Provisional Translation as of September 4, 2015

CYBERSECURITY STRATEGY

September 4, 2015

THE GOVERNMENT OF JAPAN

Contents

1. Introduction

From the late 20th Century to the early 21st Century, the world experienced irreversible and revolutionary transformations. As Gutenberg's invention of letterpress printing induced the explosion of knowledge, the invention and spread of computers and the Internet have enabled people to discuss and share thoughts throughout the world without geographic and time constraints. Composed of countless computers, sensors, and actuators that have been networked by information and communications technologies, cyberspace has greatly expanded the activities of people in physical space. The free and interactive exchanges of ideas and opinions in cyberspace, based on digital messages and information sent from every part of the world, constitute the foundation of a global democratic society. Additionally, the digital space, sparking a cascade of new business models and technological innovations, has become a frontier of economic growth.

In this new sphere of cyberspace, however, malicious activities are prevailing. Stealing personal, business, and organizational information and assets has been increasingly persistent. There are also growing threats against national safety and security; governmental bodies and business operators, which provide mission-critical information infrastructure necessary for the people's daily lives and economic activities, have been exposed to cyber attacks that would risk their business operations and continuity. In light of such malicious activities, the greatest challenge is how to best counter these threats and protect intellectual properties that are the fruits of the creativities and inspirations of individuals and businesses, while ensuring and maintaining the free flow of information that is the "backbone" of democracy, the safe and secure living environment of the people, economic and social prosperity, and peace.

Under these circumstances, Japan enacted the Basic Act on Cybersecurity in November 2014. This Act prescribes the concept of cybersecurity and defines the roles and responsibilities of the Government, local governments, and other relevant stakeholders; it also designates the Cybersecurity Strategic Headquarters as the command and control body of national cybersecurity, and gives strong authorities, such as making recommendations to national administrative organs, to the Cybersecurity Strategic Headquarters. This mission document is to be formulated pursuant to the Basic Act that prescribes the Government's responsibility to establish the Cybersecurity Strategy.

Looking towards the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games (hereinafter "Tokyo 2020 Olympic and Paralympic Games") and the prospects further ahead for the early 2020s, this strategy outlines the basic

directions of Japan's cybersecurity policy for the coming three years approximately. To the world, it articulates Japan's clear vision for cyberspace; and by implementing this strategy, Japan will endeavor to ensure a free, fair, and secure cyberspace; and subsequently contribute to the improvement of socio-economic vitality and sustainable development, the creation of a society where people can live safe and secure lives, and peace and stability of the international community as well as national security.

To achieve this objective, the Government of Japan has laid out this strategy as a platform for the common understanding and actions of relevant stakeholders.

2. Understanding on Cyberspace

2.1. Benefits of Cyberspace

Cyberspace is an artificial domain for the free exchange of ideas without regard to national borders; it is a digital frontier of infinite values generated by intellectual creations and innovations inspired by the ideas globally exchanged. The private sector-led investment and the accumulation of wisdom have been pivotal to the rapid expansion of cyberspace; and, today, cyberspace is an essential foundation of Japan's socio-economic activities, as it has attracted a great deal of users due to its non-discriminatory and non-exclusive nature of easy accessibility.

On the other hand, earthshaking changes provoked by information communications technologies (ICTs) evolution in cyberspace are only in their initial stages. Recently, all kinds of "things" or physical objects, from personal computers, home electric appliances, automobiles, to robots and smart meters, have begun to be connected to networks including the Internet, benefitting from advanced hardware, such as sensor devices, the widespread of affordable and high-speed Internet, and the advancement of Big Data analytics technologies, and more. Along with the increasing connectivity, physical objects and people in real space have become interconnected in a multi-layered manner without physical constraints, by harnessing the free flow of information and accurate data communications in cyberspace. With this cyber-physical hybrid, there is an emergence of an "interconnected and converged information society" where cyberspace and real space have become highly integrated. It is a society that enables the members of the society to create innovative services and to generate brand new values exponentially.

A free and fair cyberspace is a prerequisite to benefit from cyberspace, which is an enabler of the improvement of socio-economic vitality and sustainable development.

2.2. Increasing Threats in Cyberspace

While cyberspace has brought significant benefits to our lives, malicious activities to harm these benefits are increasing. Cyberspace, which anyone can utilize without geographic and time constraints, gives advantages asymmetrically to malicious attackers, not defenders. At the same time, the increasing dependency of socio-economic activities on cyberspace and the evolution of organized and highly sophisticated methods (modus operandi) of cyber attacks that are suspected as state-sponsored have caused grave damages and exerted negative impacts on the people's daily lives and socio-economic activities, and consequently, threats against national security have become more serious year after year.

Additionally, since malicious activities in cyberspace will cause extensive impact on all kinds of connected physical objects and services, and the damage caused by cyber attacks will spread more rapidly and widely in real space due to the arrival of the interconnected and converged information society, it is anticipated that the people's living will be exposed to more immense cyber threats in the future.

To prevent further aggravation of such threats, the realization of "free and fair cyberspace" must be in parallel with the realization of "secure cyberspace."

3. Visions and Objective

In accordance with the Basic Act on Cybersecurity[1], and based on the understanding on the current state described in the preceding chapter, Japan has set the objective of this strategy as follows.

Objective: Ensure a free, fair, and secure cyberspace; and subsequently contribute to the improvement of socio-economic vitality and sustainable development, the creation of a society where the people can live safe and secure lives, and peace and stability of the international community as well as national security.

(1) The Cyberspace Japan Aims for

For the protection of the freedom of expression, the creation of innovation, and the improvement of socio-economic vitality, cyberspace is required to be a space where freedom is assured without unnecessary restrictions; and, in which all actors who wish to access are neither discriminated nor excluded without any legitimate reason.

To prevent the people's living and the international community as a whole from being threatened by information or property theft and the malfunction of social systems posed by cyber attacks, cyberspace has to be a secure space with response capabilities against such threats, through the promotion of a better understanding on cyberspace among all actors, including individual people and organizations, and through each actor's cooperative and self-motivated activities.

Japan will make its maximum effort to ensure a **free, fair, and secure cyberspace** as illustrated above.

---

[1] The Basic Act on Cybersecurity (Act No. 104 of November 12, 2014), Article 1: "Facing domestic and foreign changes such as the intensification of threats against cybersecurity on a worldwide scale, and with the establishment of the Internet and other advanced information and telecommunications networks and the utilization of information and telecommunications technologies, and given the situation that it is an urgent issue to ensure the free flow of information and protect cybersecurity simultaneously, the purpose of this Act is to comprehensively and effectively promote cybersecurity policy by: stipulating basic principles of national cybersecurity policy; clarifying the responsibilities of the Government of Japan (hereinafter referred to as the "Government"), local governments, and other concerned public parties; stipulating essential matters for cybersecurity-related policies such as cybersecurity strategy formulation; and establishing the Cybersecurity Strategic Headquarters and so forth, together with the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Act. No. 144 of 2000), and as a result, attempting to enhance economic and social vitality, sustainable development and realizing social conditions where citizens can live with a sense of safety and security, and contributing to the protection of international peace and security as well as national security."

(2) Policy Areas the Strategy Encompasses

In the interconnected and converged information society, activities in cyberspace and those in the real world are closely linked. Ensuring a free, fair, and secure cyberspace in such hybrid society will make it possible for individuals in the real world to spend their daily lives safely and affluently; for enterprises to engage in vital economic activities; and for the international community to maintain peace and stability.

Japan is committed to ensure the rights and safety of the people, and to strive for the socio-economic development of the nation as well as building and developing international order. Standing by these ideals, and while undergoing a historical paradigm shift in the entire human society, the Government of Japan has set the following three areas as its policy goals, that are: the **improvement of socio-economic vitality and sustainable development**; the **creation of a society where the people can live safe and secure lives**; and, **peace and stability of the international community as well as national security**. The Government will implement the Cybersecurity Strategy to reach these goals.

Needless to say, Japan's economic growth, crisis management, and national security have relied on the sound functions of socio-economic systems, and looming serious threats to these socio-economic systems are challenges to the nation as a whole. It is a standing policy of the Government of Japan: to promote IT utilization[2], to assure the growth strategy[3] firmly, and to take all possible means to ensure Japan's national security[4], through cybersecurity assurance.

(3) The Future of the Nation the Strategy Envisions

Targeting the early 2020s blueprinted in this strategy, Japan has ongoing projects to promote the development of highly advanced social infrastructure, such as autonomous systems for self-driving cars and smart communities. Regarding the Tokyo Olympic and Paralympic Games scheduled in 2020, while there is a very basic premise to take all possible measures to ensure the security of various social

---

[2] Declaration to be the World's Most Advanced IT Nation (established on June 14, 2013; revised on June 24, 2014) indicates: "Under the circumstances, as Japan strives to become the world's highest level IT-based society, reinforcing cyber security will be imperative not only for national security and crisis management, but also for bolstering Japan's industrial competitiveness through the use of IT and data."

[3] National Revitalization Strategy (established on June 24, 2014) indicates: "To ensure the Growth Strategy, the free flow of information as well as the safety and reliability in IT usage must be assured…"

[4] National Security Strategy (established on December 17, 2013) indicates: "…cyberspace is necessary for promoting both economic growth and innovation through the free flow of information in cyberspace. Protecting cyberspace… is vital to secure national security."

systems supporting the Games, it will surely offer a great opportunity for Japan to showcase its national excellence to the outside world. Towards the coming future where ICTs are interconnected with and embedded in physical objects and services, it should be reaffirmed that Japan has unique advantages cultivated over long periods of time, which have earned global recognition as the "Japan brand," such as the inventions of high-quality, technically superior products and services that have satisfied consumer confidence at home and abroad, and the safe and secure social systems that have developed by organically integrating these superior products and services. What Japan needs is a strategy to leverage these national advantages or the "Japan brand" for the improvement of its national competitiveness.

To utilize cyber-physical integrated space, it is essential to have capabilities for taking appropriate actions against potential threats hidden behind its convenience; and to this end, "investment" will be required to generate immense added values. Such active "investment" will enhance and sustain Japan's reliability in the international community for many years to come, and thereby will enable Japan to make progress towards a more affluent society.

4. Basic Principles

Japan affirms the following basic principles in policy planning and implementation for reaching the objective of this strategy.

4.1. Assurance of the Free Flow of Information

The advancement of cyberspace as a hub of creativities and inspirations is relied on the assurance of the free flow of information in cyberspace. Japan considers that it is imperative to create and ensure a cyber environment where the transmitted information will be neither censored nor altered without any legitimate reason, and will be delivered to intended recipients.

In examining regulations in cyberspace, the free flow of information must be fully respected, and careful attention should be given to the protection of individual privacy as well. At the same time, due considerations should be made to maintain the proper balance between necessary regulations and the protection of privacy. As a basic condition for the free flow of information in cyberspace, morality and common sense are requested not to offend rights and interests of others.

4.2. The Rule of Law

In the interconnected and converged information society, the rule of law should be thoroughly attained to cyberspace in the same way as it is applied in physical space. The rule of law is essential for cyberspace to be developed as a secure and reliable space with equal access for everyone. In Japan, cyberspace is governed by laws, rules, and norms. Similarly, international law and other international rules and norms should be applied to cyberspace so that cyberspace would be also governed by the rule of law in an international context.

Furthermore, as cyberspace has continued to expand and it has been utilized by various actors all over the world, it is required to establish international rules and norms in conformity with universal values, such as freedom and democracy, for peace and stability of the international community.

