Note: This document is a tentative translation of "The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies" for purpose of reference and its accuracy is not guaranteed. Any entity does not accept responsibility for any disadvantage derived from the information described in the document.

The Guidance on Operations of Information Security Measures of Government Agencies and Related Agencies

August 31, 2016
The Cybersecurity Strategic Headquarters

1. Objective of this Guidance

This guidance stipulates for government agencies necessary matters for formulation and its operation of government agency's own standards based on the Common Model for Information Security Measures of Government Agencies (decided by the Cybersecurity Strategic Headquarters on 31st August in 2016. hereinafter referred to as the "the Common Model") and the Common Standards for Information Security Measures for Government Agencies (decided by the Cybersecurity Strategic Headquarters on 31st August in 2016. hereinafter referred to as "the Common Standards") and necessary matters for information security management of Incorporated Administrative Agencies and Designated Corporations (stipulated by article 13 of the Basic Act on Cybersecurity (Act No. 104 in 2014. hereinafter referred to as "the Act"); hereinafter, the same shall apply).

2. Formulation of the Common Standards Group

The Common Standards Group is the collective term of the Common Model, the Common Standards, this Guidance and the Guidelines for Establishing Government Agency's Standards for Information Security Measures (the National Center of Incident readiness and Strategy for Cybersecurity, the Cabinet Secretariat, on August 31, 2016, hereinafter referred to as "the Guideline for Establishing Standards"). The draft plan of the Common Model, the Common Standards and this Guidance is formulated by the National center of Incident readiness and Strategy for Cybersecurity (hereinafter referred to as "NISC"), the Cabinet Secretariat and decided by the Cybersecurity Strategic Headquarters (Hereinafter referred to as "Strategic HQ") after deliberating at the CISO Council (decided by the Chief of the Cybersecurity Strategic HQ on 10th February, 2015). The Guideline for Establishing

Standards is decided by the NISC after consulting with government agencies.

The NISC establishes the draft by paying attention to the following points considering the result brought by regular assessments and new threat occurrence and operations of government agencies.

(1) The Common Model and the Common Standards contain information security measures commonly necessary for all government agencies. The Common Model and the Common Standards are formulated by considering the consistency with the international standards as well as the actual situation of their role and responsibility, implementation organization and contents of measures so that government agencies are able to comply.

(2) The Guideline for Establishing Standards is to be established for the purpose of illustrating the basic measures to be taken and explaining the ideas in order to satisfy the compliance matters of the Common Standards.

3. Information Security Management of Government Agencies

(1) Introduction and plan

① Formulation of the government agency's basic policy

Government agency decides each basic policy that presents basic ideas about information security including the purpose and the target scope.

It is important to clarify the targeted information, information system, organization, employees, place, district area and its boundary to formulate the government agency's basic policy including an outsourcing viewpoint and to make sure that the boundary is adequate by confirming that the measures for information security are taken by other institutions for those matters other than the target scope.

Since the government agency's basic policy is to decide the fundamental direction of information security, it must be noted that the policy should not be frequently updated.

② Formulation of the government agency's own standards

Government agency establishes the government agency's own standards based on the basic policy of government agencies in compliance with the Common Model and the Common Standards. The government agency's own standard are to be established by referring to the Guideline for Establishing Standards to comply with the Common Standards and by considering characteristics of the organizations, handling information and so forth. When information security measures are individually fixed in common across the government agencies to immediately respond to changes of threat, those are to be reflected.

③ Formulation of promotion plan of measures

Government agency establishes a plan (hereinafter referred to as “promotion plan of measures”) to comprehensively promote information security based on risk evaluation result on information security under direction of person responsible for top information security. The promotion plan of measures can present an overhead view of a series of efforts relating to the information security of government agency including educational training and technical measures for information systems.

(2) Operations

Government agency implements efforts relating to information security based on the promotion plan of measures by providing educational training for the employees for penetrating the government agency’s basic policy and the its own standards (hereinafter referred to as “government agency’s policy”) and by strengthening technical measures for information system.

(3) Assessment and Review

Government agency confirms and assesses the annual implementation situation of efforts according to the promotion plan of measures as well as reviews and improves it as necessary. Government agency needs to assess the situation of information security measures implementation, effect and information security condition to secure the adequateness of information security.

Because it is important to recognize that the assessment is conducted from an objective viewpoint, it needs to include the audit made by the party or section which is independent from the assessment targeted organizations or persons belonging to the organizations.

