資通安全管理法施行細則-英譯對照

資通安全管理法施行細則	Enforcement Rules of Cyber Security Management Act
第一條　本細則依資通安全管理法(以下簡稱本法)第二十二條規定訂定之。	Article 1 These Rules are stipulated in accordance with Article 22 of the Cyber Security Management Act (hereinafter referred to as the Act).
第二條　本法第三條第五款所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款及第二項規定之機關。	Article 2 The term "military agency" as used in Subparagraph 5 of Article 3 of the Act refers to the Ministry of National Defense and its subordinate agency (institution), troop, school; and the term "intelligence agency" as used therein, refers to the agency specified in Subparagraph 1 of Paragraph 1 and Paragraph 2 of Article 3 of the National Intelligence Services Law.
第三條　公務機關或特定非公務機關(以下簡稱各機關)依本法第七條第三項、第十三條第二項、第十六條第五項或第十七條第三項提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形： 一、缺失或待改善之項目及內容。 二、發生原因。 三、為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。 四、前款措施之預定完成時程及執行進度之追蹤方式。	Article 3 In submitting improvement reports under Paragraph 3 of Article 7, Paragraph 2 of Article 13, Paragraph 5 of Article 16 or Paragraph 3 of Article 17 of the Act, the government agency or the specific non-government agency (hereinafter referred to as "each agency") shall submit the following contents in response to the audit result of the implementation –of the cyber security maintenance plan, and shall submit the implementation of the improvement report in the manner and within the time as designated by the competent authority, superior or supervisory authority, the central authority in charge of relevant industry: 1. Flaws or items to be improved. 2. Causes of occurrence. 3. Measures in aspects of management, technology, manpower, or resource to be taken for flaws or items to be improved. 4. The estimated completion schedules of the measures under the preceding subparagraph and the tracking method on implementation progresses.
第四條　各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供(以下簡稱受託業務)，選任及監督受託者時，應注意下列事項：	Article 4 When each agency outsources parties for setup, maintenance of information and communication system, or provision of information and communication service (hereinafter referred to as the "outsourced business") in accordance with Article 9 of the Act, attention should be

一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。 二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。 三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。 四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。 五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。 六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。 七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。 八、受託者應採取之其他資通安全相關維護措施。	paid to the following matters for the selection and supervision of the outsourced party. 1. The procedures and environment of the outsourced party in conducting outsourced business shall have completed cyber security management measures or have passed the verification of third party. 2. The outsourced party shall deploy sufficient and properly qualified and trained cyber security professionals who hold cyber security professional licenses or have similar business experience. 3. Whether the outsourced party can second-tier subcontract outsourced business，scopes and objects that may be second-tier subcontract and the cyber security maintenance measures that the second-tier subcontractor should have. 4. If the outsourced business involves classified national security information, the person who conduct the outsourced business shall be reviewed and the departure shall be controlled in accordance with the Classified National Security Information Protection Act. 5. If the outsourced business includes customized development of information and communication system , the outsourced party shall provide security testing certificate of such information and communication system; if such information and communications system is the core system of the outsourcing agency, or the outsourcing amount exceeds NT$10,000,000, the outsourcing agency shall conduct itself or contract third party to conduct the security testing; if the use of system or resource other than those developed by the outsourced party is involved, content and source of those not developed by the outsourced party shall be indicated and the certification of authorization thereof shall be provided. 6. If the outsourced party conducts outsourced businesses in violation of the relevant regulatory requirement of cyber security or becomes aware of cyber security incident, it shall immediately notify the outsourcing