Japan will continue to engage actively in the development and implementation of these international rules and norms, and will also act on the steady acceptance of such rules and norms by every country, taking into account its domestic situations.

4.3. Openness

Cyberspace must not be exclusively dominated by a certain group of actors, but must

be open to all people who want to utilize it. With its openness and by maintaining assured interoperability, cyberspace connects ideas and knowledge, and brings new values into the world. At the same time, the majority of people's access to cyberspace must not be denied for political gains of a certain small group.

4.4. Self-governance

During the past decades, the Internet has made progress powered by the self - governance of various participating actors. Even if cyber threats become national challenges requiring the nation's all-out efforts, it is impossible, and inappropriate as well, for a government to take all charges for maintaining order in cyberspace. With a view to achieving the coexistence of order and creativity in cyberspace, Japan respects self-governance capabilities that the Internet has nurtured, and regards every stakeholder's self-reliant activities for the Internet management as the basic foundation of cyber governance, thereby promoting the development and operation of a self-governance mechanism for the fulfillment of the functions and missions of various social systems connected to cyberspace, and for the deterrence of malicious cyber activities.

4.5. Collaboration among Multi-stakeholders

Cyberspace is a multi-dimensional space composed of various stakeholders' activities in a variety of layers. From this viewpoint, it is necessary for the Government and all cyberspace-related stakeholders, including Critical Information Infrastructure (CII) operators, enterprises, and individuals, to share a common vision of cybersecurity and fulfill their organizational responsibilities and duties or make individuals' efforts. The Government bears a responsibility to foster properly coordinated relationships among these stakeholders. In building such coordinated relationships, Japan will take dynamic counteractions against cyber threats, by introducing interactive and real-time information sharing and other actions, taking into account current situational factors, such as fast-growing sophisticated cyber attacks.

On these principles of the strategy, any act of terrorism and other behaviors that threaten peace, and any act to support terrorism or such destructive behaviors, will not be tolerated with respect to the freedom of people; instead, these principles should be reflected in cybersecurity policies in harmony with perspectives of people's safety and security as well as national security. In line with these five principles, and to protect the people's security and rights, Japan reserves, as options, all viable and effective measures, i.e. political, economic, technological, legal,

diplomatic, and all other feasible means. Cybersecurity policies, as expected by the people, should enable the coexistence of the freedom of expression and the protection of their privacy; and the protection of their rights by deterring malicious actors' activities supported by timely and appropriate law enforcement as well as the development of other relevant regulatory mechanisms.

Building the state of a world soundly governed by the rule of law it is a way to stabilize the global market and inspire innovations; similarly, it also contributes to Japan's national security as well as peace and prosperity in the world, as malicious actors are not tolerated in such the world.

5. Policy Measures towards Achieving the Objective

The following are the goals and directions of the policies scheduled to be implemented in coming three years, for delivering results of the strategy. They are based on the five basic principles previously described and illustrated with respect to each policy area where the strategy contributes. Each policy is expected to be consistent with the following three approaches, to the maximum extent feasible.

(1) Being Proactive, not Reactive

Perpetrators in cyberspace are always advancing their modus operandi. Given the reality that cyberspace has vulnerabilities inherent to itself, Japan will not wait until some damage would be done; instead, Japan will take necessary measures proactively, by conducting analyses on future social changes and potential risks.

(2) Acting as a Leader, not Just a Follower

For achieving the goal set in (1), with recognition that cyberspace is a space built and operated by actors of the private sector as the main driving forces, Japan will implement policies to catalyze their self-motivated activities and their own initiatives. At the same time, Japan will undertake a leading role as a responsible member of the international community and proactively contribute to peace and stability in cyberspace that is global by nature.

(3) Envisaging Cyber-Physical Space, not Only Cyberspace

All kinds of physical objects and people have been interconnected by ICTs in a more multidimensional way, and the integration of physical space and cyberspace has become more intertwined. Attention should be paid to the fact that any event in cyberspace affects society various events including those in physical space. Recognizing the transformational process leading to an unprecedented society consisting of the IoT systems, Japan will implement policies by precisely capturing such social transformation.

5.1. Improvement of Socio-Economic Vitality and Sustainable Development

In the emerging interconnected and converged information society, all kinds of physical objects, from personal computers, home electric appliances and automobiles, to robots and smart meters, are connected to networks including the Internet. This interconnectivity will lead the emergence of transformative systems (Internet of Things systems; hereinafter referred to as "IoT systems") that will be able to develop new services by using Big Data generated in the networks, and so on. As the IoT systems will prevail, the integration of cyberspace and physical space will become more advanced and intensive. It is foreseen that enterprises will shift their efforts to create new business by utilizing the IoT systems and adapt existing businesses to this more sophisticated environment. For the improvement of Japan's socio-economic vitality and sustainable development, it is highly important that enterprises in Japan will not fail to seize these new business opportunities.

When enterprises provide new services by using the IoT systems, ensuring "security as a quality feature" is a prerequisite. It means that safety and security are pre-installed as essential service quality features, which is expected by individual customers and business users in the market. Suppose a physical object was remotely controlled by cyber attacks to make unplanned movements; personal data was stolen via a wearable device that was compromised or hacked; or, a database involving various stakeholders was hit by a single cyber attack and several millions or tens of millions of personal and other information were stolen, which resulted in causing serious social and economic impacts. Such risks closely connected to real space would harm the reliability and quality of the IoT-based services. It suggests a new challenge to tomorrow's society at large, that is, how to minimize security risks at an acceptable level, in counterbalance with the merits of the services provided with the IoT systems.

In the interconnected and converged information society, for enterprises in Japan to lead the national economy by realizing the creation of new business and adapting current businesses to the more sophisticated environment, and to bring about the largest benefits of the society of this kind, it is required to take proactive measures in industry-academia-public partnerships to address the above-mentioned challenge. Likewise, it is the demands of the current digital age to achieve higher level security than ever before as a quality feature of services by using Japan's advantages developed over years, including the provision of high-quality services, the enterprise management to build stakeholder confidence, and the creation of the fair market environment. All of these efforts to meet the new demands will become

a source of corporate values and international competitiveness.

In this line of thought, with regard to the IoT systems for realizing new services in the interconnected and converged information society, enterprise management, and business environment supportive for them, the Government will take the following strategic approaches.

5.1.1 Creation of Secured IoT Systems

Given the prospect for the massive use of the IoT systems during the Tokyo 2020 Olympic and Paralympic Games, the success of this world event will not be achieved without industry-academia-public coordination to make up-front investments in the assurance of high level security as a quality future in the IoT systems. Without such joint efforts, it is also difficult for enterprise in Japan to create new business and new employment opportunities by utilizing the IoT systems.

Aiming at creating the secured IoT systems capable of meeting market needs by 2020, and subsequently enhancing the international reputations of Japan's IoT systems, the Government will make efforts as follows.

(1) Promoting New Business Harnessing Secured IoT Systems

For an IoT systems-related new business to become successful, it is imperative to achieve high level security as a quality feature, which is the base of competitiveness. The IoT systems will not become intrinsically secured, however, just by retrofitting security, which would rather cause a large increase in cost. In this context, the Government will promote the idea of "Security by Design," an approach to incorporate the assurance of security into the initial phase of the planning and design of the entire IoT systems that include existing systems as part of them. More specifically, as to IoT systems-related business, the Government will promote security measures for these systems in a cross-sectoral manner, based on the Security by Design approach, and will give its prioritized support to the growth of such new business.

(2) Improving Structural Frameworks Concerning IoT Systems Security

For the improvement of socio-economic vitality and sustainable development, it is crucial to stimulate business innovation in IoT systems-related large scale business with the pertinent cross-industrial coordination among stakeholders of industries, academia, and the public sector. In this course, such business should be promoted in the Security by Design approach. To make it possible for relevant stakeholders to collaborate based on mutual confidence and each stakeholder's self-motivated activities, it is necessary to build a common understanding on relevant matters

regarding security measures required for the business concerned, e.g. the goals, means, and time frames, and to clarify the tasks of relevant stakeholders on that basis.

For example, the development of highly trusted Intelligent Transport Systems (ITS) concerns multi-stakeholders of industries, academia, and the public sector, including relevant governmental bodies, enterprises, and research institutes. It is expected that: these stakeholders first develop objective insights on both of the coexisting advantages and risks, which would be brought by the adoption of ITS; second, they build a common understanding on related factors, e.g. required security measures, their implementation methods, and time frames; then, based on these recognitions, they make each stakeholder's tasks explicit. In this way, they can accelerate their collaborations based on mutual confidence and each stakeholder's self-motivated activities, and it will result in effective and high value-added business.

In this view, among the government-led IoT systems-related large scale business, the Cybersecurity Strategic Headquarters will handle those possibly having substantial impacts on socio-economic activities in order to facilitate program planning, policy formulation, and overall coordination required for cross-cutting cybersecurity measures; this will be done with an aim to promote the consistent and exhaustive implementation of required measures, for example, by promoting organized and converged coordination among relevant governmental bodies and entities.

(3) Considering Regimes for Enhanced IoT Systems Security

For the timely introduction of the IoT systems, which are assured with a high level security as a market-expected quality feature, in the market, appropriate security measures must be taken in the whole supply chain of the IoT systems. This means that stakeholders will need a policy platform to build a common understanding on security measures required for the entire IoT systems and the individual components of the IoT systems. In addition, they can challenge new business opportunities more easily, if there are safety guidelines and/or reliability indices, including those from security perspectives, as required in progressively introducing the IoT systems into the market. For these reasons, the Government will, in collaboration with industries and academia, establish comprehensive guidelines and standards for IoT systems security, including the components of the IoT systems, such as M2M (Machine to Machine) devices and wearable devices, in the energy, automotive, medical, and other relevant industries.

Meanwhile, it is impracticable to provide the secured IoT systems, unless necessary measures are taken, e.g. releasing and installing security patches or software updates, by quickly pinpointing technical problems developing in cyberspace. The

Government will seek measures for relevant parties to make concerted efforts: to examine the vulnerabilities of the IoT systems and devices comprising the IoT systems; to encourage the suppliers of the IoT systems and devices to take necessary actions to modify detected vulnerabilities; and to elaborate to create specific means to inform users of the IoT systems and devices about safeguard measures to fix the detected vulnerabilities. Similarly, the Government will promote relevant parties' collaboration to: synthesize and analyze the data on security quality and threats detected in the use-phase of the IoT systems; feedback the results of synthesis and analysis to stakeholders, such as IoT systems developers; and realize and provide more secured and higher-quality services.

(4) Implementing Technological Development and Demonstration Related to IoT Systems Security

For the purpose of the promotion of new business creation utilizing the IoT systems, it is necessary to advance technological development and other measures to assure security, by addressing risks associated with the procurement and introduction of unreliable and cheap devises, based on the understanding that IoT system components have the characteristics different from those of conventional information and communications devices, for example, in terms of longer life cycle from design to disposition and limited throughput capacity. From this standpoint, the Government will work on the development and demonstration of ICTs, taking into account of technical features of IoT system components.

Besides, it is crucial to take security assurance measures for the entire IoT systems, for the purpose of providing services with immense added values by using the systems composed of a variety of networked physical objects. The Government will work on the development and demonstration necessary for the examination of IoT system-related security measures and others, including the development of system testing environment, social sciences research, such as the methodological improvement of risk analysis and evaluation on the entire systems, and the confirmation methods of the authenticity of hardware including IC chips.

