

數位發展部所管特定非公務機關資通安全管理 作業辦法總說明

為明定數位發展部所管特定非公務機關之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項，爰依據資通安全管理法第十六條第六項及第十七條第四項規定，訂定「數位發展部所管特定非公務機關資通安全管理作業辦法」（以下簡稱本辦法），其重點如下：

- 一、關鍵基礎設施提供者定義（第二條）。
- 二、特定非公務機關資通安全維護計畫應包含之內容。（第三條）
- 三、資通安全維護計畫及實施情形之提出方式及時程。（第四條及第五條）
- 四、數位發展部應辦理特定非公務機關稽核事項。（第六條至第八條）
- 五、稽核小組之組成規範。（第九條）
- 六、稽核結果報告交付時程及稽核結果報告應記載之內容。（第十條）
- 七、稽核改善報告之提出方式及時程。（第十一條）
- 八、本辦法所定書面，得以電子文件為之。（第十二條）
- 九、委任或委託其他公務機關或法人辦理資通安全管理事務及其保密義務（第十三條）

數位發展部所管特定非公務機關資通安全管理 作業辦法

條文	說明
第一章 總則	章名。
第一條 本辦法依資通安全管理法（以下簡稱本法）第十六條第六項及第十七條第四項規定訂定之。	本辦法訂定依據。
第二條 本辦法所稱關鍵基礎設施提供者，指數位發展部（以下簡稱本部）依本法第十六條第一項規定指定，經行政院核定者。	明定本部所管關鍵基礎設施提供者定義。
第二章 資通安全維護計畫必要事項及實施情形之提出	章名。
第三條 本部所管特定非公務機關（以下簡稱特定非公務機關）之資通安全維護計畫，應依本法施行細則第六條第一項規定辦理。	明定資通安全維護計畫應包含資通安全管理法施行細則規定內容。
第四條 特定非公務機關應於本部通知後三個月內，依本部指定之方式提出資通安全維護計畫。 資通安全維護計畫經修正者，應於修正後一個月內向本部提報修正後之計畫。 前二項資通安全維護計畫應載明事項有不完備者，特定非公務機關應於本部通知之期限內完成補正。	一、依本法第十六條第二項及第十七條第一項之規定，特定非公務機關應訂定、修正及實施資通安全維護計畫，為確認本部所管特定非公務機關資通安全維護計畫訂定情形，故於第一項明定其應於本部通知後三個月內，依指定之方式提出。 二、特定非公務機關自行修正其資通安全維護計畫時，為利本部辦理後續稽核及實施情形之審查，該特定非公務機關亦有向本部提出修正後計畫之義務，爰於第二項予以明定。 三、第三項明定資通安全維護計畫不完備時之補正處理程序。
第五條 關鍵基礎設施提供者應於每年五月底前，依本部指定之方式提出前一年度資通安全維護計畫實施情形。 其他特定非公務機關，經本部依本法第十七條第二項規定要求提出資通安全維護計畫實施情形者，應於本部通知後二個月內，依本部指定之方式提出。	一、依本法第十六條第三項之規定，關鍵基礎設施提供者應向本部提出資通安全維護計畫實施情形，爰於第一項明定其實施情形提出方式。 二、依本法第十七條第二項之規定本部得要求所管關鍵基礎設施提供者以外之特定非公務機關，提出資通安全維護計畫實施情形，故於第二項明定其實施情形提出方式。

