

# 國家通訊傳播委員會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。
第二章 資通安全維護計畫必要事項及實施情形之提出	章名。
<p>第二條 國家通訊傳播委員會(以下簡稱本會)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，除依本法施行細則第六條第一項規定外，並應包含下列事項：</p> <p>一、資通安全偵測與防護之建置及執行方案。但經本會認定得免包含資通安全偵測之建置及執行方案者，不在此限。</p> <p>二、執行前款方案所蒐集、儲存、處理及利用使用者資料之安全保護措施。</p> <p>三、通過資通安全管理驗證之執行方案。</p> <p>特定非公務機關依本法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，除依本法施行細則第六條第二項規定外，並應包括前項各款之執行成果及相關說明。</p>	<p>一、本會為加速通訊傳播事業導入資通安全管理，強化其資通安全防護能量，業於固定通信業務管理規則、行動寬頻業務管理規則及第二類電信事業管理規則增訂資通安全管理專章，明定要求經營者建立「資通安全防護及偵測設施」及通過資通安全管理驗證之規定。為使本會所管特定非公務機關訂定之「資通安全維護計畫」，於實際執行面向與現行規定之推動方向相符，爰於第一項規定該計畫應包含上揭管理規則規定事項之建置及執行方案；另審酌部分本會所管特定非公務機關之服務未使用電信資源且經營規模較小，為使其仍能在有限資源下落實資通安全維護計畫，爰於第一項第一款但書規定，僅要求其計畫應包含資通安全防護之建置及執行方案。</p> <p>二、另審酌本會所管特定非公務機關為因應資通安全防護或偵測目的，對於其網路或系統相關資料之蒐集、儲存、處理及利用，應訂定使用目的及保護政策，並明定管理辦法及標準作業程序，無論直接或間接之利用，皆應確保使用者資料之安全，爰於第一項第二款規定其資通安全維護計畫應包含對於使用者資料之安全保護措施。另於第一項第三款規定其資通安全維護計畫應包含通過資通安全管理驗證之執行方案，以使其規劃內容更為具體明確。</p> <p>三、本會所管特定非公務機關之資通安全維護計畫，除依本法施行細則第六條第一項規定外，並應包含本條第一項所列各款事項。故該特定非公務機關依本法第十六條第三項或第十七條第二項規定提</p>

	出資通安全維護計畫實施情形，除依本法施行細則第六條第二項規定外，並應包括第一項各款之執行成果及相關說明，爰於第二項明定之。
<p>第三條 特定非公務機關應於本會通知後三個月內，向本會提出資通安全維護計畫。</p> <p>前條第一項規定事項修正時，特定非公務機關應配合修正其資通安全維護計畫，並向本會提出。</p> <p>特定非公務機關之資通安全維護計畫修正者，應向本會提出修正後之計畫。</p> <p>前三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會通知之期限內完成補正。</p>	<p>一、為利本會後續規劃稽核作業之時程，並考量特定非公務機關於本會通知後，應有一定合理之作業時間，爰於第一項明定特定非公務機關應於本會通知後三個月內提出資通安全維護計畫。</p> <p>二、資通安全維護計畫應載事項修正時，計畫本身自應配合修正，爰於第二項明定第二條第一項規定事項修正時，特定非公務機關應配合修正其資通安全維護計畫，並向本會提出。</p> <p>三、資通安全維護計畫除第二項規定之修正外，其他情形之修正，例如特定非公務機關自行修正，為利本會後續稽核，該特定非公務機關亦有向本會提出修正後計畫之義務，爰於第三項予以明定。</p> <p>四、第四項明定資通安全維護計畫不完備時之補正處理程序。</p>
<p>第四條 特定非公務機關應於本會通知之期限內，向本會提出資通安全維護計畫實施情形。</p>	依本法第十六條第三項及第十七條第二項規定，關鍵基礎設施提供者及財團法人應向本會提出資通安全維護計畫實施情形，爰明定本條。
<p>第三章 資通安全維護計畫實施情形之稽核</p>	章名。
<p>第五條 本會應每年擇定特定非公務機關，以現場實地稽核之方式，稽核其資通安全維護計畫實施情形。</p> <p>本會為辦理前項稽核，應訂定稽核計畫，包括稽核小組組成方式、稽核之方式、期間、項目與內容、基準與方法及保密義務等與稽核相關之事項。</p> <p>本會決定前項稽核計畫之基準及項目時，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等因素。</p> <p>本會依第一項規定擇定受稽核之特定非公務機關時，應綜合考量資通安全責任等級、資通安全事件發生之頻率與程度、資通安全演練之成果、受稽核之頻率與結果及其他與資通安全相關之因素。</p>	<p>一、第一項明定本會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。</p> <p>二、本會為實施稽核，於第二項明定稽核計畫之相關規定。</p> <p>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，爰於第三項明定本會於訂定稽核計畫，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。</p> <p>四、為有效利用稽核資源，提升稽核成效，爰於第四項明定本會於訂定稽核計畫，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。</p>
<p>第六條 本會辦理前條第一項之稽核，應於一個月內將稽核計畫以書面通知受稽核之特定非公務機關。</p>	<p>一、為避免本會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</p>

