented by blockchains is expanding. ・In the past, commerce was based on credit in a relatively stable framework of country, central bank, financial institution, company ... but mutual trust was formed in a new framework different from that. ・It is also required to consider the way of security in such a new trust and mutual trust framework, and a decentralized, unregulated and dynamic framework.	In this framework, the supply chain in a new industrial society is defined as the value creation process. The risks in "the new credit and mutual trust framework, decentralized and dynamic framework" can be evaluated by using three-layer model and six elements.
36	3	Corporation	Part I 2.1	The division between companies, cyber physicals and cybers seems to be fundamentally lacking in relevance. 【Reason】 This is because the current collaboration between companies can be regarded as part of the collaboration between cybers.	Three Layers' model is described in Part I 2.1. Regarding your commnents, we leave the contents as original.
36	4	Corporation	6.	Please define global harmonization. 【Reason】 It is not appropriate to present it as a feature of the framework without the definition of the word global harmonization.	This framework has been formulating with reference to major international standards. Regarding your commnents, we leave the contents as original.
36	5	Corporation	6.	Please provide guidance on the choice of security level. 【Reason】 For example, when transferring logs of production facilities and environmental sensor data to the cloud and using them for productivity improvement or analysis of inter-factory production linkage, Level 1 for data transfer only. If you want to control the control system from the cloud (including the external system via), Level 2. I think that it may be considered to use combining measures of multiple security levels within the same system.	We used your comments as a reference in revising the content. Relevant part : Part III 2.
36	6	Corporation	p.17	It is uncomfortable to describe Cyber in one. 【Reason】 This is because cyber space also exists within a company, and there are multiple domains even in a cloud-like space outside the company.	Regarding your commnents, we leave the contents as original. We will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
36	7	Corporation	Table 1.2-1	It is considered that there is a shortage of ".. collected in physical space." 【Reason】 There are several types of data sources, such as master data (IoS) in a company and data obtained from people (IoP).	Regarding your commnents, we leave the contents as original.
36	8	Corporation	Appendix C CPS.AC-4	For the <Basic> security measures, it is better to use text that includes other credentials. 【Reason】 As it seems that only the password is mentioned about the validity period of the credential.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-4
36	9	Corporation	Appendix C CPS.AC-6	Does not mention the handling for shared account especially about the security measures <Basic>? 【Reason】 It looks like uniqueness to the account.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-6
36	10	Corporation	Appendix C CPS.AC-7	In the latter case, it is not possible to monitor / control the inner boundary of the external network for the <Advanced> security measures. Also, do you need to monitor / control internal boundaries at the <Advanced> level? 【Reason】 It seems unclear whether "a network to which the system of the organization is connected" is a network to which the system belongs or a network (an external network) to which the system belongs.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-7

ID	No	Affiliation	Place	Comments	Responses to Comments
36	11	Corporation	Appendix C CPS.DS-3	CPS.DS-2 requires encryption of the communication path for the <Advanced> security measures, but it may be redundant to require encryption even at the data level. 【Reason】 This requirement is considered to assume the case where the communication entity and the data processing entity do not match originally, but is not redundant in the case where the communication entity and the data processing entity match?	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.DS-2
36	12	Corporation	Appendix C CPS.DS-9	With regard to the <Advanced> security measures, "at startup" of the measure requirements and "regularly" of the security measures may contradict each other. 【Reason】 Because activation is not always performed regularly.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.AC-6
37	1	Corporation		We applaud METI's efforts to establish a forward-looking, risk-based Framework, which we believe will become an important tool for businesses to identify, evaluate, and manage security risks. We particularly appreciate the draft Framework's focus on "Society 5.0," in which all people and things are connected through the Internet of Things ("IoT"). We agree with METI that this new connectivity will create tremendous value, and agree it will require careful consideration of the accompanying security risks.	Your comments are considered as positive feedback on this framework.
37	2	Corporation		The development of 5G will enable the type of profound transformation the draft Framework seeks to address—by allowing greater integration of cyberspace and physical space. Japan has long recognized the benefits of this type of innovation. Indeed, Japan is already in the process of expediting its 5G launch, which was originally planned for the 2020 Tokyo Olympics. Now, 5G is scheduled for pre-commercial launch in Japan this year, followed by full commercial launch in 2020. The draft Framework reinforces this commitment to continued innovation.	Your comments are considered as positive feedback on this framework.
