Proposal for Further Strengthening Cybersecurity Measures

~ Establishing Cyber Resilience to Confront the Constant Threat to Cyberspace ~

April 2024

LDP Digital Society Promotion Headquarter

PT on Cybersecurity

The cyberspace is now in a state of "constant emergency." The assurance of "freedom, fairness, and safety" in cyberspace is no longer guaranteed, and its preservation is at risk. The total number of cyber attack-related communications (packets) confirmed by the large-scale cyber attack observation network operated by NICT (National Institute of Information and Communications Technology) last year was approximately 619.7 billion, which is about 48 times higher than a decade ago. When viewed per IP address, it translates to approximately 2.26 million packets per IP address (compared to approximately 1.83 million packets the year before), equivalent to an attack-related communication occurring once every 14 seconds. Additionally, according to the National Police Agency, the number of ransomware incidents reported from prefectural police to the National Police Agency in companies and organizations last year was 197, maintaining a high level since the first half of the year before last. Extremely serious situations persist, such as unauthorized access to government agencies and academic research institutions, and cyber attacks causing disruptions to the functions of critical infrastructure, impacting socio-economic activities. Cyber threats surrounding our country are increasingly escalating. Furthermore, foreign security authorities' warnings and reports from private cybersecurity firms highlight that, for example, nation-state actors are employing increasingly sophisticated and refined methods, such as environment-adaptive techniques, making detection and defense difficult. They emphasize the need for heightened vigilance and strengthened countermeasures. In response to these threats, major Western countries and others are boldly and swiftly taking actions to enhance cybersecurity nationwide. Measures include strengthening capabilities to protect government systems and critical infrastructure, promoting public-private cooperation and information sharing frameworks to enhance the resilience of these systems, and ensuring the security of IoT devices and software. The recent Japan-

US summit reaffirmed the commitment to further deepen cooperation on cybersecurity.

On the other hand, although the efforts of the Japanese government have made some progress, taking into account the recommendations of our party, including last May's PT, the speed and effectiveness of Japan's measures against the rapidly increasing threat of cyberattacks are still far from satisfactory. If there is a delay or lack of urgency in our response, it may not only have a significant negative impact on Japan's national security, economy, and social order but also lead to a significant decline in Japan's presence in the world.

Amidst the expansion of global economic activities and supply chains, and the deepening connections between the public and private sectors, it is imperative to transform this expansion into a "strength" rather than viewing them as "vulnerabilities" or "risks" in relation to cyber attacks by implementing measures closely coordinated with diverse stakeholders. From this perspective, this proposal focuses on strengthening "public-private partnerships," "supply chains," and "international cooperation." It delves into past efforts while making recommendations on issues such as legislation related to cyber security, ensuring the effectiveness of security clearance systems, the establishment of a new organization as the command center, fundamental strengthening of measures against disinformation, formulation of a package for promoting and strengthening the cybersecurity industry, development of a new action plan for post-quantum computing cryptography, and collaboration with Taiwan, among other new challenges. Our party is determined to devote all efforts to realizing the contents of this proposal, aiming to enhance and establish resilience in the constant threat to cyberspace, thereby safeguarding Japan's national interests and the livelihoods of its citizens.

1 . Prompt Establishment of Legislation and Systems to be Implemented

○ Early realization of legislation in the field of cyber security

Despite the clear mention in the National Security Strategy formulated two years ago about "enhancing capabilities in the field of cybersecurity to a level equal to or greater than major Western countries" and "establishing legislation and strengthening

operations to realize new initiatives in the field of cyber security," more than a year has passed without progress, and the concerns and apprehension from stakeholders are reaching their peak. Delay in specific actions will naturally increase the risks. It is strongly urged to accelerate responses regarding legislation and other measures in the field of cybersecurity within the government, and to promptly convene expert meetings and submit bills to the Diet. In order to appropriately address the rapidly escalating cyber threats at an astonishing speed, it is necessary to proactively eliminate the risk of significant cyber attacks that may cause security concerns for the country and critical infrastructure, and to introduce active cyber defense to prevent the escalation of damage in the event of such cyber attacks. In implementing such measures, it is strongly urged to concretely consider the establishment and enhancement of legislation and operational frameworks to ensure comprehensive cyber security for our country, aiming to improve our capability to swiftly and effectively respond to cross-border cyber attacks targeting our nation. The measures such as "strengthening information sharing with the government when private entities are subject to cyber attacks, as well as enhancing coordination, support, etc., from the government to private entities" are deeply related to this proposal from the perspective of public-private collaboration. Therefore, it is strongly urged to proceed with consideration to ensure the effectiveness of such measures.