<p>前項特定非公務機關因業務因素或其他正當理由，未能於本會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會申請變更稽核日期。</p> <p>前項申請，除有不可抗力之事由外，以一次為限。</p>	<p>項明定本會應於實際辦理稽核之一個月前，通知受稽核機關。</p> <p>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會申請變更稽核日期，並原則以一次為限，爰為第二項及第三項之規定。</p>
<p>第七條 本會辦理第五條第一項之稽核，於實地稽核前，應先訪談受稽核之特定非公務機關；於實地稽核時，受稽核之特定非公務機關應備妥資通安全維護計畫實施情形之相關說明文件及佐證資料，供現場查閱。</p> <p>前項特定非公務機關有正當理由，未能為前項說明、配合措施或提供資料時，應以書面敘明理由，向本會提出。</p> <p>本會收受前項書面後，應進行審核，依下列規定辦理，並得停止稽核作業之全部或一部：</p> <p>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。</p> <p>二、認無理由者，應要求受稽核機關依第一項規定辦理；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機關。</p>	<p>一、第一項明定本會辦理第五條第一項之稽核時，受稽核機關之配合義務內容，以利本會藉由稽核確認受稽核機關遵循本法之情形。</p> <p>二、受稽核機關如依法律有正當理由，而未能為第一項之說明、配合措施或提供資料，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，向本會提出，俾利本會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，爰為第二項規定。</p> <p>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，本會審認其有無理由及後續處理方式，爰參照行政院訂定之「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。</p>
<p>第八條 本會為辦理第五條第一項之稽核，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。</p> <p>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。</p> <p>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：</p> <p>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。</p> <p>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</p>	<p>一、為使本會得妥適辦理對各不同場次之特定非公務機關資通安全維護計畫實施情形之稽核，爰於第一項明定本會應考量相關因素組成稽核小組。</p> <p>二、考量稽核小組所需具備之知能，爰於第二項明定本會組成稽核小組時，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，以協助本會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。</p> <p>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。</p> <p>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，且本會應與稽核小組成員以書面為約定。</p>

<p>類似之關係。</p> <p>三、本人目前或過去二年內，曾為受稽核之特定非公務機關進行與受稽核項目相關之顧問輔導。</p> <p>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。</p> <p>本會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。</p>	
<p>第九條 本會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之特定非公務機關。</p> <p>前項稽核結果報告之內容，得包括稽核之範圍、缺失或待改善事項、第七條第二項所定受稽核之特定非公務機關未能為說明、配合措施或提供資料之情形與理由及其他相關事項。</p> <p>本會應每年彙整第一項稽核結果報告，提交主管機關備查。</p>	<p>一、第一項明定本會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。</p> <p>二、第二項明定稽核結果報告應記載之內容。</p> <p>三、第三項明定本會每年彙整稽核結果報告，提交主管機關備查。</p>
<p>第十條 受稽核之特定非公務機關之資通安全維護計畫實施情形，經稽核後認有缺失或待改善者，應於收受稽核結果報告後一個月內，向本會提出改善報告。</p> <p>前項特定非公務機關提出改善報告後，應依其缺失或待改善事項之性質及程度，適時以書面提出改善報告之執行情形；本會認有必要時，得要求該特定非公務機關說明或改善。</p>	<p>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會稽核，經發現其資通安全維護計畫實施情形有缺失或待改善者，應向本會提出改善報告。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，俾利本會進行後續之監督。</p> <p>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。</p>
<p>第四章 附則</p>	<p>章名</p>
<p>第十一條 本辦法所定書面，依電子簽章法規定，得以電子文件為之。</p>	<p>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。</p>
<p>第十二條 本辦法自發布日施行。</p>	<p>明定本辦法之施行日期。</p>