九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級及內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項： 一、曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。 二、曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。 三、曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。 四、其他與國家機密保護相關之具體項目 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。	agency thereof and take remedy measure therefor. 7. If the entrusting relationship is terminated or canceled, it shall be confirmed that the outsourced party has returned, handed over, deleted or destroyed all materials in its possession for the performance of the contract. 8. The outsourced party shall take other relevant measure for cyber security. 9. The outsourcing agency shall, periodically, or whenever it becomes aware of the occurrence of cyber security incident of the outsourced party that might affect the outsourced business, confirm the implementation status of the outsourced business by audit or other appropriate method. In conducting the competency audit under Subparagraph 4 of the preceding paragraph, the outsourcing agency shall take into consideration the confidential level and content of the classified national security information in which the outsourced business is involved, and shall, to the necessary extent, check whether the personnel of the outsourced party who performs such business or other personnel who might access such classified national security information has any of the following circumstances: 1. One who had committed the offense of disclosing secret, or had committed the offense of civil disturbance or treason after the termination of the Period of National Mobilization in Suppression of Communist Rebellion, and was finally convicted, or was put on a wanted list which has not been closed. 2. One who was a former public official, was subject to administrative penalty or demerit record due to a violation of relevant regulatory for security confidentiality. 3. One who was induced or coerced by foreign government, mainland China, Hong Kong or Macau government to engage in activity unfavorable to national security or significant interest of the nation. 4. Other concrete item relating to the protection of

	classified national security information. The circumstance under Subparagraph 4 of Paragraph 1 shall be stated in the tender notice, tender document and contract; before the verification of the competency audit, the relevant personnel shall agree in writing document.
第五條　前條第三項及本法第十六條第一項之書面，依電子簽章法之規定，得以電子文件為之。	Article 5 The "in writing" document under Paragraph 3 of the preceding article and Paragraph 1 of Article 16 of the Act may be the electronic one in accordance with the Electronic Signatures Act.
第六條　本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項： 一、核心業務及其重要性。 二、資通安全政策及目標。 三、資通安全推動組織。 四、專責人力及經費之配置。 五、公務機關資通安全長之配置。 六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。 七、資通安全風險評估。 八、資通安全防護及控制措施。 九、資通安全事件通報、應變及演練相關機制。 十、資通安全情資之評估及因應機制。 十一、資通系統或服務委外辦理之管理措施。 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。 各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。	Article 6　The cyber security maintenance plan under Article 10, Paragraph 2 of Article 16, and Paragraph 1 of Article 17 of the Act shall include the following: 1. Core businesses and their significance. 2. Cyber security policy and objectives. 3. The organization promoting cyber security. 4. The deployment of dedicated manpower and fund. 5. The deployment of Cyber Security Officer of the government agency. 6. The inventory of information and information and communication systems and indicating the core ones and relevant assets. 7. Risk assessments of cyber security. 8. Protection and control measures for cyber security. 9. The reporting, responding and rehearsal mechanisms relating to cyber security incidents. 10. Cyber security information assessment and responding mechanism. 11. Management measures for outsourced information and communication system or service. 12. Assessment mechanism for personnel of the government agency who conducts business involving cyber security matters. 13. The continual improvement and performance management mechanism for the cyber security maintenance plan and implementation status. The implementation of cyber security maintenance plans submitted by each agency under Article 12, Paragraph 3 of Article 16, or Paragraph 2 of Article 17 of

第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關辦理，或經中央目的事業主管機關同意，由其所管特定非公務機關辦理。	the Act shall include the implementation results of and relevant explanations for those under each subparagraph of the preceding paragraph. The stipulation, amendment, and implementation of the cyber security maintenance plans under Paragraph 1, and the submission of the implementation thereof may be conducted by the superior or supervisory agency of the government agency; and in case of a specific non-government agency, the same may be conducted by its central authority in charge of relevant industry, the subordinate government agency of such central authority in charge of relevant industry, or the specific non-government agency regulated by the central authority in charge of relevant industry, with consent of such central authority in charge of relevant industry.
第七條　前條第一項第一款所定核心業務，其範圍如下： 一、公務機關依其組織法規，足認該業務為機關核心權責所在。 二、公營事業及政府捐助之財團法人之主要服務或功能。 三、各機關維運、提供關鍵基礎設施所必要之業務。 四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第四款涉及之業務。 前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。	Article 7　The scope of the core businesses specified in Subparagraph 1 of Paragraph 1 of the preceding article are as follows: 1. Businesses that are considered as the core accountabilities of the government agency as determined by its organizational regulation. 2. Major services or functions of government-owned enterprise and government-endowed foundation. 3. Businesses that are required by each agency for the maintenance and provision of critical infrastructure. 4. Businesses in which each agency is involved in accordance with Paragraphs 1 to 5 of Article 4, or Paragraphs 1 to 4 of Article 5 of the Regulations on Classification of Cyber Security Responsibility Levels. The term “core information and communication system” as used in Subparagraph 6 of Paragraph 1 of the preceding article refers to the system that is necessary for supporting the continual operation of core business, or that is of high level of defense requirements as determined in accordance with Schedule 9 to the Regulations on Classification of Cyber Security Responsibility Levels – principles of classification of cyber system defense requirement levels