○ Establishment of Systems to Ensure the Effectiveness of the Security Clearance System

Currently, the deliberation on the Important Economic Security Information Protection and Utilization Act, also known as the "Security Clearance Act," is underway in the Diet. Examples of "important economic security information" include "information related to cyber threats and countermeasures," and this legislation and cybersecurity measures are closely intertwined. Ensuring the effectiveness of the Security Clearance Act will contribute to strengthening cybersecurity measures. From this perspective, the following items are sought for realization:

- To further enhance international cooperation with allied and like-minded countries, it is important to develop specific measures for international cooperation, taking into account international consistency and substantive equivalence, as seen

in agreements such as the Industrial Security Agreement (ISA) between the United States and the United Kingdom, which facilitate mutual recognition of security clearances between two countries.

- In the case of information held by private entities, there are many types of information that should be preserved from a security perspective even if they are not categorized as "important economic security information." Experts have pointed out the need to consider providing clear guidelines to private entities to ensure that they can implement necessary information preservation measures and to address concerns raised during the PT hearings regarding information preservation in exchanges between private entities.

- Regarding the structure for conducting "suitability assessments" and investigations, the U.S. Department of Defense reportedly has thousands of specialized personnel conducting investigations. Similarly, ensuring an adequate workforce for conducting investigations is a significant challenge for Japan. Given the time constraints, it is necessary to promptly consider organizational structures, budgets, and securing necessary expertise after the bill is enacted, considering that enforcement is expected to start in FY2025.

- To ensure that "compliant operators" can maintain information security at appropriate levels, it is important to provide clear criteria and guidelines for internal systems, selection of handlers, and response in the event of a leak. Additionally, guidelines should be developed based on the needs of private entities, considering the clearance requirements for facilities and equipment that compliant operators must meet, while allowing them sufficient time for compliance.

- Regarding the handling of information within companies regarding whether employees possess clearance or not, it is important to prevent unreasonable reassignments based on refusals or withdrawals of consent and suitability assessment results. Furthermore, taking into account the risk of reputational damage and legal actions for listed companies, guidelines should be developed

based on feedback from private entities.

・ Although information held by independent administrative agencies is not designated as "important economic security information," it is considered desirable to preserve information held by agencies such as JAXA, JST, and NEDO. Measures should be considered to steadily promote information preservation in these organizations.

○Amendment of the Basic Cybersecurity Law

・ The current Basic Cybersecurity Law does not specify the Minister of Land, Infrastructure, Transport and Tourism, the Minister of Finance, the Minister of Health, Labour and Welfare, etc., as members of the "Cybersecurity Strategy Headquarters," despite including critical infrastructure sectors such as finance, healthcare, water supply, aviation, airports, railways, and logistics. Cybersecurity enhancement is not limited to specific areas; it affects society as a whole. From the perspective of improving communication and coordination across the government, it is advisable to promptly amend the Basic Cybersecurity Law to designate all ministers as members of the Cybersecurity Strategy Headquarters and to appoint the Prime Minister as the current head of the headquarters instead of the Chief Cabinet Secretary.

○Strengthening the Structure of the New Organization Established after the Dissolution of National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

・ In July of this year, the first phase of organizational enhancement for the new organization was initiated, which included the addition of one vice minister-level official and six director-general/deputy director-general-level officials. It is understood that the second phase of organizational enhancement will be carried out

in line with the legislation related to cybersecurity mentioned in the National Security Strategy. However, to make the execution of the law effective, it is necessary to secure sufficient budget, personnel, and specialized expertise. In doing so, it is expected that the organization designated as the central hub for cybersecurity will implement both policy and operational functions. Particularly regarding operations and responses, measures should be taken to strengthen the structure so that the organization can respond comprehensively and proactively, even in intense situations. Additionally, there is an expectation for this organization to play a strong role in promoting public-private cooperation. Establishing operational units for actual response is also crucial, and thus, there is a call for prioritized allocation of budget for their establishment, tools, and personnel training, aiming to enhance the overall readiness of the structure.

- In FY2023, led by NISC, efforts such as signing joint documents with allied countries on "Secure-by-Design/Secure-by-Default Joint Document (Revised Edition)," "Secure AI System Development Guidelines," and "Ransomware Countermeasure Initiative" have advanced On the other hand, while various ministries and agencies are engaging in international cooperation on cybersecurity measures, it cannot be said that such efforts are necessarily unified or strategic. Therefore, it is requested that the new organization, evolved from NISC, take on the role of promoting international cooperation as the command center, to grasp the entirety of cybersecurity measures in Japan and to strategically allocate and utilize government resources, enhance collaboration with the private sector, and strengthen the dissemination of Japan's initiatives.

