Content

Title：	Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency Ch
Date：	2021.08.23
Legislative：	1. Promulgated on Novenber 21, 2018 2. Amendment promulgated on 23 August 2021
Content：	Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 7 of the Cyber Security Management Act. Article 2 These Regulations stipulate “in writing” document may be an electronic document in accordance with the provisions of the Electronic Signatures Act. Article 3 Except for cause by force majeure, the competent authority shall select and determine the specific non-government agencies (hereinafter referred to as the “audited agency”) for each quarter of the year, and may audit the implementation of their cyber security maintenance plans through onsite audit every year. In selecting and determining the audited agencies under the preceding paragraph, the competent authority shall give comprehensive consideration to the significance and confidential sensitivities of its businesses, the size and nature of their cyber systems, the frequencies and degrees of occurrence of cyber security incidents, the results of cyber offense and defense exercise, the frequencies and results of audits conducted by the competent authority or the central authority in charge of the relevant industry over past years, or other factors relating to cyber security. In conducting the audit under Paragraph 1, the competent authority shall establish the audit program, the content of which shall include the basis and purposes, time period, essential fields of the audit, the manner of formation of the audit team, confidentiality obligation, the method, standards and items of the audit, and assistance issues from the central authority in charge of relevant industry. In determining the essential fields, standards and items of the audit under the preceding paragraph, the competent authority shall take into comprehensive consideration the cyber security policy of our country, domestic and foreign cyber security trends, the contents and results of past audit programs, and any other factors relating to the proper allocation of audit resources or audit effectiveness. Article 4 In conducting the audit under Paragraph 1of the preceding article, the competent authority shall deliver the audit program notice in writing to the audited agency one month before the audit. Due to business factor or other justifiable reason, the audited agency may apply to the competent authority for adjustment of the audit date within five days of the receipt of the preceding notice in writing. The preceding application is limited to one time except for the case of force majeure. Article 5 In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the audited agency to give explanations on, to collaborate the implementation of cyber security maintenance plan, or provide relevant documents and supporting information for onsite inspection, and conduct the following issues. The audited agency and its personnel shall cooperate accordingly: 1. Pre-audit interview. 2. Onsite physical audit.

The audited agency cannot give the explanations, collaborate or provide documentation for onsite inspector under the preceding paragraph for justifiable reasons under the law, they shall submit the reasons in writing to the competent authority.
Upon receipt the preceding notice in writing, the competent authority shall verify it and then take the following actions, and may suspend all or part of the audit operations:
1. If the reasons are considered justifiable, it shall record the accordance and relevant information in the audit report.
2. If the reasons are considered groundless, it shall require the audited agency to follow the requirements of Paragraph 1; if the audit operations have been suspended, it may select other time periods to continue the audit and deliver the audit program notice in writing to the audited agency ten days before the audit.
Article 6
In conducting the audit under Paragraph 1 of Article 3, the competent authority shall form an audit team composed of three to more people respectively for each audited agency, depending on the considerations under Paragraph 2 of the same article.
Informing the audit team under the preceding paragraph, the competent authority shall, taking the needs of the audit into consideration, invite representatives of government agencies or experts and scholars who have professional knowledge of cyber security policies or have professional knowledge of technologies, managements, law affairs required for such audit to act as members of such team, of which the number of representatives of the government agency may not be less than one-fourth of all members.
The competent authority shall sign, in writing, with members of audit teams on recusal due to interest conflicts and confidentiality obligations.
If the member of audit team under Paragraph 2 has any of the following circumstances, he shall avoid himself from acting as the member of that audit team:
1. He, his spouse, his relatives within the third degree, his family member, or the trustee of the property trusts of above-mentioned persons have a property or non-property interest relationship with the audited agency or the responsible person thereof.
2. He, his spouse, his relatives within the third degree or his family member has employment, contract, appointment, agency or other similar relationship with the audited agency or the responsible person in the current or the past two years.
3. He has served in the current or past two years to be a consultant of the audited agency and his mentoring project is related to the audit program.
4. Other circumstance that may be considered that his role as a member of the audit team might affect the impartiality of the audit result.
Article 7
The competent authority shall, within one month after the completion of the audit operations on the audited agency as designated for each quarter, deliver the audit reports to the audited agencies for the quarter.
The contents of the preceding audit reports shall include the scope of the audit, flaws or items to be improved, the status and reasons for the failures of the audited agency to give explanations, collaborate or provide documentations for on-site inspections under Paragraph 2 of Article 5, and the audit results of the competent authority under Paragraph 3 of the same article, and other necessary contents relating to the audit.
Article 8
If flaws or items to be improved are found in the implementation of the cyber security maintenance plan, the audited agency shall submit improvement report in the manner specified by the competent authority within one month after the competent authority has delivered the audit report, and shall deliver the same to the central authority in charge of the relevant industry. The competent authority and the central government authority in charge of the subject industry may require the audited agency to give explanations or make adjustments when necessary.
After the improvement reports are submitted under the preceding paragraph, the audited agency shall submit the implementation status of the improvement reports in the manner and within the timeframe specified by the competent authority, and shall deliver the same to the central authority in

	charge of the relevant industry. The competent authority may require the audited agency to give explanations or make adjustments when necessary. Article 9 In conducting the audit under Paragraph 1 of Article 3, the competent authority may require the central authority in charge of the relevant industry with the audited agency to dispatch personnel for necessary assistance. Article 10 The date for enforcement of these Regulations shall be decided by the competent authority. The amendments to these Regulations shall take effect on the date of promulgation.

Data Source：Ministry of Digital Affairs Laws and Regulations Retrieving System