

法規名稱：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

發布日期：民國 108 年 04 月 01 日

第一章 總則

第 1 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。

第二章 資通安全維護計畫必要事項及實施情形之提出

第 2 條

- 1 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：
 - 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。
 - 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。
 - 三、通過資通安全管理驗證之執行方案。
- 2 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。

第 3 條

- 1 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。
- 2 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。
- 3 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。
- 4 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。

第 4 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。

第三章 資通安全維護計畫實施情形之稽核

第 5 條

- 1 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。
- 2 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。
- 3 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。

- 4 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。

第 6 條

- 1 本會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之特定非公務機關。
- 2 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。
- 3 前項申請，除有不可抗力之事由外，以一次為限。

第 7 條

- 1 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。
- 2 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。
- 3 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：
 - 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，應要求受稽核之特定非公務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之特定非公務機關。

第 8 條

- 1 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。
- 2 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。
- 3 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、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。
 - 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。
- 4 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。

第 9 條

- 1 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。

- 2 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。
- 3 本會應每年彙整第一項稽核結果報告，提交主管機關備查。

第 10 條

- 1 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。
- 2 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。

第 四 章 附 則

第 11 條

本辦法所定書面，依電子簽章法規定，得以電子文件為之。

第 12 條

本辦法自發布日施行。