5.1.2 Promotion of Enterprise Management with a Security Mindset

For the creation of new business and other business activities, enterprise management in the interconnected and converged information society requires, in addition to the existing cybersecurity measures, the more comprehensive and higher standards of cybersecurity measures, including the monitoring and assessment of security risks and appropriate investment decisions on management resources; the promotion of the adoption of security functions in products and

services; cybersecurity human resources development; and the improvement of organizational cybersecurity capabilities.

For this reason, the following will be undertaken to promote the enterprise management with a security mindset at enterprises in Japan.

(1) Changing the Thinking of Senior Executive Management

It is indispensable for enterprise management that senior executives utilize their business-critical systems and trade secrets, being aware of their strategic values and roles. In bringing products and services in which high level security is assured as a quality feature to the market, and in making management decisions for new business creation, cybersecurity knowledge has become a basic competency required for enterprise senior executives. For the enhancement of Japan's socio-economic vitality as well as sustainable development, it is necessary that more enterprise senior executives will grasp such societal changes precisely, and raise awareness of security measures not as an inevitable "cost" of business but as the "investment" for more progressive management. To this end, the Government will build a guiding framework that enables stakeholders, such as the market and investors, to properly evaluate enterprises' efforts to address cybersecurity as a critical management challenge; and a framework that gives financial advantages, e.g. fund-raising, to enterprises making such efforts. Similarly, the Government will implement collaborative awareness raising activities with the private sector to cultivate the cybersecurity understanding of enterprise senior executives.

Meanwhile, to incorporate cybersecurity in their business strategies, it is necessary for enterprises to assign a chief cybersecurity executive at the board level. To this end, the public and private sectors will work together, aiming that Chief Information Security Officer (CISO)'s functions will be adequately positioned at the senior executive management level of each enterprise.

(2) Fostering Cybersecurity Workforce for Advanced Management Skills and Competencies

To leverage cybersecurity perspectives and capabilities in enterprise management, it is necessary for both senior executive management and cybersecurity professionals to share their corporate management strategy and the directions of cybersecurity challenges and solutions. The Government is planning to promote the creation of talent pools of intermediators, who are capable of understanding management policies decided by senior executive management; presenting cybersecurity visions; and facilitating the communications between senior executive management and cybersecurity professionals.

As cybersecurity measures have become indispensable in enterprise management and business strategies, there are increasing organizational needs for enterprises to develop cybersecurity talent as their in-house workforce. To respond to such needs, the Government will examine long-term human resources strategies and performance appraisal methods, taking into consideration career paths for cybersecurity professionals, intermediators, and senior executives responsible for enterprise risk management including cybersecurity risks, and will encourage senior executive management to adopt such cybersecurity workforce development policies.

(3) Strengthening Organizational Capabilities

In the interconnected and converged information society, installing assured security in products and services will enhance enterprise competitiveness and will lay the foundations for the continuity and progress of enterprise activities. In this context, the Government will seek to increase the understanding of the value of the "Security by Design" among relevant actors working on products and services. From the viewpoint of the protection of trade secret and business continuity, the Government will promote and disseminate information about effective business management, e.g. risk-analysis-based organizational management, and will take necessary measures to enhance cybersecurity throughout supply chains beyond the barriers of organizations.

Moreover, with regard to the improvement of response capabilities against cybersecurity incidents, such as cyber attacks that would pose serious business risks to enterprises, it is encouraged that enterprises will adopt necessary measures, such as creating and operating a CSIRT (Computer Security Incident Response Team) with liaison functions for incident detection and response; developing plans and tools for rapid response to and recovery from cybersecurity incidents; conducting cyber exercises; and improving corporate business functions for more effective public communications; the Government will support these efforts of enterprises for the aimed improvement in word and deed.

In addition, the Government will provide its support and advice to enterprises by creating the guidelines of and other information on cybersecurity-related management, including the improvement of organizational cybersecurity mechanisms under the leadership of senior executive management, effective measures based on the latest trends in cyber attacks and damages, and information disclosure policies; the Government will also establish an objective framework to evaluate enterprises' activities taken on the basis of such support and advice with certain evaluation methods, such as third party certification. As for information sharing, including information on measure-related challenges, best practices, and

the latest trends in cyber threats and incidents, the Government will support the further advancement and expansion of information sharing networks in the private sector and between the public-private sectors, including platform building for information sharing, by actively utilizing incorporated administrative agencies with cybersecurity-related knowledge and experiences, as well as organizations and other entities with incident information sharing and analysis functions, e.g. ISACs (Information Sharing and Analysis Centers).

5.1.3 Improvement of Cybersecurity Business Environment

For Japan's IoT Industry [5] and other ICTs-based digital businesses to become internationally competitive and subsequently become the engines of national economy, and for Japan to build capacities for the self-reliant assurance of cybersecurity, it is required to: improve domestic environment necessary for cybersecurity-related businesses to become as a growth industry; and develop a fair market environment in Japan as a basis of every business. The Government will implement the following measures, aiming at the improvement of business environment where assured cybersecurity and enhanced international competitiveness of enterprises in Japan can be achieved.

(1) Promoting Cybersecurity-related Businesses

Along with the growing IoT industry and associated businesses, it is anticipated that the demand for cybersecurity-related businesses, including consulting and human resources development business, will be further increased in the future. The Government will support the development of cybersecurity businesses, for example, by fostering enterprises having a potential for a large scale business at home and abroad, venture business, and other prospective businesses, so that they could meet the increasing demand and become a growth industry as a whole.

Initially, for the development of global networks to collect cyber-related information and for the promotion of intelligent business with data analysis and information service capabilities in this regard, the Government will work on to establish leading projects of Japan's cybersecurity-related businesses, by taking measures, such as extensive and intensive investment using sovereign wealth funds (SWFs) in the cybersecurity field.

Meanwhile, given that the utilization of secured cloud services is considered to be effective for small and medium sized enterprises and other entities having a

[5] Industry related to IoT systems, including the provision of devices and services.

difficulty in building sufficient security environments by themselves, the Government will promote the wide implementation of relevant measures, including security audit regarding cloud services.

Additionally, in the cybersecurity field that requires high maneuverability to address its constant changes, it is critical to vitalize business venture and other enterprises striving for innovative new business and technological development. For this reason, the Government will utilize SWFs to undertake such activities as the promotion of collaborative research and development (R&D), including international exchange programs among domestic and foreign venture enterprises; the promotion of public research institutes and venture enterprises; and nurturing venture enterprises by taking advantages of R&D achievements.

Furthermore, to promote cybersecurity-related businesses, it is necessary to undertake the review of the existing mechanisms flexibly. The Government will work on necessary reviews, including the clarification of the applicability of the copyright law to reverse engineering [6] for security purposes and the reexamination of necessary mechanisms.

(2) Developing Fair Business Environment

For building economic systems that always spur innovation and produce corporate profits, it is essential to protect the values of technological information, including enterprises' core technologies and production expertise. The Government will implement necessary measures, including legislative measures to safeguard enterprises' intellectual property more firmly and to enhance the measures taken in the case of violations; awareness raising activities; and practical training and exercises. Besides that, the Government will take a strict action against any reprehensible conduct using security as an excuse or a reason to produce negative effects on international trade rules and agreements.

(3) Improving Environment for Japanese Enterprises' Global Operations

For Japan's Internet of Things industry and cybersecurity-related businesses to become internationally competitive and subsequently lead the national economy as a growth industry, Japan's policy perspectives in this regard must be fully incorporated in international frameworks, including international rules and norms. Working in tandem with industries and academia, the Government will act as a global leader in international discussion for establishing the international

[6] A practice or a process of analyzing and disassembling software and hardware to uncover structures, specifications, purposes, element technology, and others.

frameworks of mutual recognition arrangement regarding the international security standards as well as the evaluation and certification mechanisms of the IoT systems, including control units; the Government will also work on information sharing and the dissemination of Japan's best practices in international settings.

For the international operations of Japan's IoT industry and cybersecurity-related businesses, it is essential to assure security in social infrastructure abroad, such as the security of data produced and circulated in the IoT systems. From this standpoint of view, the Government will support the development of necessary mechanisms for cybersecurity as well as outreach and awareness activities in the Association of Southeast Asian Nations (ASEAN) and other countries that have strong economic ties with Japan.

In addition, so-called "supply chain risk[7] management" has become critical, as the international operations of Japanese enterprises have expanded in recent years. Taking it into consideration, the Government will promote supply chain risk management, for example, by promoting necessary R&D as well as bilateral and regional cooperation with ASEAN and other countries.

[7] Risks existing in the processes of design, production, procurement, installation, and operation of devises (including IC chips) and systems; these risks include a risk that viruses and malicious programs might be installed during these processes.

5.2. Building a Safe and Secure Society for the People

In recent years, there have been a growing number of incidents seriously threatening the people's living, particularly, the security of individual personal information and properties; and associated damages have become more grave and widespread. Under the circumstances in which the cyberspace environment will be further drastically evolving, e.g., with the expanding IoT systems and the launch of the Social Security and Tax Number System (the My Number system) operation, a safe and secure society for the people cannot be built, unless multi-layered cybersecurity is assured by relevant multi-stakeholders, from governmental entities, local governments, and cyber-related business operators, to private enterprises and each individual citizen.

The functions and services of CII and those of the governmental bodies are the mission-critical infrastructure for the people's living and socio-economic activities. Since it is highly likely that any interruption of these functions and services will cause direct and significant consequences to the people's safety and security, it is crucial to take all possible measures to address and prevent such events. It is necessary to take approaches based on "mission assurance" in which mission owners should analyze risks and should have discussions with asset owners from the viewpoint to accomplish the functions and services of CII or the governmental bodies. Mission owners should ask comprehensive decisions of senior executives, providing information on vulnerabilities including resultant risks.

While Japan will certainly draw the world's attention towards the major international events, including the Tokyo 2020 Olympic and Paralympic Games, it is anticipated that these events will attract malicious actors' attention for cyber attacks and other cyber-related threats. As a matter of national prestige, Japan is determined to make concentrated efforts to address cybersecurity concerns, in close coordination among relevant stakeholders. Further, Japan will maintain and advance knowledge, skills, and experiences to be gained from these future occasions, as precious national assets that will be meaningfully utilized for the people's safety and security.

In this view, aiming at responding to cyber threats and subsequently building a society where the people can live safe and secure lives, the Government will implement the following measures.

5.2.1 Measures for the Protection of the People and Society

Protecting the people and society from cyber threats requires the seamless, secure,

and stable provision of devices and services comprising cyberspace, as the essence of a safe environment for cyberspace users. It also requires self-motivated efforts of cyberspace users, including individuals, enterprises, and organizations, to raise their cybersecurity awareness and literacy, and take cybersecurity measures voluntarily. Additionally, for inhibiting malicious behaviors and other threats in cyberspace, it is crucial to enhance necessary measures proactively to track incidents and prevent the recurrence of the incidents, together with preventive measures against potential crimes and threats in cyberspace.

(1) Building a Safe and Secure Cyber Environment for Users

Private enterprises, including digital device manufacturers, Internet service providers, network management business operators, and software developers, are the major providers of the components of cyberspace, such as devices, networks, and applications. Similarly, tools to deal with cyber risks are also provided mainly by the private sector.

Besides a pursuit for convenience, being mindful of their responsibility to eliminate vulnerabilities in all of their services and products, these cybersecurity-related business operators are encouraged to take the Security by Design approach by which security assurance is embedded into the initial phase of system planning and design, and give adequate explanation about this embedded security feature to their customers. They are also encouraged to make their efforts, in close coordination with the Government and relevant governmental entities, to improve cyber attack-related incident detection and analysis functions, and take necessary actions, such as issuing security alerts and tips for their customers and general users.

