資通安全事件通報及應變辦法_英譯對照

資通安全事件通報及應變辦法	Regulations on the Notification and Response of Cyber Security Incident
第一章 總則	Chapter 1 General Provisions
第一條　本辦法依資通安全管理法（以下簡稱本法）第十四條第四項及第十八條第四項規定訂定之。	Article 1　These Regulations are stipulated in accordance with Paragraph 4 of Article 14 and Paragraph 4 of Article 18 of the Cyber Security Management Act(hereinafter referred to as the "Act").
第二條　資通安全事件分為四級。 公務機關或特定非公務機關（以下簡稱各機關）發生資通安全事件，有下列情形之一者，為第一級資通安全事件： 一、非核心業務資訊遭輕微洩漏。 二、非核心業務資訊或非核心資通系統遭輕微竄改。 三、非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。 各機關發生資通安全事件，有下列情形之一者，為第二級資通安全事件： 一、非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。 二、非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。 三、非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。 各機關發生資通安全事件，有下列情形之一者，為第三級資通安全事件：	Article 2　Cyber security incident is classified into four levels. The cyber security incident occurred to the government agency or the specific non-government agency (hereinafter referred to as "each agency") under any of the following circumstances is the level-1 cyber security incident: 1. Minor breach of non-core business information. 2. Minor alteration of non-core business information or non-core information and communication system. 3. Impact on or interruption of non-core business operation which may be recovered within tolerable interruption time, resulting in impact on daily operation of each agency. The cyber security incident occurred to each agency under any of the following circumstances is the level-2 cyber security incident: 1. Serious breach of non-core business information or minor breach of core business information not involving the maintenance and operation of critical infrastructures. 2. Serious alteration of non-core business information or non-core information and communication system, or minor alteration of core business information or core information and communication system not involving the maintenance and operation of critical infrastructures. 3. Impact on or interruption of non-core business operation, which cannot be recovered within tolerable interruption time, or impact on or interruption of core business or core information and communication system operation not involving the maintenance and operation of critical infrastructures, which may be recovered within tolerable interruption time.

一、未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。 二、未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。 三、未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。	The cyber security incident occurred to each agency under any of the following circumstances is the level-3 cyber security incident: 1. Serious breach of core business information not involving the maintenance and operation of critical infrastructures, or minor breach of confidential, sensitive information of general official affairs, or minor breach of core business information involving the maintenance and operation of critical infrastructures. 2. Serious alteration of core business information or core information and communication system not involving the maintenance and operation of critical infrastructures, or minor alteration of confidential, sensitive information of general official affairs or core business information or core information and communication system involving the maintenance and operation of critical infrastructures. 3. Impact on or interruption of the operation of core business or core information and communication system not involving the maintenance and operation of critical infrastructures, which cannot be recovered within the tolerable interruption time, or impact on or interruption of the operation of core business or core information and communication system involving the maintenance and operation of critical infrastructures, which may be recovered within tolerable interruption time.
各機關發生資通安全事件，有下列情形之一者，為第四級資通安全事件： 一、一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。 二、一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。 三、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。	The cyber security incident occurred to each agency under any of the following circumstances is the level-4 cyber security incident: 1. Serious breach of confidential, sensitive information of general official affairs or core business information involving the maintenance and operation of critical infrastructures, or the breach of classified national security information. 2. Serious alteration of confidential, sensitive information of general official affairs or core business information or core information and communication system involving the maintenance and operation of critical infrastructures, or the alteration of classified national security information.