○Drastic Strengthening of Countermeasures Against Disinformation and Misinformation

- The Cabinet Intelligence and Research Office, the International Public Relations Office of the Prime Minister's Office, and the National Security Secretariat are working together on measures to counter disinformation by foreign entities. However, to address increasingly sophisticated and serious cases of disinformation, it is necessary to enhance capabilities for proactive and aggressive responses, including strategic communication. This requires further strengthening of the

system and utilization of specialized personnel.

・ International cooperation, such as enhancing intelligence information sharing and joint responses, is essential in combating disinformation. Additionally, it is important to build information collection and analysis systems using AI and to train human resources. Leveraging the technological expertise available in the private sector should also be maximized.

・ Not only has there been a dissemination of false or misleading information during the recent Noto Peninsula earthquake, but there have also been instances where false information about Prime Minister Kishida has been spread, posing a significant threat to social order. In response, the Ministry of Internal Affairs and Communications has established a working group under the "Study Group on Ensuring the Integrity of Information Flow in the Digital Space" to consider various rights and interests, including freedom of expression, from a specialized perspective. In light of these discussions, it is necessary to consider drastic strengthening of countermeasures against disinformation and misinformation, including institutional responses.

○Establishment, Operation, and Monitoring of a Robust Government System

・ A robust government agency system, including implementing Zero Trust, should be built and operated. To ensure this, the surveillance system of the current Government Security Operations Center (GSOC), which conducts cross-government monitoring at NISC, should be enhanced into a next-generation GSOC within the new organization. Additionally, the Continuous Risk Assessment and Response (CRSA) system, currently in the pilot phase, which continuously evaluates government systems and promptly addresses threats and vulnerabilities in government agencies, should be fully implemented and operated.

・ Alongside the above mechanisms, the governance structure for government system

monitoring should be streamlined to enable as efficient operation as possible. A comprehensive management system should be implemented and operated to monitor government systems continuously, visualize situations and challenges regarding whether appropriate services are being provided to citizens and the business sector, etc.

・ In monitoring and analysis/response based on the monitoring, the government should strive to enhance capabilities and establish systems for advanced analysis, including threat hunting and comprehensive behavioral analysis, in order to respond to recent sophisticated cyber attacks, and appropriately share the insights obtained within government departments.

・ Based on the "Secure by Design" guidance and the "Cybersecurity Framework 2.0" revised by National Institute of Standards and Technology (NIST), various guidelines for ensuring the security of information systems formulated by the Digital Agency should be created and maintained. These guidelines should be utilized to ensure security during the implementation of government systems.

・ The establishment of an advanced authentication infrastructure for government employees should be considered. Additionally, research should be conducted and progress should be made towards the introduction of systems and mechanisms for uniquely identifying users, even considering various work styles such as interagency transfers and revolving doors between the public and private sectors, and conduct pilot studies for the examination and verification of the employee ID infrastructure.

○Strengthening of NICT (National Institute of Information and Communications Technology)

・ To enhance autonomous capabilities in responding to cyber attacks, it is crucial to establish organizational and human infrastructure for collecting, storing, analyzing, and providing cybersecurity information, including the situation of cyber attacks

against Japan. Therefore, it is necessary to further enhance and strengthen the organizational infrastructure of Cybersecurity Integrated Intelligence and Human Resources Development Platform (CYNEX), which began full operation in collaboration with partner organizations at NICT in FY2023. Additionally, efforts should be made to deepen collaboration, including expanding partner organizations.

・ The "CYXROSS" project, which involves introducing domestically developed security sensors capable of verifying safety and transparency to government terminals and aggregating cybersecurity information collected for analysis at NICT, should be expanded in cooperation with the Digital Agency to increase the introduction of sensors to government terminals. By conducting cross-sectional analysis of collected information, efforts should be made to generate Japan-specific threat intelligence. Furthermore, collaboration with GSOC operated by NISC and the new organization should be established to contribute to enhancing monitoring and diagnostic capabilities for protecting government information systems.

○ Strengthening of IPA (Information-technology Promotion Agency)

・ Given the challenges such as "being required to implement various levels of measures by different trading partners" and "difficulty in assessing the security posture of each company," it is necessary to consider measures to be implemented based on the actual situation of supply chains of each company and mechanisms to visualize the status of these measures.

・ From the perspective of enhancing the functionality of aggregating and analyzing cyber attack information obtained through the industry (endpoints) and coordinating responses, it is important to fundamentally strengthen IPA's framework, which has a strong connection with the industry. Additionally, the government should advance the standardization of requirements for government procurement based on guidelines and standards.