第八條　本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告，應包括下列事項： 一、事件發生或知悉其發生、完成損害控制或復原作業之時間。 二、事件影響之範圍及損害評估。 三、損害控制及復原作業之歷程。 四、事件調查及處理作業之歷程。 五、事件根因分析。 六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。 七、前款措施之預定完成時程及成效追蹤機制。	Article 8　The investigation, handling and improvement report on cyber security incident under Paragraph 3 of Article 14 and Paragraph 3 of Article 18 of the Act shall include the following: 1. Times of the occurrences of or the awareness of the occurrences of the incidents, the completion of damage control or recovery operations. 2. The scope affected by the incidents and the damage assessment. 3. The courses of damage control and recovery operations. 4. The courses of incident investigations and handling operations. 5. Cause analysis of the incident. 6. Measures in aspects of management, technology, manpower or resources taken to prevent the reoccurrences of similar incident. 7. The estimated completion schedule and the follow-up mechanism of the measures under the preceding subparagraph.
第九條　中央目的事業主管機關依本法第十六條第一項規定指定關鍵基礎設施提供者前，應給予其陳述意見之機會。	Article 9　Before designating critical infrastructure providers under Paragraph 1 of Article 16 of the Act, the central authority in charge of relevant industry shall give such providers the opportunity to state their opinions.
第十條　本法第十八條第三項及第五項所稱重大資通安全事件，指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。	Article 10　The term “severe cyber security incident” as used in Paragraphs 3 and 5 of Article 18 of the Act refer to level-3 and level-4 cyber security incidents specified in Paragraphs 4 and 5 of Article 2 of the Regulations on the Notification and Response of Cyber Security Incidents.
第十一條　主管機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十八條第五項規定公告與事件相關之必要內容及因應措施時，應載明事件之發生或知悉其發生之時間、原因、影響程度、控制情形及後續改善措施。 前項與事件相關之必要內容及因應措施，有下列情形之一者，不予公告：	Article 11　When the competent authority or the central authority in charge of relevant industry is privy to a cyber security incident and publicize the necessary contents and countermeasures relating to severe cyber security incidents under Paragraph 5 of Article 18 of the Act, upon awareness of such incidents, times of occurrence or privy of the occurrence, causes, affection degree, control status, and subsequent improvement measures of such incidents shall be stated in the publications. Under any of the following circumstances, the

一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或公開有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。 二、其他依法規規定應秘密、限制或禁止公開之情形。 第一項與事件相關之必要內容及因應措施含有前項不予公告之情形者，得僅就其他部分公告之。	necessary contents and contingency measures relating to the incidents under the preceding paragraph shall not be publicized: 1. If it involves trade secrets or information relating to business operations of individuals, juristic persons or organizations or if the disclosure might infringe upon rights or other rightful interests of the government agency, individual, juristic person or organizations; except as is otherwise required by law, or necessary for public welfare or necessary for protection of life, body, and health of people, or with consent of the parties concerned. 2. Other circumstances of confidentiality, restriction, or prohibition on disclosure as required by law. If the necessary contents and contingency measure relating to the incidents shall not be publicized under Paragraph 1, only the other portion may be publicized.
第十二條　特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。	Article 12　If businesses of the specific non-government agency involve the accountabilities of several central authority in charge of relevant industry, the competent authority may designate via coordination more than one central authority in charge of relevant industry to solely or jointly conduct the matters to be conducted by the central authority in charge of relevant industry under the Act.
第十三條　本細則之施行日期，由主管機關定之。	Article 13　The implementation date of the Rules shall be stipulated by the competent authority.