	3. Impact on or interruption of core business or core information and communication system involving the maintenance and operation of critical infrastructures, which cannot be recovered within tolerable interruption time.
第三條 資通安全事件之通報內容，應包括下列項目： 一、發生機關。 二、發生或知悉時間。 三、狀況之描述。 四、等級之評估。 五、因應事件所採取之措施。 六、外部支援需求評估。 七、其他相關事項。	Article 3 Content of the notification of cyber security incident shall include the following items: 1. The agency occurred. 2. The time of occurrence or awareness. 3. The description of the situation. 4. Level assessment. 5. Coping measure in response to the incident. 6. Assessment of requirement for external support. 7. Other relevant items.
第 二 章 公務機關資通安全事件之通報及應變	Chapter 2 The notification and response of cyber security incident of government agency
第四條 公務機關知悉資通安全事件後，應於一小時內依主管機關指定之方式及對象，進行資通安全事件之通報。 前項資通安全事件等級變更時，公務機關應依前項規定，續行通報。 公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。 公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。	Article 4 Upon awareness of the cyber security incident, the government agency shall conduct the notification of the cyber security incident within one hour in the manner and to the objects as designated by the competent authority. In case of the change to the level of the cyber security incident under the preceding paragraph, the government agency shall continue the notification as provided for in the preceding paragraph. When the notification conducted in the manner as specified in Paragraph 1 is unavailable for some reason, the government agency shall conduct the notification in another appropriate manner within the timeframes prescribed under the same paragraph, and note the cause of unable notification from being conducted in the required manner. After eliminating of the cause of unable notification from being conducted in the manner as required under Paragraph 1, the government agency shall supplement the notification in the same manner.
第五條 主管機關應於其自身完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級： 一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。 二、通報為第三級或第四級資通安全事件者，	Article 5 After the completion of the notification of the cyber security incident, the competent authority shall complete the review of the level of such cyber security incident within the following timeframes, and may change its level according to the review results: 1. Within eight hours after receipt of the notification of a level-1 or level-2 cyber security incident. 2. Within two hours after receipt of the notification of a level-3 or level-4 cyber security incident.

於接獲後二小時內。 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，應於其自身、所屬、監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關，及前開鄉（鎮、市）、直轄市山地原住民區民代表會，完成資通安全事件之通報後，依前項規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級。 前項機關依規定完成資通安全事件等級之審核後，應於一小時內將審核結果通知主管機關，並提供審核依據之相關資訊。 總統府、國家安全會議、立法院、司法院、考試院、監察院及直轄市、縣（市）議會，應於其自身完成資通安全事件之通報後，依第一項規定時間完成該資通安全事件等級之審核，並依前項規定通知主管機關及提供相關資訊。 主管機關接獲前二項之通知後，應依相關資訊，就資通安全事件之等級進行覆核，並得依覆核結果變更其等級。但主管機關認有必要，或第二項及前項之機關未依規定通知審核結果時，得就該資通安全事件逕為審核，並得為等級之變更。	The Presidential Office, the agencies directly subordinate to the central first-level agencies, and special municipalities and county(city) governments shall, after the notification of the cyber security incident, conducted by themselves, their subordinate or supervisory government agencies, their governed villages (townships/cities), mountain indigenous district offices of special municipalities, and the subordinate or supervisory government agencies of such governed villages(townships/cities) and mountain indigenous district offices of special municipalities, and the representative councils of the above said villages (townships/cities) and Mountain Indigenous Districts of Special Municipalities councils, complete the review of level of such cyber security incident within the timeframes as required under the preceding paragraph, and may change its level according to the review results. After completion of the required review of the level of the cyber security incident, the agencies under the preceding paragraph shall notify the competent authority of the review results within one hour, and shall provide information relating to the basis of the reviews. The Presidential Office, the National Security Council, the Legislative Yuan, the Judicial Yuan, the Examination Yuan, the Control Yuan, and special municipalities and county(city) councils shall, after completion of their own notification of cyber security incident, conduct the review of the level of such cyber security incident within the timeframes as specified under Paragraph 1, and shall notify and provide the competent authority with relevant information as required under the preceding paragraph. Upon receipt of the notifications under the preceding two paragraphs, the competent authority shall further review the level of the cyber security incident according to the relevant information, and may change its level according to the review result. However, if it is deemed necessary, or if the agencies under Paragraph 2 and the preceding paragraph fail to notify of the required review results, the competent authority may directly review such cyber security incident and may change its level.
第六條　公務機關知悉資通安全事件後，應依下列規定時間	Article 6 Upon awareness of the cyber security incident, the