・ To promote the development of highly knowledgeable personnel responsible for security measures in fields such as critical infrastructure, IPA should advance the establishment of new simulated plants and the updating of existing ones as part of its "Core Personnel Development Program" to expand the number of participants.

・

・ With the opening of IPA's Kasumigaseki Satellite Office in line with the "Key Plan for Achieving a Digital Society" (Cabinet Decision of June 9, FY2023), ongoing improvement efforts should focus on verifying the operation status of the satellite office and considering its expansion to further enhance collaboration with the industry and various ministries and agencies.

2. "Public-private collaboration" and "strengthening measures across the entire supply chain."

○Building a more robust information-sharing system with the private sector

・ Establishing a robust mechanism for sharing incident information with the private sector is crucial. While incident reporting by companies is mandated by law for some critical infrastructure, further efforts are needed to advance information sharing and build trust between the public and private sectors. To achieve this, it is imperative to promptly establish and enhance mechanisms for reporting incidents across all critical infrastructure, beyond those currently mandated by law. From this perspective, it is necessary to assess the achievements and challenges of the "Cybersecurity Council," which commenced in 2019 and has been in operation for five years, and to study the strengths and weaknesses of mechanisms such as the Joint Cyber Defense Collaborative (JCDC) launched by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and similar mechanisms in other countries. Continuous review and enhancement of these mechanisms are essential. Additionally, considering the progress in legislation and other developments in the field of cyber security, it is important to explore the establishment of new

organizational structures to strengthen public-private collaboration.

○Development of cybersecurity talent

- It is urgent to undertake initiatives to cultivate professionals capable of addressing security measures, especially in fields such as critical infrastructure and essential services. Furthermore, it is necessary to enhance support for small and medium-sized enterprises (SMEs), local governments, and other entities facing shortages in skilled personnel. Additionally, there is a need to meticulously address the roles expected of security personnel within each organization and delineate the profile of skills, knowledge, abilities, and technologies necessary to fulfill these roles. Strategies for fostering such capabilities should be explored, including initiatives for training and development.

- Digital services have become integrated into the daily lives of citizens, beyond just corporate activities. Cyber incidents such as virus infections and investment scams via fake advertisements on social media affect individuals of all ages. To protect citizens' livelihoods, it is crucial to establish environments for enhancing security literacy from as early as primary school. Moreover, from the perspective of fostering cybersecurity talent nationwide, it is essential to create educational opportunities that enable individuals to pursue careers related to security measures from an early age, such as in primary school. Considering the expansion of career options and improvement of literacy, bold support measures for seamless "security education" from primary to secondary school should be implemented. Consultations from the Minister of Education to the Central Council for Education regarding the revision of the next curriculum guidelines are scheduled for this autumn. It is expected that discussions will also encompass "information education" in the 2030s, and active deliberations on security education within that framework are encouraged. Additionally, support measures should be implemented to enhance security education for students at technical colleges, universities, and graduate schools who can become immediate assets in the field.

- Initiatives, such as the "Security Camp" led by the Ministry of Economy, Trade and

Industry (METI), which aims to identify and nurture top-tier talent (full-stack engineers) capable of responding to diverse scenarios in information security, have been implemented. Since its inception, 43 individuals have graduated from this program. Moreover, the Ministry of Internal Affairs and Communications (MIC) and the National Institute of Information and Communications Technology (NICT) have conducted the "SecHack365" program, offering a one-year training course in security technology for approximately 40 selected individuals under the age of 25 annually. Since 2017, a total of 289 individuals have completed this program, and are now active in various fields, including private cybersecurity firms. It is imperative to continue these initiatives steadily to enhance the quality and quantity of talent nationwide.

- Consideration should be given to establishing organizations such as the "Cyber Guardian League (tentative name)" that not only hone the skills of trained white-hat hackers but also serve as a talent pool through mutual recognition and practical research programs. To facilitate practical research from an attacker's perspective, the necessity of exemptions from laws such as the Unauthorized Access Prohibition Act should be examined.

- Ministry of Internal Affairs and Communications and NICT offer practical cybersecurity defense exercises called "CYDER" to national institutions, local governments, and operators of critical infrastructure. Since 2017, approximately 3,000 individuals per year, totaling 20,936 individuals (including 10,578 local government employees), have participated. In realizing the concept of a digital agrarian state, it is essential for local governments to build and continuously strengthen their capabilities to respond to cybersecurity incidents alongside promoting digital transformation. As individual efforts by local governments have limitations, it is necessary for the national government to continue providing CYDER, which plays a vital role in cultivating cybersecurity talent, without imposing additional burdens on local governments, to widely and continuously support the development of security personnel at the local level.

