Content

Title：	Regulations Governing the Audit of the Implementation of Cyber Security Maintenance Plans Ch
Date：	2026.01.05
Legislative：	1.On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 10 articles in full; the date those provisions come into effect will be set by the competent authority On December 5, 2018, the Order yuan tai hu zi No. 1070217128 promulgated by the Executive Yuan effective on January 1, 2019 2.On August 23, 2021, the Executive Yuan issued Order yuan tai hu zi No. 1100182012, amending Articles 3, 6 and 10; the amendments come into effect on the date of issuance On August 24, 2022, the Executive Yuan announced yuan tai gui zi No. 1110184307 that the duties listed under the “Executive Yuan” in Article 3, Paragraphs 1, 2 of Article 4, Article 5, Paragraphs 1, 2, 3 of Article 6, Article 7, Article 8, Article 9, Paragraph 1 of Article 10 will be transferred to the “Ministry of Digital Affairs”, effective on August 27, 2022 3.On January 5, 2026, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1145000410, amending and publishing the title and full text of 14 articles, the amendments come into effect on the date of issuance (Former name: Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency; New name: Regulations Governing the Audit of the Implementation of Cyber Security Maintenance Plans)
Content：	Article 1 These Regulations are prescribed pursuant to Paragraph 4, Article 8 and Paragraph 3, Article 16 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 Government agencies shall handle their cyber security maintenance plans in accordance with Paragraph 1, Article 9 of the Enforcement Rules of the Act. Government agencies that submit reports on the implementation of their cyber security maintenance plans under Article 14 of the Act shall comply with Paragraph 2, Article 9 of the Enforcement Rules of the Act. Article 3 Government agencies shall submit reports on the implementation of their cyber security maintenance plans on the system platform designated by the competent authority. However, in special circumstances, other appropriate means may be used with the approval of the competent authority. Article 4 Government agencies that receive the implementation status of cyber security maintenance plans pursuant to Article 14 of the Act shall annually formulate an audit plan and monitor the audit status with respect to the implementation of cyber security maintenance plans by its subordinate or supervised government agencies, and the following entities under its jurisdiction: township (town, city) offices, district offices of indigenous districts in special municipalities, township (town, city) representative councils, and representative councils of indigenous districts in special municipalities. Article 5 The competent authority may annually select government agencies and specific non-government agencies to be audited, and audit the

implementation of their cyber security maintenance plans through onsite audits or other appropriate means.
Except for reasons of force majeure, government agencies shall annually select their subordinate or supervised government agencies, and the following entities under its jurisdiction: township (town, city) offices, district offices of indigenous districts in special municipalities, township (town, city) representative councils, and representative councils of indigenous districts in special municipalities, and audit the implementation of their cyber security maintenance plans through onsite audits or other appropriate means.

Article 6
In selecting audited agencies, the competent authority and government agencies (hereinafter collectively referred to as the “auditing agency”) shall take into comprehensive consideration the importance and sensitivity of their operations, the size and nature of their information and communication systems, the frequency and severity of cyber security incidents, the results of cyber security drills, the frequency and results of audits conducted in previous years by the competent authority, the government agencies that receive reports on the implementation of cyber security maintenance plans pursuant to Article 14 of the Act, the central competent authority in charge of the relevant sector, or other relevant agencies, and other factors relating to cyber security.
The annual plan prescribed in Paragraph 5, Article 8 of the Act and the audit plan prescribed in Article 4 shall include at least the following content items:
1. Audit basis.
2. Purpose of audit.
3. Scope of audit.
4. Work schedule.
5. Composition of the audit team.
6. Duty of confidentiality.
7. Principles for selecting audited agencies.
8. Audit criteria.
9. Audit methods and items.
Where the auditing agency formulates the annual plan or audit plan referred to in the preceding Paragraph, it shall take into comprehensive consideration national cyber security policy, domestic and foreign cyber security trends, the contents and results of past audit plans, and any other factors relating to the proper allocation of audit resources or audit effectiveness.

Article 7
Where the auditing agency conducts audits, it shall deliver written notice to the audited agency one month before the audit.
For operational reasons or other justifiable grounds, the audited agency may, within five days after receipt of the notice referred to in the preceding paragraph, apply in writing stating the reasons to the auditing agency referred to in the preceding paragraph to adjust the audit date.
The application referred to in the preceding paragraph may be submitted only once, except in cases of force majeure.