37	3	Corporation		We supports the draft Framework as an important mechanism for enabling businesses to identify, evaluate, and manage security risks in a highly-connected society. As IoT is deployed with low-cost sensors and actuators, increasingly sensitive information—including biometric data, location data, and infrastructure monitoring data—will flow over mobile networks. Despite this broad access and use of sensitive data, security features are not yet leveraged across the industry ecosystem or across the IoT applications that use mobile platforms. We are therefore encouraged by the draft Framework's efforts to assist companies in addressing these security risks, including its forward-looking use cases focused on connected cars, smart homes, building management, and electric power systems.	Your comments are considered as positive feedback on this framework.
37	4	Corporation		Continue the draft Framework's forward-looking approach, particularly on supply chain management. We agree with METI that as devices become increasingly connected, new supply chain issues will emerge. For example, IoT devices may be used to create new data and to control physical devices outside of the standard linear supply chain. Similarly, a consumer may use artificial intelligence to add value to data —thereby starting a supply chain that does not originate with traditional suppliers or manufacturers. To address the security issues posed by these dynamic supply chains, we encourage METI to continue its forward-looking assessment of security risks across all relevant entities. In doing so, we believe that the first link in the cybersecurity supply chain is the investment in long term research that form the foundation of any new technology system. If trusted companies are not at the forefront of such research, and standardizing it, or do not have funds to innovate, this link will not evolve. If that happens, the chain will break and the security of all connected devices and networks is affected. METI may consider establishment of a validation center that could assess potential attack surfaces in cellular infrastructure, and make recommendations on configuring such system to national carriers. The UK has had good results with this approach in their National Cyber Security Center. METI may also consider encouraging assessment of an entity's compliance with relevant international standards, including ISO, IEC, and NIST standards, especially with respect to the communication between cellular infrastructure components.	Your comments are considered as positive feedback on this framework.

ID	No	Affiliation	Place	Comments	Responses to Comments
37	5	Corporation		Continue to leverage leading global standards. We welcome METI's recognition that the draft Framework should be consistent with major standards in the United States and Europe. For example, Part III, Appendix C and Appendix D all include points of alignment between the draft Framework and major international standards, including ISO, IEC, and NIST standards. This not only ensures that enterprises that adopt measures to comply with the draft Framework will also satisfy other countries' security requirements, but it also promotes the use of leading cybersecurity practices across borders. Standards are a critical component of cyber and physical security. We encourage METI to build on the draft Framework by continuing to engage with its international counterparts to consider other methods for supporting the development of interoperable cybersecurity standards.	Your comments are considered as positive feedback on this framework.
37	6	Corporation		Ensure the Framework supports development of local, new models of cellular infrastructure manufacture. We respectfully suggest that METI look not only at the cybersecurity risks, but also at the opportunities presented by machine learning, AI, and Software Defined Networks. For example, we are watching the narrowing of the cellular infrastructure offerings down to just a handful of vendors. We have seen promising work by internet companies and new small players utilizing Software Defined Networking and off-the-shelf hardware, and believe this approach could be promising to attract new players into the cellular infrastructure market. METI may accordingly look at ways in which the Framework may stimulate a domestic infrastructure industry in Japan, which could benefit from the clear security standards and processes set out in the draft Framework.	We will use your comments as a reference in advancing cyber security policies in the future.
38	1	Corporation		This framework is a useful framework that has been created with practicality in mind when it is used, in that it refers to specific measures that are likely to be contrasted with global standards and lacking in many frameworks. In the future, I would like to expect that we will proactively publish internal and external cases (Success Stories) that utilize this framework, such as provided by NIST on the website *, from the perspective of diffusion. https://www.nist.gov/cyberframework/success-stories	Your comments are considered as positive feedback on this framework. We will use your comments as a reference in promoting this framework in the future.
38	2	Corporation		There are items about physical access control and media management. However, considering the meaning of physical security, it might make sense to add the following items newly (these items are written based on the contents of ISMS from KISA (Korean Information security agency).) 1. Designation of protected area 1) Objective It is necessary to designate physical protection zones such as secure zone, restricted zones and public zones and establish and implement protective measures for each zone in order to protect the main facilities and systems from unauthorized physical access andvarious physical and environmental disasters. 2) Item - In order to protect the main facilities and systems, the physical protection area is established and the zone protection measures are implemented. (example) . Public zone: outside area . Restricted zone: office area etc. . Secure zone: important facility and system area	Regarding your commnents, we leave the contents as original.