Therefore, the Government will enhance information gathering regarding vulnerabilities, e.g. software vulnerabilities; and the coordination and enhancement of monitoring systems to detect various cyber attacks on the Internet.

In order to protect the users of cyberspace from cyber risks which require urgent attention, such as a possible exploitation of vulnerable devices for being used as springboards of cyber attacks, and to build a safe and beneficial Internet environment, the Government will elaborate necessary measures to prevent a damage possibly induced by malware infection, in addition to provide security alerts and tips for the users of compromised devices.

Furthermore, there are ongoing efforts towards 2020 to improve Internet communications environments for foreign visitors coming to Japan, e.g. expanding public Wi-Fi spots. Under the circumstances, the Government will reexamine necessary measures from the viewpoints of cybersecurity as well as user-friendliness.

(2) Promoting Security Measures Taken by Users of Cyberspace

Regarding the Internet use with personal computers, smartphones, and other devices, on the one hand, public awareness and knowledge of cybersecurity has hardly reached a sufficient level; there is another concern, on the other hand, in current environment where cyber risks have become more complex and diversified, that Internet users with insufficient cybersecurity awareness would become victims and end up becoming offenders and causing subsequent cybersecurity incidents unknowingly.

To address such concerns, and to support the self-help efforts of the public or Internet users, the Government will promote outreach and awareness raising activities in coordination with relevant stakeholders, such as the "Cybersecurity Awareness Month" and awareness raising of appropriate actions against malware and suspicious emails. Particularly, the Government is planning awareness raising activities for the youth, more specifically those who are just about to begin to use the Internet, along with their parents or guardians. Additional efforts will be made to promote tailored awareness raising activities for those who do not belong to any organizations, such as a school or a company, for they often do not have enough opportunity to learn about cyber threats and cybersecurity measures. Moreover, the Government will continue to drive human resources development policies to foster cyber experts who are capable of answering Internet users' questions and concerns, as well as the activities of these cyber experts.

In addition to comprehensive awareness raising activities for the public at large implemented by the Government and its relevant entities, it is encouraged to revitalize local community-based outreach and awareness raising activities, for such activities are suitable to take multifaceted approaches to meet diversified needs of the people who have different backgrounds in terms of age-groups, occupations, life styles, and others. The Government's actions will include strong support for grass-roots local activities that enable the promotion of outreach and awareness raising activities at the local level in collaboration among multi-stakeholders of industries, academia, and the public and private sectors.

For the assurance of the people's security and safety, it is critical to raise awareness not only for individuals but also for organizations and entities, such as private enterprises or organizations engaging in a wide variety of economic activities, local governments responsible for administrative services directly related to local residents, and public entities including educational organizations handling huge volumes of personal information of students, school children, and their parents or guardians. Especially, for organizations and entities which have difficulties to take necessary cybersecurity measures by themselves, such as small and medium sized

enterprises and small local public entities, the Government will strengthen necessary measures, taking into consideration that they require the collaborated efforts of the stakeholders of the Government, relevant entities, industrial organizations, and others, to support awareness raising measures, including the organization of seminars, the formulation and dissemination of cybersecurity-related guidelines, the improvement of the structures to share cybersecurity information concerning the latest methods of cyber attacks and other relevant matters, and the implementation of training and exercises.

(3) Enhancing Measures against Cybercrimes

Along with the enhanced interconnectivity of cyberspace and physical space, the number of cybersecurity incidents closely related to individuals and enterprises such as illegal money transfers by exploiting Internet banking, stealing information by targeted attacks, and phishing has drastically grown. There is also a rise in the number of personal or confidential information theft, among which a large-scale personal data breach is one of the most serious cybersecurity incidents; as a result, these increasing cybercrimes have become serious social concerns. Without advanced cybercrime response and investigative capabilities, it is difficult to capture the reality of malicious cybercrimes, control cybercrimes appropriately in accordance with laws and statutes, and be ready to handle new methods of cybercrimes that would likely emerge in the near future.

For these reasons, the Government will strengthen: the improvement of structural arrangements for the enhancement of information gathering to obtain a better understanding of cyber threats; the improvement of cybercrime-related investigative capabilities; cybercrime control, international coordination and more. In addition, since advanced technical knowledge is essential to investigation, cybercrime control, and the prevention of damage and/or the spread of damage, the Government will advance accumulation of necessary know-how and technologies and other necessary skills by improving the organizational structures for digital forensics, such as the technological advancement for malware analysis and the sophistication of Internet-based data acquisition. Likewise, the Government will soundly strengthen human resources development and technological development to this end. Furthermore, for the purposes of cybercrime investigation and prevention, the Government will aim at the active use of knowledge and experiences of the private sector and the enhanced public-private partnerships including personnel exchange programs between the public and private sectors.

Since cooperation from cyber-related enterprises is indispensable for the assurance of cybercrime traceability, the Government will take measures necessary to make progress in this area. Especially with regard to the management of stored log data,

the Government will encourage relevant private enterprises to take appropriate actions based on the revision of the "Guidelines for Personal Information Protection in Telecommunications Business."[8]

5.2.2 Measures for Critical Information Infrastructure Protection

Various kinds of social infrastructures have ensured the people's living and economic activities, and a wide range of information systems has been used for the functions of these social infrastructures. In the circumstances, the public and private sectors must work together to protect CII, in particular, information and communications services, electric power supply services, and financial services, of which the functional failure or deterioration would risk enormous impacts to the people's living conditions and economic activities. Such task cannot be entirely designated to the Government as a sole stakeholder, leaving the private sector with no responsibility, or vice versa; rather, it calls for strong public-private partnerships. As CII is required to provide a continuous supply of service, for its protection, it is crucial to reduce the occurrence of system failures caused by cyber attacks or other reasons to the minimum extent; it is also crucial to carry out early detection of any system failure and prompt recovery from damage or failure.

The Government established the third edition of the "Basic Policy of Critical Information Infrastructure Protection [9] " and identified critical information infrastructure sectors[10]. Based on this CII policy, the Government has implemented various measures, including the enhancement of safety standards and awareness raising, the implementation of training and exercises, and the improvement of information sharing arrangement between the public and private sectors.

Having achieved substantial results in protecting Japan's CII, these existing measures will be implemented as they have been. Meanwhile, these measures would easily lose their effectiveness and become obsolete without any modification to

---

[8] 2004 Ministry of Internal Affairs and Communications Bulletin No.695. The Guidelines were established with the purposes of improving the user-friendliness of telecommunications services and protecting consumers' rights and interests, by establishing basic procedures respected by telecommunications business operators in terms of proper handling of information considered as secrecy of communications and other personal information.

[9] Established on May 19, 2014 by the Information Security Policy Council: revised on May 25, 2015 by the Cybersecurity Strategic Headquarters

[10] Information and communications services, financial services, aviation services, railway services, electric power supply services, gas supply services, government and administrative services (including local governments), medical services, water services, logistics services, chemical industries, credit card services, and petroleum industries.

match the needs of the constantly diversified social and technological environments related to CII. The Government will make efforts to regularly reexamine the existing measures and activities as indicated in the following sections, and coordinate and promote the specific approaches of strengthening cybersecurity for those measures and activities. Meanwhile, CII operators and their competent ministries have conducted critical information infrastructure protection (CIIP) against cyber attacks by setting the safety standards, including mandatory standards and guidelines; to this extent, with regard to CII sectors having the original standards of service maintenance and safety assurance stipulated by a specific law regulating a certain industry, the Government will carry out a constant review of the safety standards, taking account of current environmental changes in cyberspace.

(1) Conducting Constant Review on the Scope of CIIP

Due to social environmental changes, the accumulated relevant knowledge and experiences, and more, it has become necessary to include a certain sector, which is not currently identified as a CII, in the CII sectors, as the impact of the information system failure of the said sector is assumed to be serious. For this, the Government will conduct a constant review on CII itself. It should be noted that it is not necessary for the newly added CII sector to implement exactly the same CIIP measures as other incumbent CII sectors have done; because of an increasing number of the CII sectors, it becomes presumably difficult, too, to implement common measures across the CII sectors. From these standpoints, the Government will take necessary actions based on the characteristics of each sector, such as the degree of interdependence with other sector(s), the services it has provided, and any law concerning that sector. For example, the classification of the CII sectors may be one possible way of such review.

Meanwhile, as for the current CII sectors, for more reliable and secured service provision, it is essential to assure “cross-cutting sector-wide protection”, rather than “pinpoint protection” with each CII operator’s limited effort. In this sense, the Government will conduct a review on the scope of CII operators regularly. For example, the measures exclusively applied to the major operators would be expansively applied to small and medium sized enterprises; or, they would be more inclusively applied to peripheral businesses, too, such as relevant outsourcing contractors and major affiliated businesses that are indirectly related to the services provided by the CII operators.

In addition, consideration should be made to provide protection for private enterprises outside the CII sectors, since CII is not the single target of cyber attacks. With regard to Japan’s leading enterprises and those critical to national security, including those requiring certain measures, e.g. the physical protection of nuclear materials, the Government will further consider necessary measures, such as

enhanced information sharing arrangements, whether or not these enterprises fall in the definition of CII.

(2) Ensuring Effective and Prompt Information Sharing

As cyber attacks have become more complex and sophisticated, in order to counter diversified cyber threats appropriately, the public and private sectors must closely collaborate in sharing information on system failures possibly caused by cyber attacks. To make information sharing more active, it is essential to relieve CII operators' psychological burden of possibly losing credit or ruining reputation of their businesses if providing information to others; and enable them to recognize the advantages of such action. The Government will build consensus on necessary modification, such as concealing informers' identities and specifying the scope and limit of information to be shared, and create an environment where informers will not suffer any unreasonable loss or disadvantage from providing information. As for those handling the provided information, they are required to have adequate information analysis capabilities; and issue security warnings and alerts in a timely and appropriate manner based on the provided information. The Government will strive to create an interactive and advanced information sharing environment, including building platforms as a basis of collecting, analyzing, and sharing provided information so that CII operators can properly obtain information necessary for CIIP from cyber attacks.

In view of the year 2020, more effective and faster information sharing is required in building a world-class defense framework against cyber attacks. Given that it is effective to collect not only information on system failures at or above a certain level, which are subjected to reporting by a specific law regulating a certain industry and others, but also information on minor system failures as well as those showing the signs of cyber attacks or predicting cyber attacks, the Government has made efforts to collect such information, based on a consensus among relevant stakeholders; in the circumstances, the National center of Incident readiness and Strategy for Cybersecurity (NISC) and the competent ministries of CII operators will work in tandem more closely and engage in information gathering proactively. The Government will also work to strengthen coordination among relevant governmental entities, particularly to accumulate necessary information at the NISC for the purpose of building a structure for prompt information sharing with necessary measures, such as building a hotline between the NISC and CII operators, improving information sharing methods and procedures, and adopting automatic information processing.

When a CII operator reports a cyber attack to relevant governmental bodies responsible for incident response, the governmental bodies will work, as a

coordinated effort, on situational awareness to obtain an accurate understanding of what is happening, while helping the CII operator(s) manage the critical situation. The Government will extensively share obtained information on the occurred incident, including attackers' methods, with the governmental bodies, CII operators, and other relevant parties, to prevent the damage from becoming more serious and more extensive.

For the purpose of ensuring the effectiveness of these measures, the Government will conduct cross-sectoral training and exercises for stakeholders of the public and private sectors, and will continue to make necessary improvements.