When it is judged that the required information security level is not achieved or that insufficient implementation situation or effect are found for information security as a result of the assessment, improvement needs to be made in consideration with recurrence prevention. Improvement actions are required including amendment of the government agency’s standards, dissemination of the government agency’s standards through education, renewal of information system and devices and enlightenment of information security significance. It needs to be confirmed that the intended objectives are achieved by the result of improvement actions.

Chief information security officer comprehensively evaluates the situation of information security management of own government agencies in light of the promotion plan of measures and reviews direction and resource allocation to the information security management in future to/ further propel the efforts on information security.

Government agency reviews and improves information security measures for matters advised by Strategic HQ audit (the audit based on item (2) of paragraph 1 of article 25 of the Act. The same shall apply hereinafter) by following (1) to (3) processes mentioned above as required by considering the priority order.

4. Information Security Management of Incorporated Administrative Agencies and Designated Corporations

(1) Introduction and plan

The Common Standards Group means cybersecurity related policy standards for incorporated administrative agencies, etc. which is established based on item (2) of paragraph 1 of article 25 of the Act. An agency of Incorporated Administrative Agencies and Designated Corporations establishes policy standards (hereinafter referred to as "policy of Incorporated Administrative Agencies and Designated Corporations") based on implementation and plan of information security management of competent government agencies shown in 3(1).

Competent minister in charge of Incorporated Administrative Agencies describes an aim of taking information security measures based on policy of Incorporated Administrative Agencies in mid-term objective of the item indicated by the rule of paragraph 1 of article 29 of Act on General Rules for Incorporated Administrative Agencies (Act No. 103 in 1999), in mid and long-term objectives of the item indicated by the rule of item (1) of paragraph 4 of article 35 or in annual objective of the item indicated by the item (1) of paragraph 9 of article 35. Competent government agency makes necessary recommendations on information security measures for Designated Corporations under individual basis laws.

(2) Operations

An agency of Incorporated Administrative Agencies and Designated Corporations carries out the efforts on information security by spreading over the policy of Incorporated Administrative Agencies and Designated Corporations in accordance with the operations of information security management of the competent government agency shown in 3. (2).

An agency of Incorporated Administrative Agencies and Designated Corporations constructs information contact system to the competent government agency in order to swiftly and effectively utilize information on information security incident from a viewpoint of expansion prevention of damage. Since management judgement may be required to address the information security incident, information on information security incident and its handling situation are informed among people in managerial positions of the competent government agency and executive class of the subject corporations as well as practical classes by the information contact system. The competent government agency works for interactive and smooth information contact, for example, providing information to the NISC when information security incidents occur, receiving security alerts by the NISC and so on, through an information sharing system.

(3) Assessment and Review

An agency of Incorporated Administrative Agencies and Designated Corporations recognizes and assess the implementation situation in each fiscal year according to the assessment and review of information security management of the competent government agency shown in 3. (3), and then review and improve as necessary.

The Competent minister in charge of Incorporated Administrative Agencies evaluates the implementation status of information security measures and publishes the evaluation result when operations' actual performance is assessed based on Act on General Rule of Incorporated Administrative Agencies. The competent Government agency also evaluate the implementation status of information security measures toward the Designated Corporations with jurisdiction under the individual basis laws. The NISC also confirms the evaluation result and advises to the competent government agency as necessary.

An agency of Incorporated Administrative Agencies and Designated Corporations reviews and improves information security measures for matters advised by Strategic HQ audit by following (1) to (3) processes mentioned above as required by considering the priority order.

5. Improvement of Information Security Measures

(1) Assessment of Information Security Measures to Government Agencies

Because information security measures require not temporary but continuous efforts, it is important to conduct the assessment based on judgement standards possible to objectively compare and verify.

While government agencies are responsible for assessment of the implementation status of information security measures in principle, government agencies as a whole carry it out more effectively and efficiently. Therefore, the Strategic HQ and the NISC conduct the assessment and Strategic HQ audits regularly or as required for situation of preparation of information security related rules that are stipulated by government agencies on the basis of the Common Standards Group, the implementation status of measures and of information security management of government agencies from comprehensive, objective and united points of view.

(2) Audit of Information Security Measures of Incorporated Administrative Agencies and Designated Corporations

Incorporated Administrative Agencies and Designated Corporations accept Strategic HQ audit and report the audit result to the competent government agencies.

(3) Verification and Publication of Audit Result

Strategic Headquarters confirms issues with regard to implementation of information security measures by audit result of (1) and (2), consolidates direction of the overall efforts of government agencies, Incorporated Administrative Agencies and Designated Corporations (hereinafter referred to as "government agencies and related agencies") in aligning with it and publishes the outline.