第三章 資通安全維護計畫實施情形之稽核	章名。
第六條 本部除因不可抗力因素外，應每年擇定特定非公務機關，以現場稽核方式，稽核其資通安全維護計畫實施情形。 本部為辦理前項稽核，應訂定稽核計畫，包括稽核之依據與目的、期間、稽核小組組成方式、保密義務、稽核方式、項目及基準等與稽核相關之事項。 本部決定前項稽核之項目及基準時，應綜合考量我國資通安全政策、國內外資通安全趨勢、過往稽核成效及稽核資源相關因素。 本部依第一項規定擇定受稽核之特定非公務機關（以下簡稱受稽核者）時，應綜合考量其資通安全責任等級、資通安全事件發生之頻率與程度、資通安全演練之結果、歷年受本部稽核之頻率與結果及其他與資通安全相關因素。	一、第一項明定本部稽核特定非公務機關資通安全維護計畫實施情形之頻率及方式。 二、第二項明定本部為辦理第一項之稽核，應訂定稽核計畫及其內容應包括之事項。 三、為使稽核作業能切合我國資通安全政策之規劃內容，並適時反映國內外資通安全相關趨勢，強化稽核資源分配與成效，爰於第三項明定本部於訂定稽核計畫，決定稽核之重點領域與基準及其項目時，應綜合考量之因素。 四、為有效利用稽核資源，提升稽核成效，爰於第四項明定本部於訂定稽核計畫，決定受稽核機關時，應綜合考量之因素，以決定最適之受稽核機關名單。
第七條 本部辦理前條第一項之稽核，應於一個月前將稽核計畫以書面通知受稽核者。 前項受稽核者因業務因素或其他正當理由，無法於本部指定之時間配合稽核者，得於收受前項通知後五日內，以書面敘明理由向本部申請變更稽核日期。 前項申請，除有不可抗力之事由外，以一次為限。	一、為避免本部辦理稽核影響受稽核機關之日常業務，並使受稽核機關有充裕時間預為準備，以增進稽核效能，爰於第一項明定本部應於實際辦理稽核之一個月前，通知受稽核機關。 二、若受稽核機關因業務等因素，未能配合稽核者，得於收受前項通知後五日內，以書面敘明理由向本部申請變更稽核日期，並原則以一次為限，爰為第二項及第三項之規定。
第八條 本部辦理第六條第一項之稽核，得要求受稽核者說明資通安全維護計畫實施情形、提供相關佐證資料供現場查閱，並配合執行下列事項： 一、稽核前訪談。 二、現場實地稽核。 受稽核者依法律有正當理由，不能為前項說明、提供資料或配合措施時，應以書面敘明理由，向本部提出。 本部收受前項書面後，應進行審核，依下列規定辦理，並得停止稽核	一、第一項明定本部辦理第六條第一項之稽核時，受稽核機關之配合義務內容，以利本部藉由稽核確認受稽核機關遵循本法之情形。 二、受稽核機關如依法律有正當理由，而不能為第一項之說明、提供資料或配合措施，例如提供資料將侵害第三人之正當權利，此時受稽核機關應以書面敘明其理由，向本部提出，俾利本部依第十條第二項規定記載於稽核結果報告或其他相關紀錄，爰為第二項規