- Forming regionally-rooted security communities involving diverse stakeholders

responsible for promoting DX in each region is also crucial for enhancing security measures at the local level.

・ To address the shortage of cybersecurity professionals, it is important to consider promoting the utilization of Registered Information Security Engineers (Registered SecSpes) in user companies. This could involve considering requirements for deploying or utilizing Registered SecSpes in subsidy programs and reassessing systems to reduce the high costs associated with maintaining registration. In addition, an environment should be developed to enable the acquisition of basic knowledge and skills for professional personnel, such as security personnel from local vendors and users of small and medium-sized enterprises.

○Proposal for promoting and strengthening the cybersecurity industry

・ Japan's cybersecurity heavily relies on foreign technologies and products. This dependency poses a risk of a "negative spiral" where data from Japanese user companies is not stored domestically, making it increasingly difficult for domestic companies to provide high-quality products and services that utilize such data. Moreover, excessive reliance on foreign products and technologies for securing important data of Japanese user companies threatens Japan's independence.

・ In the rapidly growing cybersecurity market, it is crucial from both economic security and industrial policy perspectives to strengthen the supply side to ensure that Japanese security companies can demonstrate relative strengths in certain areas and secure footholds in areas they need to control. Furthermore, such capabilities enable strong collaboration with allied and like-minded countries. In major foreign countries, security companies actively develop products and expand their market presence driven by government and corporate demand, leading to scaling up. Japan should aim to establish a "security economy" by building an ecosystem of demand and supply, following this model.

・ However, it is important to note that these initiatives should not hinder the use of high-quality foreign products. While necessary international collaboration should

continue, it is important for Japan to aim for a situation where the supply of "high-quality" domestically produced security products and services is strengthened, especially in critical areas, as the cybersecurity market expands. Furthermore, to enhance competitiveness as an industry, it is crucial to actively market these products and services overseas, leveraging the resulting profits to create a cycle of reinvestment in new research and development, talent acquisition, wage increases, facility investments, and so forth. Creating a situation akin to "earning while protecting" should be the objective, fostering a cycle where profits are reinvested to sustain growth and innovation.

・ Therefore, it is strongly urged to present a package of enhanced measures for promoting the cybersecurity industry, based on the aforementioned awareness of issues.

・ With the increasing incidents of data leaks and incidents originating from cloud services, there is a need for mechanisms for security assessment and management to understand the starting point for countermeasures. However, the majority of companies find it challenging to allocate resources for assessments or update assessment methods in line with technological advancements. Therefore, it is important to foster private companies and services that can conduct assessments rapidly in alignment with the latest technological trends and consider support measures for this purpose.

・ Regarding the IoT conformity assessment system, which is scheduled to commence partial operation within this fiscal year, it is essential to develop a domestic roadmap, taking into account economic security considerations. Furthermore, it is important to encourage businesses to utilize the system by highlighting that existing IoT products already in circulation and use will also be subject to conformity assessment at the time of its implementation.

○Further strengthening cybersecurity measures for small and medium-sized enterprises (SMEs)

- To enhance cybersecurity measures for SMEs, it is essential for them to assess and evaluate their current security levels according to their company size. Based on this assessment, it is important for each company to prioritize measures while considering limited resources. Consideration should be given to enhancing support for SMEs' cybersecurity measures, such as dispatching security experts and providing assistance for implementing security tools. Establishing mechanisms supported by Information Security Management Specialists to improve the quality of assessments could also be considered.

- Additionally, companies that already deploy security evaluation platforms for cloud services or offer cyber insurance may possess data evaluating the security levels of SMEs. It is worth considering mechanisms to utilize such data for policymaking in Japan based on industry-specific and size-specific analyses. Furthermore, mechanisms utilizing corporate disclosure systems could be explored to enable companies to disclose security measures taken in their annual reports, thus enhancing the visibility of security levels.

- Through pilot projects aimed at matching SMEs with cybersecurity professionals and promoting the utilization of Registered Information Security Engineers (Registered SecSpes) through support organizations, efforts should be made to expand the pool of Registered SecSpes by exploring measures to reduce the registration and maintenance costs of qualifications.

- Collaboration with relevant agencies and industry associations should be pursued to further promote and disseminate the "Cybersecurity Assistance Team Service," creating new categories with expanded requirements to meet the needs of medium-sized and larger SMEs.

- IPA should aggregate valuable information and knowledge on cybersecurity for SMEs and disseminate timely information to them.

- These initiatives can collectively contribute to strengthening cybersecurity measures for SMEs, ensuring their resilience against cyber threats.