(3) Offering Tailored Support to CII Sectors

As for local governments, their responsibility and the cooperative measures taken by the Cybersecurity Strategic Headquarters to support them are prescribed under the Basic Act on Cybersecurity. All local governments, regardless of their scales, have a unique status, as they are required the security standards similarly to those of the Government and government-related entities, because of their functions, e.g. handling sensitive information. There is an environmental transition expected in local governments, for they will need to adopt new systems due to the nationwide introduction of the My Number system. The Government will provide necessary assistance, in accordance with the Basic Act on Cybersecurity, for their security assurance, and will examine and take necessary measures regarding the information systems of local governments, with the object of strengthening cybersecurity for the operation of the My Number system.

The Government will take necessary cybersecurity measures, based on consideration of effective approaches, including operation systems development and improved operational frameworks build upon advanced cybersecurity measures; those measures include the separation of the systems for handling the affairs using the individual numbers prescribed under the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure from the Internet. At the same time, the Government will enhance monitoring and oversight mechanisms based on professional and technological knowledge and experiences, in coordination with relevant entities. Furthermore, aiming at building the monitoring and detection mechanisms to supervise the interconnected national and local operation systems of the My Number systems as a whole, the Government will build frameworks with capabilities of monitoring and prompt detection of cybersecurity incidents, taking account of possible information sharing with the Government Security Operation Coordination team (GSOC). Additionally, with regard to the intergovernmental and public-private coordination for authentication at the occasion of introducing the My Number system, the Government will also

work to improve environments necessary to make the best balance between increased user-friendliness and security assurance.

With regard to industrial control systems (ICS), there is a concern that IT malfunction may evoke the disruption of safety assurance and the interruption of the provision of sustainable services. Smart meters in the electric power supply services sector and factory automation systems in chemical and petroleum industries are good examples. For ICS to become more resilient, it is necessary to reaffirm the importance of assuring the safety of ICS, by implementing information security measures for ensured continuous service delivery.

In addition, there has been the shift of ICS to the openings of technologies and networks, e.g. the use of standard products and the introduction of open-standard protocols. As a result, the open control systems have become popular, for example, as replacements of the existing conventional equipment; on the other hand, that has created a pressing need for addressing vulnerability issues and unauthorized access. Under the circumstances, the Government will collect, analyze, and disseminate useful information, e.g. information on vulnerabilities of ICS and ICS equipment and information on cyber attacks. It will be done based on the information sharing arrangement in a harmonized manner with the sharing of information on other than ICS. The Government will promote the use of internationally approved third-party certification schemes that enable objective evaluations on the level of satisfactory security performance, taking into account that specialized knowledge and skills are necessary for the procurement and operation of ICS and other associated equipment.

5.2.3 Measures for the Protection of Governmental Bodies

As for the governmental bodies and government-related entities, the Government has addressed cybersecurity assurance by establishing and utilizing, as a main measure, the common standards for the governmental bodies. Up to these days, the Government has worked on further improving the standard of government-wide measures, and reflecting newly emerged threats and challenges in the common standards, where necessary.

Meanwhile, it is expected that social environment will be transformed more rapidly by 2020. It is more than likely that cyber attacks against the governmental bodies and government-related entities will become more sophisticated and manipulative, and that IT-related products and services would become more multi-functional and diversified. In anticipation of such rapid transformation, the Government must be ready to face a dramatic increase in cyber threats or unforeseen challenges accompanied by that. Many of the information systems currently in the design or

development planning phases will be operational in 2020, and will be required to remain secured for many years to come. Meanwhile, most of cybersecurity measures cannot work like a quick remedy for cyber threats. In this context, it should be taken into account that cybersecurity assurance in 2020 cannot be achievable unless proactive actions are taken well in advance before new threats and challenges emerge.

It is a prerequisite for the governmental bodies and government-related entities to continue the full implementation of ongoing cybersecurity measures so that they can take flexible and prompt counteractions to address not only existing threats and challenges but also unforeseen threats and other emerging concerns. The Government will focus its forward-looking effort on the priorities outlined in the following sections; incorporate them timely in the regulations, such as the common standards for governmental bodies; and ensure the full implementation of these regulations by certain measures, such as audit and daily learning.

(1) Strengthening Defense Capabilities of Information Systems and Promoting Multi-layered Measures against Presumed Cyber Attacks

To respond to cyber attacks, such as spear phishing e-mail attacks apparently aiming at stealing, damaging, or altering information, the Government will take government-wide, multi-layered measures based upon the assumption of cyber attacks. This must also include contingency plans for the possibility a certain entity would be used as a springboard for the entity that is the original target of a cyber attack. In promoting these measures, the Government will ensure that they are based on the common standards for the governmental bodies, and will conduct risk analysis intending to perform its administrative responsibilities, for the optimization of these measures as the entire governmental bodies.

i. Incident prevention

The Government will robustly implement preventive measures, such as giving support for announced software vulnerabilities and detected malware and utilizing electronic signature and certification technology, and will make prompt and flexible readjustments corresponding to environmental changes.

More specifically, the Government will strengthen: cybersecurity-related information gathering and analysis functions; and the organizational arrangements for government-wide information sharing and for cooperation with the private sector. The Government will also advance supply chain risk management and other measures to incorporate security assurance into the planning and designing phases of information systems. Furthermore, the Government will promptly and flexibly readjust the measures taken for the information systems in operation, in view of

environmental changes. Additionally, the review and improvement of the implementation status of information security measures will be undertaken through penetration tests and other examinations.

ii. Prevention of damage and the spread of damage

It is extremely difficult to prevent all cybersecurity incidents, such as malicious penetration into information systems by cyber attacks exploiting unrevealed vulnerabilities or using malware, including Zero-Day attacks. For this reason, while aiming to prevent the outbreak of cyber attacks, the Government remains equally determined to respond to cybersecurity incidents effectively and in a timely manner in order to obtain early situational awareness and to limit the harmful consequences of an attack as well as the spread of damage that the attack might cause.

More specifically, the Government will work on the enhancement of GSOC's functions covering the entire governmental bodies to detect and analyze cybersecurity incidents; the enhancement of governmental Computer Security Incident Response Teams (CSIRT) as well as situational awareness and risk management functions of every governmental body; and the acceleration and sophistication of information provision and sharing in the case of a cybersecurity incident. At the same time, the Government will implement training and exercises for incident readiness and subsequently incorporate lessons learned from such training and exercises in its cybersecurity policies and measures; the Government will also aim to improve the capabilities of personnel with designated cybersecurity duties and the coordination among these personnel; and to fully enforce organizational responses to cybersecurity incidents under the direction of senior executive officers of each governmental body. Moreover, for risk reduction by the improvement of monitoring effectiveness and other means, the Government will work on further reduction and consolidation of connections to the Internet in the governmental information systems. Additionally, the Government will strive to: reinforce fact-finding activities in the case of emergencies, including critical incidents involving a governmental body or governmental bodies; share the results of the fact-finding analysis in order to prevent the damage of the incident from spreading; and incorporate them in the existing measures.

iii. Damage mitigation

For mitigating damage over the period starting from the incident occurrence to the completion of the initiated emergency measure, the Government will take necessary measures to prevent the spread of penetration and not to allow attackers to accomplish the purpose(s) of their attacks.

More specifically, special consideration will be made on the improvement of

preventive measures against unauthorized access to personal information, sensitive information, and other information with high confidentiality or integrity requirement i.e. those of which leakage and manipulation would cause serious negative impacts on the people, society, and more. In this context, the Government will strive to achieve more trusted information management, including the separation of information systems, where necessary, according to the substance of administrative functions as well as the nature and quantities of information processed; and the use of operational regulations. The Government will also accelerate its effort to implement "defense-in-depth" measures against targeted cyber attacks, including those concerning system availability, such as system breakdown. In addition, the Government will work to establish methods to evaluate priorities regarding: the enhancement of incident response corresponding to different risks and their impacts; and focused measures for information systems.

(2) Achieving More Resilient Organizational Response Capabilities

The Government will seek to achieve more resilient organizational response capabilities that enable more flexible and prompt responses to accelerating changes.

The following are examples of the planned activities: the review and improvement of organizational arrangements and frameworks to enhance measures concerning the governmental bodies and government-related entities, by conducting periodic self-assessment, management audit from an independent perspective, and other assessments; and the promotion of risk-based and organized measures for and management of information systems, such as the formulation of risk management policies and the standards of measures on a basis of risk assessment, the establishment of a scheme for contingency planning based on consensus of stakeholders for unforeseen circumstances, and so on. Since there is no panacea for responding to unknown threats and other cyber concerns, the Government will also plan to create a community that contributes to government-wide information sharing on cybersecurity incidents and active dialogues. In addition, since human resources are the key of organized response capability, the Government will work to ensure enhanced cybersecurity literacy in the entire staff including senior executive officers. At the same time, the Government will foster and acquire cyber talent who will take a leading role to advance response capabilities of the governmental bodies and government-related entities; this will be done by utilizing qualifications and other special skills as one of objective criteria to evaluate individuals' competencies.

(3) Adapting to Technological Advancement and Change in Business Performance Styles

To perform administrative functions in a way adjusting to the sophistication and

rationalization of administrative affairs by the utilization of multi-functioned and diversified IT products and services, and in a way to meet the demands of the digital era, the Government will make efforts to prevent incidents and the deterioration of security standards due to the inappropriate use of new IT products and services.

More specifically, the Government is planning to collect the government-wide status data regarding the adoption of new IT products and services as well as the information on implemented measures; and to establish and implement the common measures across the governmental bodies, taking into account the characteristics of these IT products and services. In terms of the changes in the styles of performing administrative functions based on the IT use, the relevant governmental bodies and government-related entities will closely collaborate to adapt the performance styles appropriately, based on assured cybersecurity.

(4) Comprehensively Enhancing Measures through the Extended Scope of Monitoring and Others

To strengthen cybersecurity throughout the government bodies as a whole, the Government will aim at the comprehensive enhancement of measures taken by incorporated administrative agencies and by special corporations closely working with the governmental bodies to perform their public functions.

More specifically, the Government will work on: the improvement of incident response capabilities of such entities; the enhancement of auditing of such entities by their competent ministries; and the promotion of cybersecurity measures at such entities, in accordance with the governmental measures (as described above from (1) to (3)), taking into consideration their characteristics. The Government will gradually add such entities, in particular, to the subjects of monitoring by GSOC, taking into consideration equitable-burden sharing among beneficiaries; include such entities as the subjects of auditing and fact-finding activities that the NISC conducts as a mandate given by the Cybersecurity Strategy Headquarters; and take other necessary measures. With regard to the above-mentioned measures, the Government will examine promptly the necessary revisions of the relevant laws, in view of possible arrangement for coordination with relevant entities with professional knowledge and skills, and will take appropriate actions, where necessary.

5.3. Peace and Stability of the International Community and Japan's National Security

A free, fair, and secure cyberspace is global common domain, where communications in a global scale are available, and is a foundation for peace and stability of the international community. In particular, regarding cyberspace Japan firmly believes that recognizing the diversity of values, respecting self-governance and securing people's freedom of speech and corporate activities based on the rule of law will bring peace and stability to the international community, thereby ushering in prosperity for all. Indeed, Japan has built an economy and society where an extremely high-quality life and sustainable development are possible, through utilizing the benefits of free, fair, and secure cyberspace. On the other hand, domestically and internationally, social systems' dependency on cyberspace has been increasing and thus the situation in which cyber attacks significantly affect the socioeconomic activities in the real world with sophisticated method and with greater impact is arising. Under these circumstances, defending cyberspace from cyber attacks and ensuring its secure use are critically important challenges for peace and stability of the international community and Japan's national security which must be addressed imminently and drastically.