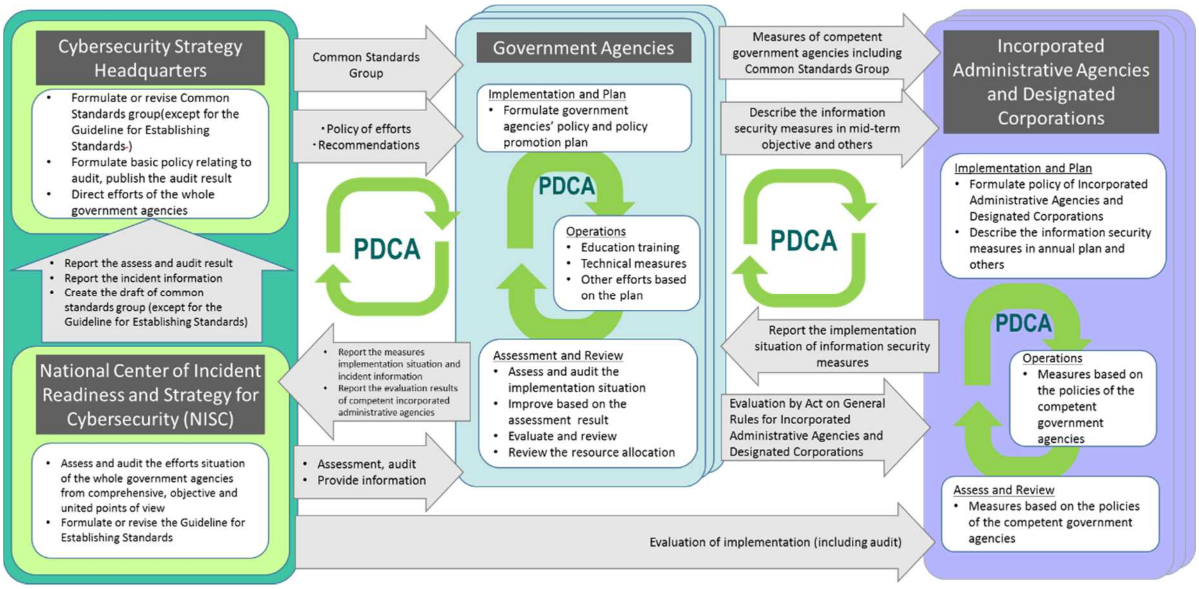
Cybersecurity Strategy Headquarters
• Formulate or revise Common Standards group(except for the Guideline for Establishing Standards)
• Formulate basic policy relating to audit, publish the audit result
• Direct efforts of the whole government agencies
• Report the assess and audit result
• Report the incident information
• Create the draft of common standards group (except for the Guideline for Establishing Standards)
National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
• Assess and audit the efforts situation of the whole government agencies from comprehensive, objective and united points of view
• Formulate or revise the Guideline for Establishing Standards
Common Standards Group
・Policy of efforts
・Recommendations
PDCA
• Report the measures implementation situation and incident information
• Report the evaluation results of competent incorporated administrative agencies
• Assessment, audit
• Provide information
Government Agencies
Implementation and Plan
• Formulate government agencies' policy and policy promotion plan
PDCA
Operations
• Education training
• Technical measures
• Other efforts based on the plan
Assessment and Review
• Assess and audit the implementation situation
• Improve based on the assessment result
• Evaluate and review
• Review the resource allocation
Measures of competent government agencies including Common Standards Group
Describe the information security measures in mid-term objective and others
PDCA
Report the implementation situation of information security measures
Evaluation by Act on General Rules for Incorporated Administrative Agencies and Designated Corporations
Evaluation of implementation (including audit)
Incorporated Administrative Agencies and Designated Corporations
Implementation and Plan
• Formulate policy of Incorporated Administrative Agencies and Designated Corporations
• Describe the information security measures in annual plan and others
PDCA
Operations
• Measures based on the policies of the competent government agencies
Assess and Review
• Measures based on the policies of the competent government agencies

Figure. Overall picture of information security management of government agencies and related agencies

6. How to Proceed Information Security Measures

(1) Establishment of Basic Principles, Direction of Chief Information Security Officer and Promotion Systems

To ensure the information security of each government agency or related agency, it is the principle to take one's own responsibility to manage the information to be handled and implement the information security measures suitable to each operation and information system configuration in tandem with request and expectation concerned to ensuring information security by people and businesses.

