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
Revised July 25, 2018
The Cybersecurity Strategic Headquarters

1. Objective of this Guidance

This guidance stipulates necessary matters for the following actions in relation to the application of standards related to cybersecurity at the national administrative organs stipulated in Item 2, Paragraph 1, Article 25 of the Basic Act on Cybersecurity (Act No. 104 of 2014; hereinafter referred to as "the Act"), as well as Incorporated Administrative Agencies (referring to corporations regulated in Paragraph 1, Article 2 of the General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999); hereinafter, the same shall apply) and Designated Corporations (referring to designated corporations regulated in Article 13 of the Act; hereinafter, the same shall apply) (hereinafter referred to as the "Agencies"): formulation of draft versions of the Common Model of Information Security Measures for Government Agencies and Related Agencies (decided by the Cybersecurity Strategic Headquarters; hereinafter referred to as the "the Common Model") and the Common Standards for Information Security Measures for Government Agencies and Related Agencies (decided by the Cybersecurity Strategic Headquarters; hereinafter referred to as "the Common Standards") by the National center of Incident readiness and Strategy for Cybersecurity (hereinafter referred to as the "NISC"); formulation of the Guidelines for Establishing Agencies' Standards for Information Security Measures (decided by the NISC; hereinafter referred to as the "Guidelines for Establishing Standards"); application of information security measures at Incorporated Administrative Agencies and Designated Corporations, and the application of information security measures for the information systems commonly used among the multiple Agencies (excluding information systems where everything from the hardware to applications are managed and operated by a single agency or entity; hereinafter referred to as "common platform systems").

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 Standards. The draft plans of the Common Model, the Common Standards, and this Guidance were formulated by the NISC and were decided by the Cybersecurity Strategic Headquarters after deliberating at the Cybersecurity Measures Promotion Committee (decided by the Chief of the Cybersecurity Strategic on February 10, 2015). The Guideline for Establishing Standards were decided by the NISC after consulting with national administrative organs.

The NISC establishes the draft by paying attention to the following points considering the occurrence of new threats and the result brought by regular inspection of the application status at Agencies.

(1) The Common Model and the Common Standards contain information security measures commonly necessary for all 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 Agencies are able to comply. The Common Standards regulate matters that Agencies must observe for each item of the information security measures (hereinafter referred to as "requirements").

(2) The Guideline for Establishing Standards is to be established for the purpose of illustrating the basic measures to be taken to satisfy the requirements of the Common Standards (hereinafter referred to as "basic measures") and explaining the ideas for the formulation and implementation of measures by Agencies. The basic measures are designed to observe the requirements. As such, Agencies must satisfy the corresponding requirements by referring to the Guideline for Establishing Standards and take the measures enumerated in the basic measures or measures that are equal to or greater than these.

3. Duties of the Competent Ministers and Others Regarding the Information Security Measures of Incorporated Administrative Agencies and Designated Corporations

(1) Introduction and plan

The competent minister in charge of Incorporated Administrative Agencies includes an aim of taking information security measures in mid-term objective of the item indicated by the

rule of Paragraph 1, Article 29 of the Act on General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999), mid and long-term objectives of the item indicated by the rule of item (1), Paragraph 4 of Article 35, or in annual objective of the item indicated by the item (1), Paragraph 9 of Article 35, according to policies established based on the Common Standards Group. The national administrative organ overseeing Designated Corporations makes the necessary recommendations on information security measures for the designated corporations in question based on the individual governing laws.

(2) Evaluation

The competent minister in charge of Incorporated Administrative Agencies also evaluates the implementation status of information security measures and publishes the evaluation result when operations' actual performance is assessed based on the Act on General Rule of Incorporated Administrative Agencies. The national administrative organ in charge of Designated Corporations evaluates the implementation status of information security measures for the designated corporations in question based on the individual governing laws.

The NISC also confirms the evaluation results regarding the information security measures of Incorporated Administrative Agencies and Designated Corporations and advises the national administrative organs holding jurisdiction over these corporations as necessary.

4. Information Security Measures of Information Systems Shared by Multiple Agencies

Common platform systems are operated and managed in cooperation with the information systems at each organization using the platform systems. Thus, careless mistakes need to be prevented 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 for the overall information system should be ensured properly.

Consequently, organizations that conduct development and operation management of common platform systems to serve as a foundation and organizations that manage information systems linked to the common platform system (hereinafter referred to as "development and operation management organizations") need to clarify roles and responsibilities of each organization for preparation of the system to conduct operation management of the infrastructure information system to serve as a foundation and to establish the system to be

able to adjust and implement the information security measures reliably and promptly.

The development and operation management organizations consider the relevance of the respective policies 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 ensure adequate operations and management.

- Responsibility demarcation across each organization
- Cooperation and collaboration system for ordinary and emergency conditions
- Concrete measures for emergency condition, etc.

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.

Agencies, which conduct development and operation management of common platform systems, can establish common rules for information security for the common platform systems by consulting with Agencies that manage information systems linked to the said common platform systems, regardless of provisions of policies defined by each organization, in order to commonly implement information security measures for common platform systems.

Supplementary provisions

The Guidelines for Formulation and Implementation of Standards for Information Security Measures for the Central Government Computer Systems (decided by the Information Security Policy Council on September 15, 2005) is abolished.