Addressing these challenges to ensure Japan's security, the Government will drastically enhance the response capabilities of the whole nation and further engage in cooperation and collaboration with allies and like-minded countries as well as confidence building measures with relevant states. In addition, from the viewpoint of pursuing a free, fair, and secure cyberspace, the Government strongly disapproves of exclusive possession, control, censorship, theft or destruction of information by oppressive regimes as well as malicious use of cyberspace by non-state actors including terrorists. Japan will proactively contribute to the maintenance of international order and ensure its national security by building peace and stability of the international community from the policy of "Proactive Contribution to Peace" based on the principle of international cooperation.

Under the above recognition, the Government adopts the following strategic approaches for building peace and stability of the international community as well as its national security. For the implementation of these measures, the Government will further advance the centralization of relevant information including those on cybersecurity measures of the governmental bodies and related entities into the Cabinet Secretariat, and enhance its common external responses.

5.3.1 Ensuring Japan's National Security

As all kinds of things, including the social systems, are networked and cyberspace is increasingly integrated with the real world; many organizations have heavily relied upon cyberspace. As a result, cyber attacks have become capable of causing great damages to state's politics, society, economy, and culture. Today, Cyberspace is not only for economic activities, but also for national security and intelligence activities. Disruptive activities, theft of classified information and falsification of data by organized, well-prepared, and advanced cyber attacks including those that are suspected as state-sponsored, are actual threats today.

To protect cyberspace from these advanced cyber attacks, it is necessary to take prompt and appropriate measures based on advanced knowledge at all phases: prevention, detection, and response. For this reason, through analyzing cyberspace in peacetime, the Government intends to further enhance its capabilities of early identification and situational awareness including the signs of cyber attacks by various actors, and of detecting and addressing threats promptly. To this end, it is critical to strengthen the Government's functions of information gathering and situational awareness, including information sharing with foreign governmental entities, and situational analysis, and to promote cross-sectoral and cross-cutting efforts comprehensively.

Moreover, it is necessary for Japan's national security to protect the function of social systems owned by the Government and critical infrastructure operators from cyber attacks. Regardless of the public or private sector, vertically-segmented structure and rigid conventionalism would be a favorable condition for attackers. The Government will share such an understanding with various relevant actors and further strengthen current cooperation with them to achieve a seamless and multi-layered protection against these attacks. In addition, the Government will further enhance its capability to respond to cyber attacks, which can occur at any phases, appropriately and accordingly to their scale and level.

Furthermore, bearing in mind that cyber attacks can be easily conducted across national borders, and there are some cases in which cyber attacks are suspected to be state-sponsored or linked with military operation in real world, it is essential to proactively enhance cooperation and collaboration with allies and like-minded countries or organizations on sharing threat information and human resources development among others. It is also important to advance confidence building with other countries.

(1) Enhancing Response Capabilities of Relevant Governmental Bodies

In order to respond to more diversified and complex cyber threat, it is critical to

enhance Japan's whole resiliency and capabilities. To this end, the Government will strengthen the capabilities of law enforcement agencies, the Self-Defense Forces, and other relevant organizations in both quantity and quality. In order for these organizations to play full part, the Government will consider a wide range of effective means such as reviewing various systems including human resources development and recruiting, introduction and learning of latest technologies, and R&D. In addition, to counter cyber attacks targeting the classified information owned by governmental bodies, the Government will enhance the efforts related to counter-cyber-intelligence in the Cabinet Information Research Office and other relevant entities.

(2) Utilizing and Protecting Japan's Advanced Technology

Japan's advanced technology is not just for securing Japan's economic advantage but are also a critical national asset in terms of national security. In particular, actors who deal with critical information for national security, e.g. technologies related to outer space, nuclear energy, security, and equipment of the Self-Defense Forces, need to keep in mind that critical information could become a possible target of cyber attackers worldwide. These actors will take all feasible means to ensure its cyber security to ensure Japan's national security, and effectively utilize the advanced technologies. Relevant actors will take necessary measures: further raising cybersecurity awareness of all the people involved in advanced technologies, enhancing monitoring and response capability against foreign cyber attacks, tightening examination and verification of goods and service procurement and taking other necessary measures, including enhanced collaboration between the public and private sectors for information sharing.

(3) Protecting Governmental Bodies and Social System

As governmental bodies have a mission to defend and support the people's living and socio-economic activities, the shutdown of their functions is a significant concern to the national security. The execution of missions of the governmental bodies relies on CII and other services provided by business operators responsible for the social systems. These business operators themselves have an important mission to continuously provide services indispensable for the people and society. Therefore, ensuring cybersecurity of these CII operators is of extreme importance for Japan's national security and the assurance of the missions of the governmental bodies as well as the continuous provision of services indispensable for the people and society. To this end, it is necessary for these operators, in collaboration with the governmental bodies, to take all feasible measures with a clear recognition of how the effect of cyber attacks on the provision of services will impact the execution of missions of the governmental bodies and the business operators themselves.

In this context, the Government and business operators in charge of CII and other social systems will further enhance their daily efforts to bring, share, and analyze beneficial information, such as vulnerabilities and attack information, and address to threats in a necessary manner. It is also expected to accelerate interactive information exchange between the public and private sectors.

As the defense authorities, the Ministry of Defense and the Self-Defense Forces will further enhance protection of their own networks and infrastructure, and deepen coordination with stakeholders relevant to the assurance of missions of the Self-Defense Forces in light of the possibility that cyber attacks against the social systems indicated above may become a major impediment to the accomplishment of their missions.

5.3.2 Building Peace and Stability of the International Community

Ensuring both cyber security and the free flow of information at a global scale is necessary for peace and stability of the international community.

Cyberspace is a space where data is transmitted and processed through hardware and software, which are managed and operated by various global actors and actors in countries all over the world, and linked by autonomous and cooperative networks. Therefore, in order to have active communications, social, economic, and cultural activities in such a space with international nature, it is necessary to ensure appropriate cybersecurity of globally widespread components, so that people can trust it when using it.

Through the free flow of information at a global scale, cyberspace has become a foundation for all kinds of social, economic, and cultural activities on earth, and has promoted mutual understanding across national borders. This remarkable global nature of cyberspace would be undermined if the authorities divide it with their excessive restriction or control.

In addition, in order to ensure security of cyberspace, it is important that Japan will implement measures to create an internationally stable cyber environment that leads to peace and stability of the international community, as well as Japan.

Under this recognition, with a view to build peace and stability of the international community, Japan will take a leading role as a responsible member of the international community, and engage in ensuring cyber security through international cooperation with various stakeholders as well as securing the free flow of information at a global scale based on the following policies.

(1) Establishing the International Rule of Law in Cyberspace

Recognizing the diversity of actors and values, Japan will take active roles in establishing the international rule of law in cyberspace, with the basic principle of the free flow of information.

i. Developing international rules and norms

Japan is of the view that existing international law applies to cyberspace. With regard to security in cyberspace, the Government has participated in the Group of Governmental Experts (GGE) established in the First Committee of the UN General Assembly, and the GGE submitted a report indicating that "international law … is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." Japan will further actively engage in the discussions on the application of specific individual international law, and subsequently make contributions to the development of international rules and norms for cyberspace with the view that existing international law is applicable to cyberspace.

In addition to the GGE, there have been discussions among multi-stakeholders focusing on socio-economic aspect, Internet governance and other topics in various fora including the UN and its specialized agencies, the Organisation for Economic Co-operation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC) and the Global Conference on Cyberspace. Japan will further cooperate with domestic and foreign stakeholders in these discussions and actively promote the development of international rules and norms with a view that ensuring the openness, interoperability, autonomy and the free flow of information in cyberspace will make a significant contribution to the development of society, economy, and culture.

ii. Materializing International Rules and Norms

Japan will contribute to the development of international rules and norms for cyberspace and will proactively engage in their materialization. For instance, in the national security field, Japan will advance confidence building measures, as described later, at conferences of international organizations or cyber dialogues with other countries, based on the results of discussions on the application of a specific individual international law. With regard to measures against cybercrimes, as a Party to the Convention on Cybercrime, Japan will make efforts in the expansion of its Parties, strengthen international cooperation among law enforcement authorities for a prompt and effective assistance in investigation, and enhance international investigation for arresting transnational criminals to effectively address cybercrimes that easily transcend national borders. The Government will

take the initiative in implementing international rules and norms and subsequently make contributions to the establishment of the rule of law in cyberspace and bring peace and stability to the international community.

(2) International Confidence Building Measures

Cyberspace has become a basis for all kinds of activities, including social and economic activities as well as military operations. Under such circumstances, it is necessary to deepen international discussions at the UN and other fora on how to prevent unexpected situations stemming from cyber attacks and share common understanding among many countries. To this end, the Government will actively provide information on its fundamental stance and share stances with many countries at multilateral conferences, such as the UN, as well as bilaterally in cyber dialogues and conferences. Moreover, Japan will promote international confidence building by creating multi-layered contact mechanisms, e.g. points of contact among countries or the private sectors, for transnational cybersecurity incidents during peacetime and conduct contact exercises and other measures.

(3) Measures against the Malicious Use of Cyberspace by International Terrorist Organizations

In order for cyberspace to remain a domain that contributes to peace and stability of the international community, it is necessary to prevent malicious use of cyberspace by international terrorist organizations. With the expansion of cyberspace, non-governmental actors that advocate extremism have been using cyberspace for malicious purposes such as the dissemination and demonstration of their ideas, recruiting and solicitation, and fund-raising for terrorism. Taking into account the international statements such as the resolutions of UN Security Council, Japan must implement measures against such international terrorist organizations in coordination with the international community. For this, the Government will take necessary measures, e.g. strengthening information gathering and analysis on activities of international terrorist organizations in cyberspace, including the utilization of technologies that gather terrorism-related information on the Internet.

(4) Cooperation on Cybersecurity Capacity Building

As a responsible member of the international community founded on freedom and democracy, Japan will actively engage in capacity building based on its experience and accumulation in ICT development.

It is necessary for various actors around the world to cooperate and address the transnational threats in cyberspace as the lack of competence of some countries or regions to address these threats would be a risk for the entire world including Japan.

In fact, it is confirmed that many cyber attacks against Japan have come from abroad.

In addition, the activities of the Japanese people and companies are globalizing; e.g. the number of people traveling abroad and enterprises expanding overseas are increasing. With the development of informatization, these activities become increasingly reliant to cyberspace and social infrastructure managed and operated by their destinations.

For these reasons, cooperation on capacity building to ensure cybersecurity of countries around the world would not only contribute to those countries that need the assistance but also benefit Japan and the entire world.

With the development of information communications society, Japan has been developing legislation and policy frameworks for cyber security, and it has engaged in the assurance of cybersecurity of governmental bodies, CII operators, other organizations, and individuals; measures against cybercrimes; human resources development to foster cyber experts; and R&D of cybersecurity technologies. Based on these experiences and accumulated knowledge, the Government will further actively cooperate on capacity building as a responsible member of the international community with a basic principle of the free flow of information. To this end, in full coordination and cooperation, the Government as a whole will make capacity building plans and implement them efficiently and effectively.

(5) Developing World-class Human Resources

In addressing these international cybersecurity efforts, it is necessary for the Japan to continuously participate in and contribute to international conferences to state its position and deepen communications with various actors around the world. The participants of such conferences would be required to have sufficient cybersecurity expertise as well as understanding on the context of each country's society, economy, culture and other aspects. Therefore, the Government will develop abundant high-quality international human resources, in both the public and private sectors that have technical expertise on cyberspace, and are well-versed in international relations, international security, international cooperation among other fields, and capable of successfully working at the international arena.