ID	No	Affiliation	Place	Comments	Responses to Comments
				2. Protection of facilities 1) Objective According to the importance and characteristics of each protected area, it should have enough facilities such as temperature and humidity control, fire detection, fire extinguishing equipment, leak detection, UPS, emergency electronic generator and duplicated power line. In addition, when important systems are operated through outsourcing vendors, security requirements should be reflected in contracts and reviewed periodically. 2) Item - Are the operational procedures established and managed in accordance with the importance and characteristics of each protected area with necessary equipment in preparation for fire, power failure and other disasters? - Are facilities installed and maintained to protect the main systems and personnel from fire in the protected area? - Are emergency bells, emergency lights and emergency pathway signs installed so that personnel can evacuate safely in the event of a fire or other disaster? - Are facilities installed to detect leaks to ensure that the main systems in the protected area are protected from flooding and are they continuously operated and maintained? - Are facilities providing a constant temperature and humidity installed and maintained? - Are facilities providing stable supply of electricity installed and maintained? - If important systems are operated through outsourcing vendors, are the security requirements for physical protection reflected in contracts and reviewed periodically?	
38	3	Corporation		There is no description about the human resources or human resources required to carry out the framework. After confirming, 2.2.6 “Table 1.2-1 Six components involved in the value creation process” of two components defines human. In addition, CPS.RA-2, CPS.AE-3, CPS.AE-2,3 describe personnel skills for SOC / CSIRT and incident response. Therefore, although comprehensively describing measures requirements and a collection of measures, human resources or human resources (skills) mention only SOC / CSIRT and incident response. If you comprehensively describe measures requirements and examples of measures, I think it is better to add the necessary skills for each measure.	The human resources skills are being discussed in "Study Group on Industrial Cybersecurity" WG 2 (Management, Human Resources, International). We will continue to consider the human resources skills required to utilize the framework.
38	4	Corporation	p.56, 80 etc	The words “Abnormal activities” and “Anomalies” appear to be used interchangeably, whereas the Japanese version uses the same word. The two words, anomaly and abnormality both refer to something that is not normal. Anomalies more focus on data those are collected. Abnormality has more of a negative implication. It is nearly always used to refer to something that is bad, whereas anomaly may or may not be bad.	We used your comments as a reference in revising the content. Relevant part : Part III 3.
38	5	Corporation	CPS.MA-1	Measure requirement of CPS.MA-1 does not match with NIST Cybersecurity Framework Ver.1.1 PR.MA-1 The Cyber/Physical Security Framework - Discuss and apply the method of conducting important security updates and the like on IoT devices and servers properly and in a timely manner. - Introduce IoT devices having a remote update mechanism to perform a mass update of different software programs (OS, driver, and application) through remote commands, where applicable NIST Cybersecurity Framework Ver.1.1 Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	We used your comments as a reference in revising the content. Relevant part : Part III 3.11. CPS.MA-1

ID	No	Affiliation	Place	Comments	Responses to Comments
38	6	Corporation	CPS.PT-2	Measure requirement of CPS.PT-2 is not enough to cover NIST Cybersecurity Framework Ver.1.1 PR.PT-2 and PR.PT-3. As described in PR.PT-3; The principle of least functionality is incorporated by configuring systems to provide only essential capabilities The Cyber/Physical Security Framework Physically block unnecessary network ports, USBs, and serial ports accessing directly the main bodies of IoT devices and servers. ---> Contents are limited to specific parts.	We used your comments as a reference in revising the content. Relevant part : Part III 3.12. CPS.PT-3
38	7	Corporation	D-3-8 A.9.2.1	A.9.1.1 Access controlpolicy/Access control policy A.9.2.1 A.9.2.1 User registration and deregistrationUser registration and de-registration Duplicate words are used.	We revised the content, taking into account your comments. Relevant part : Appendix D-3
38	8	Corporation	Part III CPS.AC-4 CPS.DS-5	CPS.AC-4 / CPS.DS-5 In case that the lockout mechanism is active, DoS condition may occur by intentionally making lockout attack. This attack cannot be prevented even if there are sufficient processing capacity and storage capacity. It is desirable to consider another measures against DoS such as behavior detection.	We revised the content, taking into account your comments. Relevant part : Part III
38	9	Corporation	Part III CPS.SC-2 CPS.MA-1	CPS.SC-2 / CPS.MA-1 It is desirable to check support lifecycle before use; use only the products for which support life cycle for the provision of updates and patches is defined; discard the system before the end of the support lifecycle. It is desirable not to use products whose support lifecycle is not defined.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.SC-2
38	10	Corporation	Part III CPS.CM-3	CPS.CM-3 does not match with NIST DE.CM-4 and DE.CM-5	We used your comments as a reference in revising the content. Relevant part : Part III 3.14 CPS.CM-3
38	11	Corporation	第III部	Wrong CIS references - Page 57 > CPS.AM-4 | CIS CSC 112 -> CIS CSC 11 - Page 70 > CPS.AT-2 | CIS CSC 917 -> CIS CSC 17 - Page 71 > CPS.DS-1 | CIS CSC 1713, 14 -> CIS CSC 13, 14 - Page 71 > CPS.DS-2 | CIS CSC 1713, 14 -> CIS CSC 14 - Page 71 > CPS.DS-3 | CIS CSC 1713, 14 -> CIS CSC 14	We revised the content as suggested in your comments.