○Promotion of botnet countermeasures

- Due to the neglect of IoT devices such as routers and network cameras that possess vulnerabilities, whether in corporate environments or households, incidents are increasingly occurring where such devices are hijacked, incorporated into botnets, and exploited for cyber attacks like DDoS attacks. Additionally, unauthorized configuration changes leading to information leaks are becoming more common. Addressing these issues is urgent. To effectively tackle this situation, the revised NICT Act, implemented in April of this year, serves as a basis for NICT to promote investigations into IoT devices with vulnerabilities and those already infected. Moreover, it is imperative to advance the new NOTICE project to achieve proper management of IoT devices through enhanced collaboration with users, telecommunication operators, manufacturers, system integrators (SIs), and other stakeholders, as well as clear information dissemination. Furthermore, there should be considerations for enabling Internet Service Providers (ISPs) to practically disconnect vulnerable IoT devices from networks, which could serve as platforms for cyber attacks while infected.

- For identifying Command and Control (C&C) servers issuing instructions to botnets, telecommunication providers should leverage AI-based flow analysis to detect them early and comprehensively. By promoting effective collaboration with stakeholders, both at the terminal and network levels, a comprehensive approach to IoT botnet countermeasures can be pursued.

○Operation of the certification system for e-seals

As digital transformation (DX) accelerates within companies, ensuring the reliability of

electronically transmitted data between organizations becomes crucial. To promote the use of "e-seals," which identify the issuer of electronic data and prevent impersonation or tampering, consideration should be given to advancing discussions to commence the operation of the certification system for e-seals under the Minister of Internal Affairs and Communications within FY2024.

This certification system aims to establish trust in electronic transactions by providing a reliable mechanism for verifying the authenticity and integrity of digitally signed documents, contributing to the secure exchange of electronic data in various sectors.

○Promotion of "Open RAN"

"Open RAN" is a framework for network infrastructure deployment that involves "horizontal specialization" with equipment from multiple vendors. It enables the entry of various vendors, including Japanese companies, and facilitates the realization of a secure, open, and transparent 5G network without excessive reliance on specific vendors. Through collaboration between governments and the private sector in allied countries, specifications between devices should be standardized and opened up, further promoting Open RAN both domestically and internationally.

This approach fosters innovation, competition, and interoperability in the telecommunications industry, ultimately benefiting consumers with enhanced network performance, flexibility, and choice.

○Addition of sectors to critical infrastructure

Following the cyber attack incident at Nagoya Port, which led to the addition of ports as critical infrastructure in March 2024, it is essential to consider adding cloud service providers and Managed Service Providers (MSPs), among other cyber infrastructure operators, to the list of critical infrastructure providers. Considering the significant influence of these entities, they play a crucial role in ensuring the resilience and security of our critical infrastructure.

Moreover, relying solely on reactive measures to add sectors after incidents occur can put us in a reactive position. Hence, it is imperative to explore agile and flexible approaches for adding sectors to critical infrastructure swiftly and proactively in the future. This proactive approach will enhance our ability to identify and protect vital sectors from emerging cyber threats effectively.

○Cybersecurity measures for the Osaka-Kansai Expo

Building upon the success of cybersecurity measures implemented during the Tokyo 2020 Olympics, it's essential to leverage the legacy and apply similar strategies to ensure robust cybersecurity for the Osaka-Kansai Expo. For instance, implementing a cybersecurity defense training program tailored for Expo-related organizations, such as the "CIDLE" program, based on NICT's expertise in lectures and practical exercises, would be beneficial. This initiative should be conducted in close collaboration with relevant stakeholders to ensure comprehensive cybersecurity measures are in place for the Expo.

By proactively addressing cybersecurity concerns and fostering a culture of awareness and preparedness, we can help safeguard the Expo against potential cyber threats and ensure its success as a global event.

○Enhancement of cybersecurity measures in healthcare institutions

・To ensure security while advancing healthcare digital transformation (DX), it is imperative to continue conducting assessments of network infrastructure and implementing offline backup systems in hospitals. These measures are essential to safeguard sensitive patient data and critical medical systems from cyber threats. By regularly assessing network configurations and ensuring robust backup procedures, healthcare institutions can mitigate the risk of data breaches and system disruptions, thus maintaining the integrity and availability of healthcare services.

・In the realm of medical devices, it is important to continue advancing initiatives that call for the implementation of cybersecurity measures as part of the standards medical

devices must meet, based on laws related to ensuring the quality, efficacy, and safety of pharmaceuticals, medical devices, etc., in accordance with IMDRF guidance.