5.3.3 Cooperation and Collaboration with Countries around the World

By cooperation and in partnership with countries around the world, Japan will realize peace and stability of the international community as well as of Japan's national security. International cooperation and partnership also contributes to the strengthening of international capabilities to counter cyber attacks in which state

involvement is suspected. On the solid basis of the Japan-U.S. Security Arrangements, Japan will keep in mind its geographical and economic relation or the extent of shared values with partner countries, and as a responsible member of international community founded on freedom and democracy, Japan will expand and develop cooperation with other countries. In addition, from a perspective of avoiding and preventing unexpected escalations caused by cyber incidents arising from cyber attacks, Japan will make efforts in confidence building, establish international cooperation systems in various fields, and ensure cyberspace security.

(1) Asia Pacific

Asia Pacific region has a deep historical connection with Japan, and the flow of people among nations and investment by Japanese companies are increasing. As a responsible member of this region, Japan will vigorously promote international partnership on the cybersecurity field, cooperation towards capacity building, and collecting and sending information in this region, through various bilateral and multilateral channels.

Japan has a history of partnership with ASEAN for more than 40 years. In the cybersecurity field, Japan has a close and cooperative relationship through multiple channels such as the ASEAN-Japan Information Security Policy Meeting. Through the framework of international conferences or joint projects, and the continuous implementation of various and practical capacity building based on the needs of each country, Japan will further deepen and expand cooperation in the cybersecurity field with ASEAN countries, and actively contribute to the realization of resilient cyberspace of ASEAN. In addition, considering economic, social, and cultural situations of each ASEAN country, and the various views towards cyberspace, Japan will enhance bilateral cooperation with each member countries.

Japan will strengthen its cooperation and partnerships with regional strategic partners that share basic values. Japan will enhance bilateral cooperation in the cybersecurity field through various channels between those countries, such as the sharing and utilization of information on cybersecurity- related policies and cyber attacks from peacetime; and joint exercises against cyber attacks, and will address challenges in cyberspace in regional and international arena, hand in hand.

Japan will also exchange its views towards cyberspace or information on cybersecurity strategies, discuss the possibility of cooperation in the cybersecurity field, and deepen mutual understanding and partnership with other countries in the Asia-Pacific region. Japan will also actively participate in the regional frameworks, such as APEC and ASEAN Regional Forum (ARF), and take part in the development of economy, society, and culture by ensuring security and the free flow of

information in regional cyberspace.

(2) North America

Based on shared basic values, Japan will enhance its cooperation with the North American countries in the cybersecurity field. In particular, the United States is Japan's ally that closely cooperates at all levels, based on the Japan-U.S. Security Arrangements. Sharing common values on cyberspace as well, both countries closely cooperate and share information through the Japan-U.S. Cyber Dialogue, the Japan-U.S. Policy Cooperation Dialogue on the Internet Economy, the Japan-U.S. Cyber Defense Policy Working Group, and other various bilateral channels. Japan will continuously deepen its cooperation with the United States in a concrete manner, such as the sharing and utilization of information on cybersecurity-related policies and cyber attacks; response to cybersecurity incidents; and the implementation of joint projects in the area of advanced technology. Japan will also closely cooperate with the United States in responding to a wide range of cyberspace issues, including the development and implementation of international rules and norms, international security, and Internet governance, and make collaborative efforts for international peace and stability together. Furthermore, the defense authorities of both countries will advance sharing information on threats, joint training and exercises against cyber attacks, and cooperation for human resources development; and strengthen operational cooperation between the Self-Defense Forces and the United States Armed Forces under the new Guidelines for Japan-U.S. Defense Cooperation. By solidifying the whole-of-government cooperation, Japan will enhance the U.S.-Japan Alliance's deterrence and response capabilities.

(3) Europe

European countries which share basic values and principles, e.g. market economy, are Japan's partners that take leading roles in building peace and stability of the international community. As for the cyberspace issues, Japan will further strengthen cooperation with each country and relevant organizations of Europe, through various channels, including defense authorities; for instance, Japan will enhance the sharing and utilization of information on cybersecurity-related policies and cyber attacks from peacetime, joint training and exercises against cyber attacks, joint projects in the field of advanced technologies, as well as response to and cooperation on cyberspace issues in the international arena.

(4) Latin America and the Caribbean, Middle East and Africa

Regarding the Latin America and the Caribbean region as well as the Middle East and Africa region, Japan will build and strengthen its partnership with countries that share common values with Japan, and consider the possibility of cooperation and

partnership with other countries on capacity building and other measures.

5.4. Cross-Cutting Approaches to Cybersecurity

In order to achieve the three policy goals the improvement of socio-economic vitality and sustainable development; the creation of a society where the people can live safe and secure lives; and peace and stability of the international community as well as national security it is imperative for the Government to make a tireless effort for advancing prominent research and technological development and fostering outstanding talent as the engines for the accomplishment of these goals. Such cross-cutting approaches require a long period of time to produce tangible results and require a wide range of activities as well; the Government will take steps in mid and long term perspectives, and will make progress in these activities by harnessing relevant public-private business partnership or arrangements and those of relevant governmental bodies.

5.4.1 Advancement of R&D

ICTs have interwoven with the people's social activities, and used more widely in their economic activities, too, as the drivers of innovation. Along with the significant expansion of networked systems and devices, including those utilized by CII and others, now more than ever, there is a growing need for cybersecurity measures taken by the Government, private enterprises, and other relevant stakeholders. To combat evolving cyber attacks which have become more advanced, sophisticated, and complex on a daily basis, it is crucial to promote productive R&D to invent creative and innovative cybersecurity technologies in comprehensive R&D areas, including networks, hardware, and software. In line with the following R&D policies, the Government will promote R&D in coordination with relevant stakeholders, by profiting from the combination of diverse information, perspectives, and advantages held by each stakeholder.

(1) Improving Detection and Defense Capabilities against Cyber Attacks

For the protection of the Government, CII, enterprises, organizations, and individuals from cyber threats, including more sophisticated and complex cyber attacks, in the interconnected and converged information society where the IoT and cyber-physical systems have prevailed, it is required to further advance detection and defense capabilities based on a better understanding of actual situations. R&D for capacity building in this regard requires the profound environmental improvement that enables R&D to be implemented with a good grasp of actual threats and concrete needs. Additional attention should be paid to the point that it is important to put cybersecurity R&D into practical use with consideration of social

needs and promote the active utilization of R&D accomplishments in society. To this end, the Government will promote information and data sharing necessary for governmental bodies, researchers, and other relevant stakeholders in a user-friendly manner. For example, to boost resilience against cyber attacks, data suitable for academic evaluation, including the data transmitted in M2M systems, will be continuously collected in actual environments, and subsequently used for the development of data analysis technologies. Moreover, the Government will initiate necessary actions, including the examination of relevant laws and statutes as well as standards concerning research. It is also the Government's plan to improve defense capabilities, for example, by incorporating cybersecurity into the planning phase of the R&D projects promoted by the Government.

(2) Promoting Interdisciplinary Research on Cybersecurity

In combatting cyber threats, it is not sufficient enough anymore merely to consider risks on information systems or conduct academic research, since the impacts of cyberspace in the real world have increased due to the advanced integration of cyberspace and physical space. It requires the exploration of analysis methodologies across multiple areas, including laws and statutes, policies, current affairs, and technologies. From this standpoint, the Government will promote: the collaboration with multidisciplinary research that encompasses various fields, including social sciences perspectives, e.g. law, international relations, international security, and business management; the promotion of research on cybersecurity in interdisciplinary fields; and the examinations and R&D in a way to look ahead to future social and technological transformation, such as Big Data and Artificial Intelligence (AI). Needless to say, the results of various R&D, including those in the fields of science and technologies, must not produce adverse effects in human society.

(3) Securing Cybersecurity Core Technologies

To take measures against predicted cyber threats, including cyber attacks that are evolving every day, it is vital for Japan to secure its core technologies required to make self-reliant efforts for the invention and development of technological fundamentals of cyber attacks and cyber defense, the frameworks of systems, and so on. With regard to basic research that fosters core technologies, although they may not be exactly profitable in terms of business revenue, it should be noted that some of them, e.g. cryptographic research, will become a potential source of new business opportunities, if partnered with successful entrepreneurial ventures and other prospective actors, and that there are mission-essential technologies from a national security viewpoint and for other reasons. For this reason, the Government will seek to make steady progress in building supportive environments for R&D at appropriate research institutes, such as public research institutes, universities, and

other relevant organizations.

(4) Enhancing R&D in International Coordination

As for technological measures to tackle more advanced and sophisticated cyber attacks, in order to develop more progressive technologies for internationally-coordinated measures that enable accurate responses to cyber attacks, it is highly effective that "unique" technologies of different counties are organically linked each other and developed in such linkage, since cyber attacks are launched beyond the national borders. The Government will work hard on R&D in international coordination, paying careful attention to research contents and national security concerns. As part of ongoing collaborative efforts for various international standardizations, the Government will also strive to establish and disseminate the various international standards and the frameworks for mutual recognition related to cybersecurity technologies and others.

(5) Partnering with Relevant Entities

R&D achievement cannot be made overnight. It is a task requiring long term engagement. It is a common challenge not only for the field of cybersecurity but also for other fields of research to build R&D supportive environment and nurture researchers. The Government will promote active measures comprehensively in industry-academia-public coordination, taking cybersecurity viewpoints and environmental changes into account, and in coordination with the Council for Science, Technology, and Innovation and other relevant organizations that are major stakeholders of such measures.[11]

5.4.2 Development and Assurance of Cybersecurity Workforce

Today, ICTs are widely and extensively ingrained in the people's living as the social foundation. In the emerging interconnected and converged information society, cybersecurity is an essential literacy, to one degree or another, for a variety of human resources, from cybersecurity experts and conventional ICTs experts to IoT users. Cybersecurity workforce development is a pressing task for Japan, as there is a critical domestic shortage of cybersecurity experts, both in quality and quantity[12].

[11] For example, "Ensuring Cybersecurity in Critical Information Infrastructure, etc." was selected as a candidate of a new research project for the "Cross-Ministerial Strategic Innovation Promotion Program (SIP)" at the Council for Science, Technology and Innovation on June 18, 2015.

[12] According to the estimate of May 2013 made by the Information-Technology Promotion Agency, Japan (IPA), there were approximately 265,000 experts working in the field of information security; among them, however, only around 105,000 experts were considered to have required skills to perform their duties, and the rest of 160,000 were considered to be necessary for some kind of education or training to acquire the

As described in the following sections, the Government will make efforts to: expand cybersecurity education and education in cybersecurity-related fields; identify, foster, and recruit talented individuals; and create career paths in a long term perspective for cybersecurity-related personnel. Overall, the Government will establish guidelines to improve human resources development comprehensively and soundly.

It should be noted that it is necessary for such human resources to develop not only technological capabilities but also high ethical standards.

(1) Promoting Human Resources Development Corresponding to Social Needs in Higher Education and Vocational Training

Regarding highly skilled experts who will lead a future society, it is necessary to implement the quantitative and qualitative human resources development that matches social needs, in more organic industry-academia-public coordination. The Government will support higher education institutions, such as graduate schools, universities, and colleges of technology to implement programs to offer students learning opportunities to develop a solid foundation in both the basic theory and practice of cybersecurity and to advance their practical cybersecurity skills. In this regard, the Government will encourage these higher education institutions to ensure that these programs will have a component to evaluate students' basic qualities, in terms of their knowledge and other necessary competencies.