Article 8
When conducting audits, the auditing agency may require the audited agency to provide explanations regarding the implementation of its cyber security maintenance plan, render assistance, or provide relevant documents and supporting materials for the audit team’s review, and may carry out the following matters. The audited agency and its personnel shall cooperate accordingly:
1. Pre-audit interviews.
2. Onsite audits or other suitable audit approaches.
Where the audited agency is unable, for legally justifiable reasons, to provide explanations, render assistance, or provide materials for the audit team’s review under the preceding paragraph, it shall submit a written statement of reasons to the auditing agency referred to in the preceding paragraph, which shall review the matter upon receipt.

Where, after conducting the review referred to in the preceding paragraph, the auditing agency finds the reasons justified, it shall record the basis of the review and the relevant information in the audit report and may suspend all or part of the audit operations. Where it finds the reasons unjustified, it shall require the audited agency to proceed in accordance with Paragraph 1. Where audit operations have been suspended, the auditing agency referred to in Paragraph 1 may resume the audit at another scheduled time and deliver a written notice to the audited agency ten days before the audit.

Article 9
When conducting audits, the auditing agency shall, based on the factors set out in Paragraph 1, Article 6, form a separate audit team of three or more members for each audited agency.
When forming an audit team under the preceding paragraph, the auditing agency shall, taking audit needs into consideration, invite government agency representatives or experts and scholars possessing expertise in cyber security policy or the technical, management, legal, or practical matters required for the audit to serve as members of the team. Government agency representatives shall account for no less than one-fourth of all members.
The auditing agency shall agree in writing with members of the audit team on conflict-of-interest recusal and confidentiality obligations.
A government agency representative or expert or scholar referred to in Paragraph 2 who falls under any of the following circumstances shall voluntarily recuse themselves from serving as a member of the audit team for the audit:
1. They, their spouse, their relatives within the third degree of kinship, their family members, or the trustee of any property trust of the aforementioned persons have a pecuniary or non-pecuniary interest in the audited agency, its representative, or its responsible person.
2. They, their spouse, their relatives within the third degree of kinship, or their family members currently have, or have had within the past two years, a relationship of employment, contracting, mandate, agency, or other similar relationship with the audited agency, its representative, or its responsible person.
3. The agency, organization, or unit where they are currently employed or were employed within the past two years has served as a consultant to the audited agency, and the consulting items are related to the audited items.
4. Other circumstances sufficient to indicate that their serving as a member of the audit team will affect the impartiality of the audit results.

Article 10
The auditing agency shall, within one month after completion of the audit operations for the audited agencies designated for each quarter, deliver the audit report to the audited agencies for that quarter.
The audit report referred to in the preceding paragraph shall include the scope of the audit, deficiencies or items requiring improvement, the circumstances and reasons under Paragraph 2, Article 8 where the audited agency was unable to provide explanations, render assistance, or provide materials for the audit team's review, the review results of the auditing agency under Paragraph 3 of the same article, and other necessary matters relating to the audit.

Article 11
Where deficiencies or areas for improvement are identified in the implementation of an audited agency's cyber security maintenance plan, the audited agency shall, within one month after the auditing agency delivers the audit report, submit a corrective action report in accordance with Paragraph 1, Article 6 of the Enforcement Rules of the Act to the government agency that receives reports on the implementation of its cyber security maintenance plan pursuant to Article 14 of the Act, or to the central competent authority in charge of the relevant sector for review; the reviewing agency shall then forward the report to the competent authority. For audits conducted pursuant to Paragraph 2, Article 5, the reviewing agency shall forward the audit results together with the report

to the competent authority.
After submitting a corrective action report, the audited agency shall, in accordance with Paragraph 2, Article 6 of the Enforcement Rules of the Act, submit the implementation status of the corrective action report to the government agency that receives reports on the implementation of its cyber security maintenance plan pursuant to Article 14 of the Act or to the central competent authority in charge of the relevant sector for review; the reviewing agency shall then forward the report to the competent authority.
Where the agency receiving the corrective action report under Paragraph 1 or the agency receiving the implementation status of the corrective action report under the preceding paragraph deems it necessary, it may require the audited agency to provide explanations or make adjustments.

Article 12
When the competent authority conducts audits, it may require the agencies that receive reports on the implementation of cyber security maintenance plans as provided in Article 14, Paragraph 3 of Article 20, and Paragraph 2 of Article 21 of the Act to dispatch personnel or provide other necessary assistance.

Article 13
The competent authority may delegate the handling of the audits of the implementation of cyber security maintenance plans, the submission of corrective action reports, and other related matters prescribed in these Regulations to its subordinate agency, the Administration for Cyber Security, Ministry of Digital Affairs.

Article 14
These Regulations shall come into effect on the date of promulgation.

Files： 資通安全維護計畫實施情形稽核辦法.pdf