Content

Title：	Regulations for the Review of Products Harmful to National Cyber Security Ch
Date：	2025.12.19
Legislative：	On December 19, 2025, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1145000392 establishing and publishing the full text of 11 articles; according to Article 11, it comes into force on December 1, 2025
Content：	Article 1 These Regulations are stipulated in accordance with Paragraph 3 of Article 11 of the Cyber Security Management Act (hereinafter referred to as “the Act”). Article 2 Where a government agency or a specific non-government agency deems that an information and communication system, service, or product may constitute a Product Harmful to National Cyber Security, the agency shall complete and submit a reporting form, together with relevant supporting documents, to the competent authority for review in accordance with the following provisions: 1. The Office of the President, the National Security Council, the Five Yuans, and their directly affiliated government agencies shall submit the report directly. 2. The respective second-level central government agencies shall submit the report on behalf of their subordinate or supervised government agencies. 3. Municipal governments, municipal councils, county (city) governments, and county (city) councils shall submit the report directly. 4. Municipal or county (city) governments shall submit the report on behalf of their subordinate and supervised government agencies, township (town, city) offices and their representative councils, as well as district offices of indigenous districts in special municipalities and their representative councils, and any government agency subordinate to or supervised by any of the foregoing. 5. The central competent authority in charge of the relevant sector shall submit the report on behalf of specific non-government agencies. Article 3 When conducting the review referred to in the preceding article, the competent authority shall consider the potential impact of the use of the information and communication system, service, or product on national cyber security and shall, adopting a risk-based approach, assess the possible effects on national interests, government operations, or social stability, to determine whether it constitutes a Product Harmful to National Cyber Security. Article 4 The review procedures for Products Harmful to National Cyber Security are as follows: 1. Where the reporting form is not in the required format, the contents are incomplete, or other matters require supplementation or correction, the competent authority may notify the report-ing agency to make supplementation or correction within a specified period. Where supple-mentation or correction is impossible, is not made by the deadline, or is incomplete, the competent authority may close the case. The same applies where the same information and communication system, service, or product has already been reviewed by the competent authority and no new facts or evidence exist 2. Where the reported information and communication system, service, or

product is of a Main-land China brand, the competent authority may proceed directly to cyber security information sharing in accordance with Article 5.
3. Where the circumstances in the preceding subparagraph do not apply, the competent authority shall conduct the review based on the bill of materials (BOM) or software bill of materials (SBOM) submitted by the reporting agency.
4. The competent authority may, where necessary, seek opinions from relevant agencies, organ-izations, businesses, or experts and scholars, and may convene meetings for discussion.
5. Where the results of the reviews under the preceding two subparagraphs determine that the reported item constitutes a Product Harmful to National Cyber Security, the competent authority shall share cyber security information in accordance with Article 5.
The meeting referred to in Subparagraph 4 of the preceding paragraph shall be chaired by the head of the competent authority or their designee. The National Security Council, the National Security Bureau, the Ministry of the Interior, the Ministry of Justice, the Ministry of Economic Af-fairs, and the Mainland Affairs Council shall be invited to attend; other agencies or experts and scholars may be invited to attend the meeting for consultation where necessary.

Article 5
Cyber security information concerning Products Harmful to National Cyber Security shall be shared only with government agencies. This restriction shall not apply where special circumstanc-es exist.
Where the central competent authority in charge of the relevant sector receives such cyber security information, it shall implement the control measures prescribed in Article 27 of the Act.

Article 6
Where a government agency receives cyber security information concerning Products Harmful to National Cyber Security pursuant to Paragraph 1 of the preceding article, it shall take the follow-ing measures:
1. Conduct an inventory of its information and communication systems, services, and products, as well as information and communication equipment issued for official use, to determine whether any Products Harmful to National Cyber Security have been downloaded, installed, or used.
2. Where any Products Harmful to National Cyber Security have been downloaded, installed, or used, the government agency shall immediately remove, uninstall, or cease using them. Where such use is required for official duties and no alternative solution is available, the matter shall be handled in accordance with the proviso to Paragraph 1 of Article 11 of the Act.

Article 7
Where a government agency uses Products Harmful to National Cyber Security on a project basis pursuant to the proviso to Paragraph 1 of Article 11 of the Act, it shall implement the following measures:
1. Use shall be limited to designated areas and designated personnel, and no images or sound may be transmitted for direct viewing or listening by unspecified persons.
2. Periodically verify whether alternative solutions are available.
3. Other matters as designated by the competent authority.
Where the government agency no longer requires such use for official duties or an alternative so-lution becomes available, it shall immediately destroy the products or seal them for storage.

Article 8
Personnel participating in reviews conducted under these Regulations shall keep confidential any trade secrets or other matters that are required by law to be kept confidential and that they become aware of in the course of such participation.

Article 9
Where, prior to the enforcement of these Regulations, a government agency

	had already used Products Harmful to National Cyber Security on a project basis, it may continue such use after the enforcement of these Regulations; provided that it shall comply with Article 7. Article 10 Where, in conducting reviews under these Regulations, the competent authority identifies cyber security information that falls within the scope of the Cyber Security Information Sharing Regulations, such information shall be handled in accordance with those Regulations. Article 11 These Regulations shall come into force on December 1, 2025.
Files：	危害國家資通安全產品審查辦法英譯條文.pdf

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