Furthermore, for building industry-academia-public partnerships, the Government will take measures of practical exercises for human resources development, such as developing cyber training conditions in a cloud environment and supporting educational material development through industry-academia-public partnerships, in addition to the improvement of close coordination and information sharing among them.

In the current circumstances where cybersecurity has become a business-essential challenge for organizational management, e.g. enterprise business management, the role of the intermediators capable of dualistic thinking, both from management strategy and technological viewpoints, is highly important; it is because they can work as moderators between the board level and security-related professional personnel, and as a result, can work to promote the appropriate allocation of business resources to security. In this sense, the Government will support higher education institutions to develop "hybrid" human resources or individuals multi-

---

lacked skills. On the other hand, according to the same estimate, approximately further 80,000 information security experts would be potentially in short.

talented with comprehensive knowledge and skills in various fields, from cybersecurity and ICTs, social sciences such as law and business management, to organizational management and others.

For the provision of secured products and services, cybersecurity-related knowledge is indispensable in engaging in the manufacture of products and services. Taking into consideration that cybersecurity is an essential literacy for multiple people, from experts in all of the ICTs-related fields to ICTs users, the Government will examine possible measures, including recurrent education at higher education institutions, the expansion of opportunities for practical exercises in industry-academia-public coordination, and the promotion of the active use of vocational training.

(2) Expanding Elementary and Secondary Education for Cybersecurity

In the interconnected and converged information society, it is the essential foundation for enriching and developing the people's socio-economic activities and living that the IoT systems and other ICTs are fully available for use by all actors, including individuals, enterprises, and governmental entities. In this society, cybersecurity is a literacy, to one degree or another, required for everyone. Cybersecurity literacy includes logical thinking capability and understandings of ICTs as well as the basic mechanisms of equipment. It is vital to cultivate such literacy based on school children's developmental stages starting from the elementary and secondary education levels. Moreover, learning cybersecurity at the pre-tertiary education level is critical for the development of cyber experts at the higher education stage; pre-tertiary learning is equally required for conventional ICTs experts and ICTs users to become cybersecurity literate.

The Government will further promote elementary and secondary education for: nurturing practical skills, scientific understanding of information, and participatory attitudes towards the data-driven society; facilitating understanding of information morality, including information security and other associated understandings; and fostering logical thinking capability and understandings of ICTs as well as the basic mechanisms of equipment, and more. It is also the Government's plan to improve and expand training and other activities for teachers to improve their ICTs-based teaching capabilities.

(3) Identifying, Fostering, and Recruiting World-class Exceptional Talent

With regard to cybersecurity-related human resources, the Government will continue to make efforts to discover exceptionally talented individuals, in addition to promote cybersecurity education offered by educational institutions, such as graduate schools engaging in cybersecurity-specific advanced research cooperation.

It is also aimed to promote the development of self-help cybersecurity capabilities to examine appropriate incident responses, through research on various methods of counteractions against cyber attacks, including defensive and offensive methods.

Moreover, given the fact that cybersecurity has become a global challenge, the exceptionally talented domestic human resources are expected to become globally competent; in other words, it needs to nurture individuals who are capable of working across the national borders. For this reason, the Government will actively launch various initiatives, such as more supports for organizing contest events by inviting overseas participants, and building networks among talented individuals. With such initiatives, talented domestic individuals will become more motivated by knowing their levels of cybersecurity skills compared with the global standards, while staying in Japan.

(4) Building Long Term Career Paths for Cyber Experts

A majority of organizations are using ICTs as a tool to achieve their business objectives. This means that organizations using ICTs are required to address cybersecurity as their business management issue. At these organizations, all business levels, from the operational level to the board level, need to be equipped by human capacity with cybersecurity expertise to ensure cybersecurity readiness, based on the different needs at each business level. As for cybersecurity-related industries, their human resources challenge is to employ not only cybersecurity-specific personnel but also those who perform supervisory duties for them. Moreover, to clarify career paths corresponding with the organizational needs will be beneficial for enterprise senior executives, educated cybersecurity personnel, and human resources developers.

In this regard, the Government will aim at creating a virtuous circle of supply and demand of human resources through appropriate measures: the visualization of competency, by developing qualification schemes to evaluate cybersecurity-related personnel's practical skills timely and appropriately and by establishing the standards of basic skills required to perform assigned functions at organizations; the promotion of activities for better matching of occupational supply and demand, including the expansion of internship opportunities, with consideration of the nature of businesses concerned and host organizations' needs; the development of career paths for cybersecurity human resources across industries, academia, and the public sector; the promotion of other relevant measures in various perspectives, including business finance, and so on.

(5) Strategizing Human Resources Development for Enhanced Organizational Capacities

There are rapidly increasing and aggravating cyber attacks that target whole organizations, including governmental bodies and CII operators. To tackle cyber attacks in an accurate and timely manner, it is not enough to make the efforts of individuals to enhance their cyber defense capabilities; what is important is aligning these individual efforts in an organic fashion for building enhanced organizational capacity. For the overall organizational improvement of cybersecurity capabilities in effective and efficient way, it is crucial to create competitive environments where different organizations could learn from each other, while helping individual organizations grasp their current levels of practical skills as well as challenges specifically.

For this reason, the Government will work to systematize organizational capabilities necessary to counter cyber attacks, and make practical exercise activities more comprehensive to improve such organizational capabilities. The enhancement of the public-private collaboration frameworks will be also undertaken by the Government for the purposes of collective damage control and recurrence prevention or reduction in the event of serious cyber attacks or other cybersecurity incidents.

6. Promotion and Implementation of Cybersecurity Strategy

The Cybersecurity Strategic Headquarters performs the command and control body functions to promote this strategy, and, as its secretariat, the NISC takes a leading role to implement cybersecurity policies in line with this strategy. To this end, the NISC fulfills its functions: to implement required measures, including the network-based cybersecurity vigilance and monitoring of malicious activities against information systems of administrative organs, audit, and fact-finding activities; and to enhance governmental cybersecurity capabilities, in terms of information gathering and analysis on domestic and foreign cybersecurity, international cooperation, cybersecurity workforce development for and by the governmental bodies, and others. To fully perform its responsibilities, the NISC will take necessary measures, including: further enhancing its response capabilities by appointing highly advanced cybersecurity experts from the private sector and other means; and building frameworks for rapid information sharing with relevant governmental bodies (including those of senior executives) so that the NISC can obtain necessary information quickly in the case of a cybersecurity incident and the Government as a whole can take appropriate actions.

The governmental bodies have the responsibilities to implement cybersecurity measures, in close coordination with the NISC, necessary for the fulfillments of their functions, and to share information with and provide essential advice for organizations and business operators under their jurisdictions. Especially, to boost national cybersecurity capabilities as a whole, the enhanced coordination will be intended among parties concerned, including active information sharing among industries, academia, and the public sector, in addition to relevant governmental bodies. In particular, to become capable of taking necessary measures in the case of a cybersecurity incident, while controlling the situation in a steady and calm manner, it is essential to work on the routine basis to enhance the governmental structures for incident readiness, i.e. detecting, analyzing, and responding to cyber attacks and other cybersecurity incidents. In this sense, the Government will implement the government-wide measures to strengthen its information gathering and analysis functions, e.g. coordination with the private sector and cyber counterintelligence activities, for the purposes of: expanding daily information gathering activities; and foreseeing and detecting cyber threats promptly. The Government will also build the organizational structures with advanced capabilities for information gathering, analysis, and sharing to perform an integrated cycle of detection, analysis, decision making, and response regarding cyber attacks.

With regard to its crisis management function, with the aim of its further enhancement, the Government will review its ways of taking initial responses to cyber attacks and other cybersecurity incidents and confirming the status of measures taken against them, such as the recommendation(s) made by the Chief of the Cybersecurity Strategic Headquarters. At the same time, the Government will build an organizational framework that enables the governmental bodies, independent administrative agencies, cybersecurity business operators, and other relevant stakeholders to respond jointly to cyber incidents, such as massive cyber attacks; the Government will also make proactive efforts for coordination with relevant parties having specific expertise, in terms of incident responses to massive cyber attacks, practical training and exercises for human resources development and others, in coordination among industries, academia, and the public sector. These efforts include measures to: utilize the knowledge and experiences of relevant entities, such as Information-Technology Promotion Agency (IPA), for monitoring, audit, fact-finding activities, and other functions performed by the Government; and utilize the technical knowledge and skills of relevant entities, such as the National Institute of Information and Communications Technology (NICT), regarding infrastructure for simulation exercises as well as monitoring and analysis for strengthening cybersecurity-related response capabilities. To achieve these purposes, the Government will take necessary measures, including legislative measures.

In recent years, there is an increase in highly advanced and well-planned cyber attacks that might be suspected as state-sponsored. Countering such cyber attacks is one of the most critical challenges for Japan's crisis management and national security. The Cybersecurity Strategic Headquarters will collaborate and share information with the crisis management organs, including the serious terrorism response headquarters, where necessary, and take appropriate actions concerning national security, in close coordination with the National Security Council.

Moreover, it is an upmost necessity for Japan to work towards ensuring cybersecurity for the major international events, including the Tokyo 2020 Olympic and Paralympic Games, to the maximum extent feasible. Especially with regard to the Tokyo Olympic and Paralympic Games, based on a clear understanding of cybersecurity risks and challenges related to the Tokyo 2020 Olympic and Paralympic Games, the Government will accelerate the formulation process of the Tokyo 2020 Olympic and Paralympic CSIRT as a core organ responsible for: the accurate prevention and detection of cyber attacks against relevant entities involving the management and operation of the Olympic and Paralympic Games and other associated businesses as well as those against the services provided by relevant CII; and the sharing of information absolutely necessary for these

stakeholders to take appropriate measures. The Government will take steady actions step by step to: build and maintain necessary organizations, facilities, and cooperative relationships; assure a pool of cybersecurity experts; and conduct comprehensive preparatory training based on the process taken for and during the 42nd G7 Summit in the Ise-Shima region in 2016 as well as the Rugby World Cup held in Japan in 2019. Capabilities developed through these measures will be utilized later for the sustainable enhancement of Japan's cybersecurity.

These cybersecurity policies are highly critical from the viewpoint of crisis management and national security. To promote them more firmly, the Government will start feasible measures promptly and, where necessary, take actions, without delay, to establish new procedures required for the implementation of certain measures. Such measures include: securing and executing the budget appropriate for the Government as a whole by certain ways, e.g. the reallocation of the budget and other resources to additional necessary expenses and others, with cost-saving efforts, such as streamlining and increasing efficiency in administrative affairs by the review of administrative works, system reforms, and the reexamination of other activities; and appointing highly talented individuals as in-house cybersecurity experts at the governmental bodies, by assuring employment conditions that would suit the professional values of their expertise.

7. Plan Process and Review

Based on the current state of the nation as well as the future scenarios for Japan's society in the early 2020s, this strategy extracts critical issues that Japan has faced, and outlines the basic strategic directions over the coming three years, for the resolution of these issues. For the steady implementation of the strategy, in compliance with the Basic Act on Cybersecurity, the Cybersecurity Strategic Headquarters will establish an annual plan for each fiscal year during the triennium, and will produce an annual report for the corresponding year, by reviewing the status of progress in policy implementation.

At the same time, the Cybersecurity Strategic Headquarters will establish the guidelines and basic policy of budget plans for the governmental bodies to implement cybersecurity measures effectively in line with the directions the strategy indicates. Bearing in mind that the situations and technical premises in cyberspace are frequently evolving in an incoherent fashion, the Government will undertake a functional review flexibly, where necessary, regardless of the timeframe the three year plan covers.