38	12	Corporation		There are minor spelling errors throughout the document; e.g. page 7, section (3) amaong -> among. Please run spelling check.	We revised the content as suggested in your comments. Relevant part : Part 7.(3)
38	13	Corporation	CPS.CO	CPS.CO-2 states that "the point that tackles the restoration of the social evaluation for the organization is positioned," not only the social evaluation restoration for the organization but how about adding the point "assessing the impact of incidents on society and working on communication activities to prevent confusion throughout the society" to CPS. CO? 【Reason】 In a society where everything is connected, not only the impact caused by the incident on the whole society will be greater than before, and it is also assumed that one incident may trigger another. Although the example “inside and outside stakeholders” described in “3.17. CPS. CO – communication” does not include “region and society”, if certain incidents have occurred in recent years, the need for communication (information dissemination) to organizations that have caused an incident is increasing, and if "Connected Industries" gets more popular, they are expected to increase in the future.	We used your comments as a reference in revising the content. Relevant part : Part III 3.17 , 3.18

ID	No	Affiliation	Place	Comments	Responses to Comments
39	1	Group	Executive Summary	The sentence "The expansion of the supply chain means that the aggressors will spread the origin of attacks widely on the networked supply chain ..." is hard to understand the meaning of the sentence, how about doing as follows. Alternative) "The expansion of the supply chain means that the origin of the attack will spread widely on the networked supply chain, the opportunity for the aggressor to get the origin of the attack increases, and the range that the defender should protect will expand rapidly. "	We revised the content as suggested in your comments. Relevant part : Executive Summary
39	2	Group	1.	"The information society (Society 4.0) so far does not share necessary knowledge and information," but I think it has been shared even in the information society. Therefore, it may be easier for readers to understand what "sharing" means here.	We revised the content, taking into account your comments. Relevant part : Introduction 1.
39	3	Group	2.	What does "conversion processing" specifically mean? Also, if it differs from "analog" to "digital" conversion, I think it is necessary to explain what "conversion processing" means. If possible, readers may be easy to understand if there is an example.	We used your comments as a reference in revising the content. Relevant part : Introduction 2.
39	4	Group	7.	It is described "Determination of trustworthiness list", but it is easier for readers to understand if the explanation is included in the first P8 main text or P8 footnote. Or how about P20 as a reference?	We used your comments as a reference in revising the content. Relevant part : Introduction 7.
39	5	Group	Part I 1.	It says, "Not only the trust point of the organization's trust," but it may be an error of "not only the view of the organization's trust."	We revised the content as suggested in your comments. Relevant part : Part I 1.
39	6	Group	Figure 1.2-4	Since I do not know which part the “layer 2” notation refers to, what about surrounding the area of “layer 2” with some color? If you want to point to the entire pink horizontal axis, it may be better to place it within the pink horizontal axis. If you point to the horizontal axis where the blue horizontal axis and the pink horizontal axis are in contact with each other, it may be better to specify the range of the “second layer”, such as enclosing it with other colors .	We used your comments as a reference in revising the content. Relevant part : Part I Figure 1.2-4
39	7	Group	Figure 2.1-9	According to the sentence of IEC TR 63069, "design each safety function specification and security specification function based on the risk analysis results", but "security specification function" is not an error of "security function specification".	We used your comments as a reference in revising the content. Relevant part : Part II Figure 2.1-9
39	8	Group	Part III 3.8. CPS.AT	It says "to your staff and partners," but is it not an error of your staff?	Regarding your commnents, we leave the contents as original.
39	9	Group	Part III 3.9. CPS.DS	"The data and records are defined to protect the confidentiality, integrity, and availability of the data ~", but what does "record" here mean? "Data" is "information (data)" in the measure requirements of Table 3.3-10 CPS.DS category, so it can be received as "information". "Record" can be inferred from "information (not digitized)" and "Recording", so supplementation is necessary.	We used your comments as a reference in revising the content. Relevant part : Part III 3.9.