3 . Enhanced measures with a focus on “international cooperation”

○Strengthening the security of IoT devices and software components

- Regarding the IoT conformity assessment system scheduled to commence partial operation within FY2024, efforts should be made to formalize requirements for certain IoT devices in government procurement and other areas to enhance effectiveness. Additionally, consideration should be given to the direction of the assessment system, including medium to long-term perspectives, by indicating the standards required by each industry. Proactive leadership and promotion of international cooperation towards ensuring interoperability with similar systems being considered or implemented in Europe, the United States, Singapore, and elsewhere should be pursued.

- To further promote the adoption of SBOM (Software Bill of Materials), necessary measures should be explored while collaborating with the industry, such as formalization in government procurement and the study of efficient vulnerability management methods using SBOM, visualization of the scope of responses in identifying and managing vulnerabilities using SBOM, and consideration of the role of guarantees in contracts.

- With respect to the "Secure by Design" guidance jointly developed by the United States and co-signed by the Japanese government, the initiatives that software developers should undertake should be organized and presented to businesses to encourage compliance. Building on the principles of the "Japan-US-Australia-India Cybersecurity Partnership" established at the QUAD Leaders Summit, efforts should be accelerated in Japan towards the domestic and international implementation of baseline security standards and the continuous harmonization thereof, as well as the cohesive development of frameworks for software security in government procurement.

○Launching an international framework (IAP) for the realization of DFFT led by Japan

- Towards the realization of DFFT (Dependable and Free Flow of Data), which was proposed by former Prime Minister Abe at the G20 Osaka Summit and subsequently endorsed in the G7 Hiroshima Summit Declaration and the G7 Digital and Technology Ministers' Meeting at the end of last year, when establishing the OECD international framework (IAP: Institutional Arrangement for Partnership) as a platform, Japan strongly demands active leadership in discussions, including improving transparency in policies and regulations regarding cross-border data transfers. We strongly urge Japan to enhance collaboration among industry, academia, and government and take a proactive stance in leading international discussions on data governance. This includes advancing considerations for establishing data spaces, taking into account efforts in Europe and the Asian region, such as improving the transparency of policies and regulations regarding cross-border data transfers, as well as conducting demonstrations for building data spaces related to battery supply chains and steel supply chains.

○Expansion and continuation of joint public-private exercises

- The practical cyber defense exercises (CYDER) conducted by the Ministry of Internal Affairs and Communications and NICT with Pacific island countries should be continued and the participating countries should be expanded to prevent any weak areas. Furthermore, collaboration with willing countries such as the US and Australia should be strengthened to enhance the content. As the PALM10 (10th Pacific Islands Leaders Meeting) is scheduled to be held this year, the enhancement of cybersecurity measures with Pacific island countries should be included in the summit declaration.

- The Japan-ASEAN Cybersecurity Capacity Building Center (AJCCBC) project, which promotes projects that contribute to improving cybersecurity capabilities within the ASEAN region, should strengthen collaboration with willing countries and participating companies. Japan should provide and conduct training programs

and various cybersecurity exercises that are being implemented domestically. It is crucial to address the differences in technical skills among participating countries and participants by providing additional exercise content, implementing follow-up after training, and expanding the course offerings.

・ Training programs for industrial control system cybersecurity exercises for the Indo-Pacific region, which are held annually, should be continued in cooperation with the US and EU governments and others.

○Cooperation with Taiwan

・ The increasing economic ties, particularly in the semiconductor industry, necessitate the enhancement of cybersecurity measures in collaboration with Taiwan for both economic security and cybersecurity in the context of potential "Taiwan contingencies" or cybersecurity in gray zone areas.

・ The Japan-Taiwan Exchange Association, a private organization in Japan, hosts seminars and workshops on cybersecurity within the framework of the Global Cooperation and Training Framework (GCTF), where experts from Japan, Taiwan, the United States, Australia, Canada, and other countries share their knowledge and experiences. The government should closely collaborate with the Japan-Taiwan Exchange Association and focus on deepening cooperation between Japan and Taiwan, initially among experts.

・ Moreover, an international working group was established in November 2023 under the Supply Chain Cybersecurity Consortium (SC3), in which a wide range of economic organizations and industry-specific trade associations participate, in order to promote cybersecurity measures for both large and small enterprises. Therefore, the government should promote collaboration with institutions and organizations abroad, particularly in the Asia-Pacific region where Taiwan, with its many manufacturing suppliers, is located.

・ Furthermore, to ensure security in the semiconductor-related industries, where

domestic investment is strongly encouraged, collaboration with companies in Taiwan and the United States is vital. Efforts should focus on understanding the current situation through surveys and investigations, exploring necessary policies, establishing platforms for sharing cybersecurity measures, concerns, and case studies, and engaging in continuous dialogue involving companies and industry associations in Taiwan.