完成損害控制或復原作業，並依主管機關指定之方式及對象辦理通知事宜： 一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。 二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。 公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。 前項調查、處理及改善報告送交之時限，得經上級或監督機關及主管機關同意後延長之。 上級、監督機關或主管機關就第二項之調查、處理及改善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求公務機關提出說明及調整。	government agency shall complete the damage control or recovery operation within the following timeframes, and shall conduct the notification in the manner and to the objects as designated by the competent authority: 1. Within seventy-two hours of the awareness of a level-1 or level-2 cyber security incident; 2. Within thirty-six hours of the awareness of a level-3 or level-4 cyber security incident. After completion of the damage control or recovery operation under the preceding paragraph, the government agency shall continue the investigation and management of the cyber security incident, and shall submit the investigation, management and improvement report within one month in the manner designated by the competent authority. The timeframe of submission of the investigation, management, and improvement reports under the preceding paragraph may be extended with the consent of the superior or supervising agencies and the competent authority. If the superior or supervising agencies or the competent authority deem necessary or deem there is any non-compliance with the regulatory requirement, improper matters or other matters to be improved in the investigation, management, and improvement reports under Paragraph 2, they may require the government agency to give explanations and make adjustments.
第七 條 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，就所屬、監督、所轄或業務相關之公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。 主管機關就公務機關執行資通安全事件之應變作業，得視情形提供必要支援或協助。 公務機關知悉第三級或第四級資通安全事件後，其資通安全長應召開會議研商相關事宜，並得請相關機關提供協助。	Article 7 The Presidential Office, the agencies directly subordinate to central first-level agencies, and the special municipalities and county(city) governments shall provide necessary assistance or support in respect of the notification and response operation of the cyber security incident implemented by the government agency which is subordinate to, or supervised or regulated by, or whose businesses are related to them, if circumstances so require. The competent authority may provide necessary support and assistance in respect of the response operation of the cyber security incident implemented by the government agency, if circumstances so require. After the government agency becomes aware of a level-3 or level-4 cyber security incident, its Cyber Security Officer shall convene the meetings to discuss relevant matters, and may request relevant agencies to provide assistances.

第八條 總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關、所轄鄉（鎮、市）、直轄市山地原住民區公所與其所屬或監督之公務機關及前開鄉（鎮、市）、直轄市山地原住民區民代表會，應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。 前項演練作業之內容，應至少包括下列項目： 一、每半年辦理一次社交工程演練。 二、每年辦理一次資通安全事件通報及應變演練。 總統府與中央一級機關及直轄市、縣（市）議會，應依前項規定規劃及辦理資通安全演練作業。	Article 8 The Presidential Office, the agencies directly subordinate to central first-level agencies, and the special municipalities and county(city) governments shall plan and conduct cyber security exercise for themselves, their subordinate or supervisory government agencies, their governed villages(townships/cities), mountain indigenous district offices of special municipalities, and the subordinate or supervisory government agencies of such governed villages (townships/cities) and mountain indigenous district offices of special municipalities, and the representative councils of the above said villages(townships/cities) and Mountain Indigenous Districts of Special Municipalities councils, and shall submit the implementation status thereof and the result reports thereon to the competent authority within one month after the completion thereof. Content of the exercise operation under the preceding paragraph shall include the following items at least: 1. Social engineering exercise shall be conducted once every six months. 2. The notification and response exercise of the cyber security incident shall be conducted once a year. The Presidential Office and the central first-level agencies and special municipalities and county/city councils shall plan and conduct the cyber security exercise operation required under the preceding paragraph.
第九條 公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： 一、判定事件等級之流程及權責。 二、事件之影響範圍、損害程度及機關因應能力之評估。 三、資通安全事件之內部通報流程。 四、通知受資通安全事件影響之其他機關之方式。 五、前四款事項之演練。 六、資通安全事件通報窗口及聯繫方式。 七、其他資通安全事件通報相關事項。	Article 9 The government agency shall stipulate the operational regulations on the notification of the cyber security incident, the content of which shall include the following matters: 1. The process and the accountabilities of judgment and determination of levels of the incident. 2. Assessment of the impact scope and damage degrees of the incident and the response abilities of the agencies. 3. The process of internal notification on the cyber security incident. 4. The method and time of notification to other agencies impacted by the cyber security incident. 5. The exercises under the preceding four paragraphs. 6. The contact window and methods of notification of the cyber security incident. 7. Other matters relating to the cyber security incident.
第十條 公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：	Article 10 The government agency shall stipulate the operational regulations on the response of the cyber security incident, the content of which shall include the following matters:

一、應變小組之組織。 二、事件發生前之演練作業。 三、事件發生時之損害控制機制。 四、事件發生後之復原、鑑識、調查及改善機制。 五、事件相關紀錄之保全。 六、其他資通安全事件應變相關事項。	1. The organization of the response team. 2. The exercise prior to the occurrence of the incident. 3. The mechanism of damage control on the occurrence of the incident and request for technical support or other necessary assistance from the central authority in charge of relevant industry concerned. 4. Recovery, identification, investigation, and improvement mechanisms after the occurrence of the incident. 5. The preservations of records relating to the incident. 6. Other matters relating to the response of the cyber security incident.
第三章 特定非公務機關資通安全事件之通報及應變	Chapter 3 The notification and response of cyber security incident of the specific non-government agency
第十一條 特定非公務機關知悉資通安全事件後，應於一小時內依中央目的事業主管機關指定之方式，進行資通安全事件之通報。 前項資通安全事件等級變更時，特定非公務機關應依前項規定，續行通報。 特定非公務機關因故無法依第一項規定方式通報者，應於同項規定之時間內依其他適當方式通報，並註記無法依規定方式通報之事由。 特定非公務機關於無法依第一項規定方式通報之事由解除後，應依該方式補行通報。	Article 11 Upon awareness of the cyber security incident, the specific non-government agency shall conduct the notification of the cyber security incident within one hour in the manner as designated by the central authority in charge of relevant industry. In case of change to the level of the cyber security incident under the preceding paragraph, the specific non-government agency shall continue the notification as provided for in the preceding paragraph. If the notification conducted in the manner as specified in Paragraph 1 is prevented for any cause, the specific non-government agency shall conduct the notification in another appropriate manner within the timeframes prescribed under the same paragraph, and note the cause for not being able to report by the prescribed manner. After the elimination of the cause for preventing the notification from being conducted in the manner as required under Paragraph 1, the specific non-government agency shall supplement the notification in the original manner.
第十二條 中央目的事業主管機關應於特定非公務機關完成資通安全事件之通報後，依下列規定時間完成該資通安全事件等級之審核，並得依審核結果變更其等級： 一、通報為第一級或第二級資通安全事件者，於接獲後八小時內。 二、通報為第三級或第四級資通安全事件者，於接獲後二小時內。 中央目的事業主管機關	Article 12 After the specific non-government agency has completed the notifications of cyber security incident, the central authority in charge of relevant industry shall complete verification of the level of such cyber security incident within the following timeframes, and may change its level according to the verify results: 1. Within eight hours after receipt of the notification of a level-1 or level-2 cyber security incident. 2. Within two hours after receipt of notification of a level-3 or level-4 cyber security incident.