作業之全部或一部： 一、認有理由者，應將審核之依據及相關資訊記載於稽核結果報告。 二、認無理由者，應要求受稽核者依第一項規定辦理；已停止稽核作業者，得擇期續行辦理，並於十日前以書面通知受稽核者。	定。 三、為明確規範特定非公務機關依第二項規定，提出未能配合之書面理由時，本部審認其有無理由及後續處理方式，爰參照「特定非公務機關資通安全維護計畫實施情形稽核辦法」第五條第三項規定，明定第三項規定。
第九條 本部為辦理第六條第一項之稽核，應依同條第四項之考量因素及實際稽核需求組成稽核小組。 前項稽核小組成員三人至七人，由具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識之公務機關代表或專家學者擔任；其中公務機關代表不得少於全體成員人數之三分之一。 前項公務機關代表或專家學者有下列情形之一者，應主動迴避擔任該次稽核之稽核小組成員： 一、本人、其配偶、三親等內親屬、家屬或上開人員財產信託之受託人，與受稽核之特定非公務機關或其負責人間有財產上或非財產上之利害關係。 二、本人、其配偶、三親等內親屬或家屬，與受稽核之特定非公務機關或其負責人間，目前或過去二年內有僱傭、承攬、委任、代理或其他類似之關係。 三、目前或過去二年內，本人或任職之機關(構)或單位，為受稽核之特定非公務機關之顧問，其輔導項目與受稽核項目相關。 四、其他足認擔任稽核小組成員將影響稽核結果公正性之情形。 本部應以書面與稽核小組成員約定利益衝突之迴避事項及執行稽核之保密義務。	一、為使本部得妥適辦理對特定非公務機關資通安全維護計畫實施情形之稽核，爰於第一項明定本部應考量相關因素組成稽核小組。 二、考量稽核小組所需具備之知能，爰於第二項明定本部組成稽核小組時，所邀請之公務機關代表或專家學者應具備資通安全政策或該次稽核所需之技術、管理、法律或實務專業知識，以協助本部進行稽核及提供專業意見。且為確保稽核結果之公平性，爰明定公務機關代表於稽核小組之人數所占比例不得少於三分之一。 三、為確保稽核結果之客觀性，以及避免爭議，爰於第三項明定第二項之公務機關代表或專家學者應主動迴避擔任稽核小組成員之情形。 四、為保障受稽核機關之權益，爰於第四項規明定稽核小組之利益衝突迴避事項及保密義務，且本部應與稽核小組成員以書面為約定。
第十條 本部應於稽核作業完成後一個月內，將稽核結果報告交付受稽核者。 前項稽核結果報告之內容，應包括稽核之範圍、缺失或待改善事項、第八條第二項所定受稽核之特定非公務機關未能為說明、提供資料或配合	一、第一項明定本部應於受稽核機關之稽核作業完成後一個月內，將稽核結果報告交付受稽核機關。 二、第二項明定稽核結果報告應記載之內容。 三、考量資通安全署係綜理國家資通安全之規劃、推動與執行機關，並

措施之情形與理由及其他相關事項。 本部辦理稽核後，應於次年一月底前彙整第一項稽核結果報告，並送本部資通安全署。	為掌握各中央目的事業主管機關就特定非公務機關之稽核情形，爰第三項明定本部每年彙整稽核結果報告，並送本部資通安全署。
第十一條 受稽核者經發現其資通安全維護計畫實施有缺失或待改善者，應於收受稽核結果報告後一個月內，依本部指定之方式，向本部提出改善報告。 受稽核者依前項規定提出改善報告後，應依其缺失或待改善事項之性質、程度，適時以書面提出改善報告之執行情形；本部認有必要時，得要求受稽核者進行說明或調整。	一、依本法第十六條第五項及第十七條第三項之規定，特定非公務機關受本部稽核，經發現其資通安全維護計畫實施情形有缺失或待改善者，應向本部提出改善報告。為利執行，爰明定受稽核機關經發現其資通安全維護計畫實施情形有缺失或待改善者，應提出改善報告之程序，並應提出改善報告之執行情形，俾利本部進行後續之監督。 二、受稽核機關提出改善報告應包含之內容等相關事項，另依本法施行細則第三條之規定辦理。
第四章 附則	章名
第十二條 本辦法所定書面，依電子簽章法規定，得以電子文件為之。	明定本辦法所定書面，依電子簽章法之規定，得以電子文件為之。
第十三條 本辦法所定特定非公務機關提出資通安全維護計畫與其實施情形之通知、收受及該計畫實施情形之稽核事務，本部得委任或委託其他公務機關或法人辦理。 前項受委任或委託之公務機關或法人對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。	一、除政策制定等本質上不宜委任或委託辦理之事務外，本部推動資通安全業務，如有需要，得依行政程序法第十五條或第十六條規定，委任或委託其他公務機關或法人辦理。為利實務運作，爰為本條規範。 二、本部依本條規定為委任或委託，因涉及公權力之移轉，應考量事務之性質、對象之屬性等事項，先行評估委任或委託辦理之適當性後，再行為之。 三、為保障特定非公務機關之秘密不因本部之委任或委託而洩露，爰於第二項明定受委任或委託者在執行過程中就獲悉之秘密有保密義務。
第十四條 本辦法自發布日施行。	明定本辦法之施行日期。