Summary of the Japan's Cybersecurity Strategy (July 27, 2018 Cabinet Decision)

Medium and Long-Term

1. Introduction

1-1. A Paradigm Shift Brought About by Cyberspace (In cyberspace, people can leverage creation and innovation to significantly expand their activities. A paradigm shift to "Society 5.0" where no human have experienced before.)

1-2. Changes Since 2015 (Increasing seriousness of threats with cyberspace and real space unification, necessity of new strategy far-seeing the Games of the XXXII Olympiad and the Tokyo 2020 Paralympic Games.)

2. Understanding on Cyberspace

2.1. Benefits of Cyberspace

- Knowledge, technologies and services in cyberspace, such as Artificial Intelligence (AI) and Internet of Things (IoT) are becoming established in society, and leading innovations that are transforming the existing structures. They are gaining routine use in numerous domains and bring about abundance for humanity.

2.2. Increasing Threats in Cyberspace

- There is always the latent risk that the providers of these technologies will lose the ability to control them. Attacks directed at IoT, critical infrastructure, supply chains, as well as incidents suspected to have been state-sponsored will increase socio-economic losses exponentially.

3. Visions and Objectives of this Strategy

3.1. Adherence to the Basic Position on Cybersecurity

(1) Objectives of the Basic Act on Cybersecurity; (2) Basic Ideals ("free, fair and secure cyberspace"); (3) Basic Principles (assurance of the free flow of information, the rule of law, openness, autonomy, and collaboration among multi-stakeholders)

3.2. Basic Vision of Cybersecurity as a Goal

(1) Goal (Cybersecurity for sustainable development (Promotion of "Cybersecurity Ecosystem")), (2) Three Approaches (1. Mission Assurance for Service Providers; 2. Risk Management; 3. Participation, Cooperation, and Collaboration)

During the Strategy Period (2018~2021 3years)

4. Policy Approaches towards Achieving the Objective

Enabling Socio-Economic Vitality and Sustainable Development

1. Advancing Cybersecurity as Value Creation Driver

<Examples>

- Raising executive awareness (from "cost" to "investment")
- Incentives for cybersecurity investment (Market evaluation by information disseminated and disclosed by companies, use of insurance in cybersecurity)
- Enhancing cyber security business based on security-by-design

2. Achieving a Supply Chain that Creates Values through Diverse Connections

<Examples>

- Formulating Cybersecurity Framework for supply chain risk of business operators including small and medium-sized enterprises. (supply network of devices, data and services)

3. Building Secure IoT Systems

<Examples>

- Improving structural framework for IoT systems and international standard
- Establishment and international delivery of model for addressing vulnerabilities of IoT devices

Building a Safe and Secure Society for the People

1. Measures for the Protection of People and Society

<Examples>

- Implementation of active preventive measures against threats (proactive cyber defense)
- Enhancing measures against cybercrimes

2. Protection of Critical Infrastructure through Public and Private Sector Cooperation

<Examples>

- Improvement and promotion of safety principles (positioning of cybersecurity measures as safety regulations within related laws and regulations)
- Strengthening and enhancing security in local governments

3. Strengthening and Improving Security in Governmental Bodies and Government-Related Entities

<Examples>

- Managing the state of information systems in real-time
- Preemptive efforts leveraging cutting edge technology

4. Ensuring a Safe and Secure Educational and Research Environment at Universities etc.

<Examples> - Promoting measures in the light of the diversity of universities and research institutes

5. Initiatives for the Tokyo 2020 Games and Beyond

<Examples>

- Promoting the development of the Cyber Security Incident Response Coordination Center
- Leveraging the results as legacy

6. Building an Information Sharing/Collaboration Framework that Extends beyond Traditional Frameworks

<Examples>

- Promoting information sharing/collaboration between multi-stakeholders

7. Strengthening the Incident Readiness Against Massive Cyberattacks

<Examples>

- Strengthening the incident readiness against massive cyberattacks in order to work on risk management for both cyberspace and real space

Contribution to the Peace and Stability of the International Community and Japan's National Security

1. Commitment to a Free, Fair, and Secure Cyberspace

<Examples>

- Communicating the idea of a free, fair and secure cyberspace
- Promoting the rule of law in cyberspace

2. Strengthening Capabilities for Defense, Deterrence, and Situational Awareness

<Examples>

- Ensuring national resilience ((1) Mission assurance;(2) Protection of Japan's advanced technologies and defense related technologies;(3) Measures against the malicious use of cyberspace by terrorist organizations)
- Enhancing deterrence capabilities ((1) Measures for effective deterrence; (2) Confidence building measures)
- Strengthening cyber situational awareness ((1) Increasing the capabilities of relevant governmental bodies; (2) Threat information sharing)

3. International Cooperation and Collaboration

<Examples>

- Sharing expertise and coordination policy
- International collaboration for incident response
- Cooperating for capacity building

Cross-cutting Approaches to Cybersecurity

Development and Assurance of Cybersecurity Human Resource	<Examples> Training and adoption at the strategic management level, Training for the operational and expert level (including advanced human resources), Preparing a foundation for development of cybersecurity human resource, Strengthening the assurance and development of cybersecurity human resource at Agencies, Promoting international partnership
Advancement of Research and Development	<Examples> Promoting practical R&D (Improving the capability of detection and defense against attacks and developing a system for carrying out the necessary technical inspections), Responses with a view to the mid- and long-term evolution of technology and society including AI
Cooperation by Everyone who is the Main Player in Cybersecurity	<Examples> Developing action plan for public awareness on cybersecurity, Disseminating necessary information toward the people (enhancing Cybersecurity Awareness Month), Promote of cybersecurity education

5. Promotion and Implementation of Cybersecurity

Towards the realization of this Strategy, under the Cybersecurity Strategy Headquarters, the related government bodies will keep working on improving their cybersecurity capabilities under the leadership of National center of Incident readiness and Strategy for Cyersecurity(NISC), and NISC will play its leading role as the focal point in coordinating intra-government collaboration and promoting partnerships between industry, academia, and the public and private sectors. The Headquarter will seek to secure and execute the budget necessary for the government so that the measures executed.