To achieve this, Chief Information Security Officer leads promotion of information security measures of each organization, clarifies the direction and decides direction of resource allocation of work force and budget necessary to the information security measures.

Since it is necessary to consider the characteristics of handled information, operations and organizations to propel the information security measures efficiently and practically, organization and system are established to promote information security measures to undertake cross-functionally across the organization sections.

Given that government agencies deal with a number of important information including subtle personal information through their operations, it is vital to make employees recognize that people expect them to manage it in right way, regularly share such recognition with Incorporated Administrative Agencies and Designated Corporations under jurisdiction and exercise supervision etc.

(2) Implementation of Information Security Measures

Government agencies and related agencies ensure a certain security level by properly operating formulated government agencies' policy or policy of Incorporated Administrative Agencies and Designated Corporations. Information security measures are taken by recognizing risks in detail for significant operation and information.

It is essential to implement the information security measures by enhancing efficiency and the effect of operations taking operation requirement and operation flow into consideration in order not to cause any conduct of circumventing the rule by implementing the security measures excessively.

Government agencies and related agencies are required to recognize risks and implement the information security measures in compliance with any guidelines applied to government agencies and related agencies if they are available.

(3) Information Security Measures of Information Systems Shared by Multiple Agencies

Information system shared by multiple agencies (excluding such information systems whose entire operations including hardware and software are controlled and managed by a single agency. Hereinafter referred to as "common platform systems") is operated and managed in cooperation with information systems of each organization. Thus, prevention of careless mistakes needs to be attempted for the information security measures across each organization. Considering the possibility that information security incidents of partial information system linked to common platform system impacts on other information systems, information security management should be implemented decently and information security levels should be ensured properly as an overall information system.

Consequently, organization to prepare and manage the operation of common platform systems and organization to manage information systems linked to the common platform system (hereinafter referred to as “preparation and operation management organizations”) need to clarify role and responsibility of each organization for preparation of the system to manage operation of the infrastructure information system and to establish the system to be able to adjust and implement the information security measures surely and immediately.

The preparation and operation management organizations consider relevance of each government agency’s policy or policy of Incorporated Administrative Agencies and Designated Corporations to establish the document that stipulates comprehensively measures to ensure information security of the common platform systems and sort out the following matters in order to have adequate operations and management.

- Responsibility demarcation of each organization
- Cooperation and collaboration system for ordinary and emergency conditions
- Concrete measures for emergency condition

Full consensus needs to be made across each organization and attention needs to be paid in order not to hinder smooth and prompt implementation of information security measures in considering and implementing the points mentioned above.

Organization that prepares and manages operation of common platform system can establish common rules for information security of common platform system by consulting with organization that manages information system linked to the subject common platform systems regardless of provisions of government agencies’ policy or policy of Incorporated Administrative Agencies and Designated Corporations that are defined by each organization in order to commonly take information security actions of common platform system.

(4) Information Sharing of Information Security Incidents

It is vital to share in suitable time and decently information on information security incidents with concerned sections inside and outside the organizations in order to address promptly and precisely information security incidents by the whole government agencies and related agencies.

Hence, government agencies swiftly contact the NISC about information pertaining to the information security incidents when information security incidents are recognized by the government agencies or the Incorporated Administrative Agencies and Designated Corporations under jurisdiction, and also government agencies communicate with the NISC for information of collected information security incidents at ordinary times.

Incorporated Administrative Agencies and Designated Corporations share information closely among the competent government agencies about information security incidents.

The NISC becomes a nodal point to share information with government agencies and relevant external organizations at ordinary times and actively provides information to government agencies with consensus of the information source so as to utilize collected and consolidated information for prevention of damage or prevention of damage expansion caused by information security incidents and for emergent actions, recovery measures and recurrence prevention.

(5) Handling of Information Security Incidents

When an information security incident is recognized, the government agency identifies immediately the situation and take actions for prevention of damage expansion and for emergent measures and recovery with initiative of the CSIRT (Computer Security Incident Response Team) that is set by them.

Incorporated Administrative Agencies and Designated Corporations also address the information security incidents as well as the government agencies when information security incidents are recognized.

The NISC collaborates and adjusts across government agencies as a key organization of united government to tackle information security incidents. Also the NISC technically supports and advises to government agencies including assistance of improving the CSIRT ability, and provides support by the Cyber Incident Mobile Assistance Team (CYMAT) as required by government agencies.

Supplementary provisions

The Guidance on establishment and operation of the Common Standards for Information Security Measures for Government Agencies (decided by the Information Security Policy Council on September 15, 2005) is abolished.