依前項規定完成資通安全事件之審核後，應依下列規定辦理： 一、審核結果為第一級或第二級資通安全事件者，應定期彙整審核結果、 依據及其他必要資訊，依主管機關指定之方式送交主管機關。 二、審核結果為第三級或第四級資通安全事件者，應於審核完成後一小時內，將審核結果、依據及其他必要資訊，依主管機關指定之方式送交主管機關。 主管機關接獲前項資料後，得就資通安全事件之等級進行覆核，並得為等級之變更。	After completion of the verification of the cyber security incident as required under the preceding paragraph, the central authority in charge of relevant industry shall proceed with the following requirement: 1. If the verification result indicates a level-1 or level-2 cyber security incident, they shall periodically summarize the verification result, basis, and other necessary information, and then submit them to the competent authority in the manner as specified by the competent authority. 2. If the verification result indicates a level-3 or level-4 cyber security incident, they shall, within one hour of the completion of the verification, submit the verification result, basis, and other necessary information to the competent authority in the manner as specified by the competent authority. Upon receipt of the documentation under the preceding paragraph, the competent authority may review the level of the cyber security incident, and may change its level.
第十三條 特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜： 一、第一級或第二級資通安全事件，於知悉該事件後七十二小時內。 二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。 特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。 前項調查、處理及改善報告送交之時限，得經中央目的事業主管機關同意後延長之。 中央目的事業主管機關就第二項之調查、處理及改	Article 13 Upon awareness of the cyber security incident, the specific non-government agency shall complete damage control or recovery operation within the following timeframes, and shall conduct the notification in the manner as designated by the central authority in charge of relevant industry: 1. Within seventy-two hours of the awareness of a level-1 or level-2 cyber security incident. 2. Within thirty-six hours of the awareness of a level-3 or level-4 cyber security incident. After completion of damage control or recovery operation under the preceding paragraph, the specific non-government agency shall continue the investigation and management of the cyber security incident, and shall submit the investigation, management, and improvement report within one month in the manner as designated by the central authority in charge of relevant industry. The timeframe of submission of the investigation, management, and improvement report under the preceding paragraph may be extended with the consent of the central authority in charge of relevant industry. If the central authority in charge of relevant industry

善報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。 特定非公務機關就第三級或第四級資通安全事件送交之調查、處理及改善報告，中央目的事業主管機關應於審查後送交主管機關；主管機關就該報告認有必要，或認有違反法令、不適當或其他須改善之情事者，得要求特定非公務機關提出說明及調整。	deems necessary or deems there is any non-compliance with regulatory requirement, improper matter or other matter to be improved in the investigation, management, and improvement reports under Paragraph 2, they may require the specific non-government agency to give the explanation and make adjustment. Upon review of the investigation, management, and improvement report on a level-3 or level-4 cyber security incident submitted by the specific non-government agency, the central authority in charge of relevant industry shall submit such report to the competent authority; if the competent authority deems necessary, or deems there is any non-compliance with regulatory requirement, improper matter, or other matter to be improved, it may require the specific non-government agency to give explanation and make adjustment.
第十四條 中央目的事業主管機關就所管特定非公務機關執行資通安全事件之通報及應變作業，應視情形提供必要支援或協助。 主管機關就特定非公務機關執行資通安全事件應變作業，得視情形提供必要支援或協助。 特定非公務機關知悉第三級或第四級資通安全事件後，應召開會議研商相關事宜。	Article 14 The central authority in charge of relevant industry shall provide necessary support or assistance in respect to the notification and response of cyber security incident implemented by the specific non-government agency under its authority, if circumstances so require. The competent authority may provide necessary support and assistance in respect to the notification and response operation of the cyber security incident implemented by the specific non-government agency, if circumstances so require. After the specific non-government agency becomes aware of a level-3 or level-4 cyber security incident, it shall convene meetings to discuss relevant matters.
第十五條 特定非公務機關應就資通安全事件之通報訂定作業規範，其內容應包括下列事項： 一、判定事件等級之流程及權責。 二、事件之影響範圍、損害程度及機關因應能力之評估。 三、資通安全事件之內部通報流程。 四、通知受資通安全事件影響之其他機關之時機及方式。 五、前四款事項之演練。 六、資通安全事件通報窗口及聯繫方式。 七、其他資通安全事件通報相關事項。	Article 15 The specific non-government agency shall stipulate the operational regulations on the notification of the cyber security incident, the content of which shall include the following matters: 1. The process and the accountabilities of judgment and determination of levels of the incident. 2. Assessment of the impact scope and damage degrees of the incident and the response abilities of the agencies. 3. The process of internal notification on the cyber security incident. 4. The method and time of notification to other agencies impacted by the cyber security incident. 5. The exercises under the preceding four paragraphs. 6. The contact window and methods of notification of the cyber security incident. 7. Other matters relating to the cyber security incident.