4 . Establishment of a policy package for Post-Quantum Cryptography (PQC) adaptation

○Necessity and Threats

- Currently, there is significant progress in computer performance, necessitating the utilization of cryptographic algorithms that ensure appropriate security strength. Moreover, with advancements in quantum computing technology, there are concerns about the potential decryption of currently used public key encryption schemes. In addition to the innovation in hardware technology, expecting the practical application of resistant quantum computers by the late 2020s, it is imperative to consider innovations in algorithm and software technology simultaneously. It is difficult to expect countries or entities that successfully decrypt encryption to promptly disclose such facts. Therefore, Japan should be mindful of the possibility that it may not promptly recognize the fact that encryption has been decrypted.

- It is crucial to recognize accurately that High Noise Data Leakage (HNDL) attacks, especially in anticipation of the practical application of quantum computers, are not merely future risks but threats that are already occurring at present.

○Challenges

- Considering the current international situation, there is a significant risk that Japan may incur substantial losses in terms of security and economy if the response is delayed. However, based on Japan's past experiences with transitioning

cryptographic technologies, it typically takes several years to a decade to complete the transition.

- In the United States, 2030 is considered a crucial milestone, and there is a common understanding among both the government, including the White House, and the private sector. NIST has been progressing towards Post-Quantum Cryptography (PQC) adaptation by standardizing PQC and conducting assessments within government agencies. It has been revealed that the first standardization is expected to be completed in the summer of 2024, and the finalized specifications will made public.

- Many of Japan's critical information systems are networked, posing the risk of information leakage if a single point in the network is breached. However, from the perspective of individual companies, the damage and risks of information leakage may be underestimated. This reality can hinder the incentive for companies to have swift and robust responses.

○Recommendation

- In order for the government to take responsibility for promoting the adaptation of Post-Quantum Cryptography (PQC) technology in Japan's critical information systems, including the private sector, an "Action Plan for Post-Quantum Cryptography Adaptation (tentative name)" including the following five items should be formulated and clearly positioned in the "Cyber Security Strategy" as well.

①Development and Publication of a Transition Plan (Roadmap) Considering the Entire Country

It is essential to utilize cryptographic algorithms with the necessary security strength, considering the risk of decryption due to the current improvement in computer performance, for existing cryptographic technologies. Aim to transition to stronger cryptographic algorithms by 2030, such as algorithms with 128-bit security strength.

Additionally, considering advancements in quantum computing technology, promptly conduct impact assessments and evaluations for Post-Quantum Cryptography (PQC) adaptation. Define priority response systems, especially in critical areas like public sectors, finance, telecommunications, and energy, to clarify the scope and priority of adaptation.

Set response deadlines according to priority. Among them, the highest priority response systems in critical areas should be set to be completed by 2030.

②Development and Publication of "Post-Quantum Cryptography (PQC) Adaptation Guidelines for Enterprises" (tentative title)

- Develop and publicize "Post-Quantum Cryptography (PQC) Adaptation Guidelines" by leveraging pioneering efforts from leading companies as best practices.

- Incorporate the concept of "Crypto Agility," which emphasizes the importance of not only adopting PQC technology but also establishing robust processes, governance, and skilled personnel within each company and society to effectively address threats. This includes considerations for technology (architecture and PQC technology), processes, organizational capabilities, and governance structures.

③Clarification of the driving force and strengthening of the necessary personnel and authority

- To advance the overall "Action Plan for Post-Quantum Cryptography (tentative title)," it is essential for the government to clearly establish a command center regarding post-quantum cryptography preparedness.

- The responsible ministries and agencies should develop a "schedule" for post-quantum cryptography preparedness within their respective industries.

- In order for the command center department and each ministry to proactively promote post-quantum cryptography preparedness in their respective areas of responsibility, it is necessary to cultivate and secure personnel with the required knowledge and expertise.

④Support measures necessary for promoting the transition

- To ensure that businesses do not hesitate to take necessary measures in the "highest priority response areas," it is essential to implement support measures. Particularly for small and medium-sized enterprises (SMEs), post-quantum cryptography readiness itself may pose an excessive burden. Therefore, it is crucial to consider robust support measures.

- Measures to promote the development of related technologies should be implemented, including research and development support for improving post-quantum cryptography performance, increasing key lengths for symmetric encryption, and achieving cryptographic agility. Support should also be provided for product development. Additionally, measures such as making these advancements a condition for government procurement contracts should be considered.

⑤Support for international standardization and overseas expansion

- To ensure that quantum-resistant cryptographic technologies and products developed domestically are actively utilized overseas, it is necessary to work actively on international standardization of promising technologies and overseas dissemination of promising products, as the need for quantum-resistant cryptography extends beyond our country to various other nations.