39	10	Group	Part III 3.17. CPS.CO	"For example, you can get support from an organization like a law enforcement agency," but "for example" at the beginning is not necessary.	We revised the content as suggested in your comments. Relevant part : Part III 3.17
39	11	Group	Part III 3.19. CPS.MI	I think "to reduce security incidents" is more appropriate than "to eliminate security incidents" but "to reduce security incidents".	We revised the content as suggested in your comments. Relevant part : Part III 3.19
40	1	Corporation		Scope on Industry The paper is focused on a program called “Connected Industries“ which will create value by building connections between a wide variety of disparate industrial data. The requirements and concerns of citizens regarding privacy in a “Society 5.0“ are sometimes shortly mentioned but not elaborated in detail. Possibly there is a separate paper for it. If so we would be happy to comments this paper, too. If not we suggest to develop it and offer our support. This additional paper could be based on the GDPR since we have the Japan-EU adequacy agreement in place with reciprocal recognition on adequate levels of data protection.	This framework provides an overall framework for security measures. Specific security measures are different for each industrial sector or each company, we will continue to consider appropriate security measures in each sector-specific sub working group of "Study Group on Industrial Cybersecurity" WG1, taking into account your comments.
40	2	Corporation		Hacker targets Cybersecurity is critical to the Connected Industries program. An attacker has many more possible targets in the new, interconnected supply chain, so cyber defenses must be drastically increased. The Hacker targets in the industry are elaborated in detail. Additional there are hacker targets on consumer site We suggest to see the end user also as a part of the interconnected supply chain. He should be transparently informed and well educated about cybersecurity risks and how he can support to minimize them. So far training and education is only considered to all individuals in the organization so that they can fulfill assigned roles and responsibilities to contain the occurrence and influence of prevent security incidents from occurring.“ (page 116), but not to the consumer. The consumer is a risk source, too and should be emphasized upon.	In this framework, end users are regarded as a part of the supply chain, and the security measures that should be implemented by service providers are mainly summarized, and end users are also regarded as stakeholders. We will use your comments as a reference in advancing cyber security policies in the future.
40	3	Corporation	Appendix A.	Smart Home Smart Home is considered as use case #4. We like to share the following picture about our view of the smart home supply chain. The end user/operator is part of it.	We will use your comments as a reference in advancing cyber security policies in the future. In the use cases of this framework, end users are regarded as “residents” and are recognized as part of the supply chain, including operators.

ID	No	Affiliation	Place	Comments	Responses to Comments
40	4	Corporation		Artificial Intelligence Artificial Intelligence (AI) is mentioned as tool to analyze the huge amounts of data which have to be secured. We see AI in a broader scope: ・ AI can also be used as tool to prevent Cyber Attacks. There are commercially available AI platforms to better identify and predict possible intrusions and data breaches. ・ Just the opposite AI can be used to develop and execute cyber security attacks. ・ AI itself can decide to attack other systems without being controlled or understood by humans. So far these are “dreams of the future“, but AI will become more and more independent and decide independently with a higher degree of autonomy. The German government has developed its AI strategy which includes some points regarding AI security and privacy. It has been commented by TÜV Rheinland and is available here: https://www.bmbf.de/files/Nationale_KI-Strategie.pdf (only in German).	We will use your comments as a reference in advancing cyber security policies in the future.
40	5	Corporation		Encryption Encryption of data and encryption of the communication channel are key points for security. This is considered for example in NIST Cybersecurity Framework and other publications, which are referenced in the paper (e.g. page 77). It is also mentioned: "Encrypt information (data) with an appropriate level of security strength, and store them(L1_1_a_DAT). We like to point out how important data encryption in the internal memory of an IoT device is. In many cases the Wi-Fi password is stored unencrypted in an IoT, for example: https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/. Wi-Fi credentials of the user have been recovered (stored in plaintext into the flash memory). We suggest to emphasize this point more strongly with clearer and more prescriptive recommendations.	We used your comments as a reference in revising the content. Relevant part : Appendix C CPS.DS-1
40	6	Corporation		Certification and Cyber Assurance Within the ecosystem there should be a role for independent verification, validation and certification of devices and IoT systems being developed by manufacturers. This will bring about transparency and a degree of assurance in the overall supply chain.	We will use your comments as a reference in advancing cyber security policies in the future.