第十六條 特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項： 一、應變小組之組織。 二、事件發生前之演練作業。 三、事件發生時之損害控制，及向中央目的事業主管機關請求技術支援或其他必要協助之機制。 四、事件發生後之復原、鑑識、調查及改善機制。 五、事件相關紀錄之保全。 六、其他資通安全事件應變相關事項。	Article 16 The specific non-government agency shall stipulate the operational regulations on the response of the cyber security incident, the content of which shall include the following matters: 1. The organization of the response team. 2. The exercise prior to the occurrence of the incident. 3. The mechanism of damage control on the occurrence of the incident and request for technical support or other necessary assistance from the central authority in charge of relevant industry concerned. 4. Recovery, identification, investigation, and improvement mechanisms after the occurrence of the incident. 5. The preservations of records relating to the incident. 6. Other matters relating to the response of the cyber security incident.
第四章 附則	Chapter 4 Supplementary Provisions
第十七條 主管機關就各機關之第三級或第四級資通安全事件，得召開會議，邀請相關機關研商該事件之損害控制、復原及其他相關事宜。	Article 17 For level-3 or level-4 cyber security incident of each agency, the competent authority may convene meetings and invite relevant agencies to discuss the damage control, recovery, and other relevant matters of such incident.
第十八條 公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目： 一、社交工程演練。 二、資通安全事件通報及應變演練。 三、網路攻防演練。 四、情境演練。 五、其他必要之演練。	Article 18 The government agency shall cooperate with the competent authority which shall plan and conduct the cyber security exercise. The content of exercise may include the following matters: 1. Social engineering exercise. 2. The notification and response exercise of the cyber security incident. 3. Cyber offense and defense exercise. 4. Scenario exercise. 5. Other necessary exercise.
第十九條 特定非公務機關應配合主管機關規劃、辦理之資通安全演練作業，其內容得包括下列項目： 一、網路攻防演練。 二、情境演練。 三、其他必要之演練。 主管機關規劃、辦理之資通安全演練作業，有侵害特定非公務機關之權利或正當利益之虞者，應先經其書面同意，始得為之。 前項書面同意之方式，	Article 19 The specific non-government agency shall, in coordination with the competent authority, plan and conduct the cyber security exercise, the content of which may include the following matters: 1. Cyber offense and defense exercise. 2. Scenario exercise. 3. Other necessary exercise. If the cyber security exercise planned and conducted by the competent authority has imminent threats of infringement to the rights or legitimate interests of the specific non-government agency, such exercise may be conducted only with written consent of such agency. The written consent under the preceding paragraph may be made by electronic documents in accordance with the Electronic Signatures Act.

依電子簽章法之規定，得以電子文件為之。	
第二十條　公務機關於本辦法施行前，已針對其自身、所屬或監督之公務機關或所管之特定非公務機關，自行或與其他機關共同訂定資通安全事件通報及應變機制，並實施一年以上者，得經主管機關核定後，與其所屬或監督之公務機關或所管之特定非公務機關繼續依該機制辦理資通安全事件之通報及應變。 前項通報及應變機制如有變更，應送主管機關重為核定。	Article 20　If, before the enforcement of these Regulations, the government agency has, independently or jointly with other agencies, formulated the notification and response mechanism for itself or for its subordinate or supervisory government agencies or for its regulated specific non-government agencies, and have enforced such mechanism for more than one year, and maybe approved by the competent authority, they and their subordinate or supervisory government agencies or their regulated specific non-government agencies may continue to conduct the notification and response of cyber security incident according to such mechanism. In case of change to the notification and response mechanism under the preceding paragraph, such change shall be submitted to the competent authority for approval again.
第二十一條 本辦法之施行日期，由主管機關定之。	Article 21　The implementation date of the Regulations shall be stipulated by the competent authority.