

數位發展部所管特定非公務機關資通安全管理作業辦法修正草案總說明

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）於一百一十二年十月四日發布施行，迄今未修正。為配合一百一十四年九月二十四日修正公布之資通安全管理法（以下簡稱本法），及一百一十五年一月五日修正發布之資通安全管理法施行細則、資通安全維護計畫實施情形稽核辦法等法令，並因應實務運作需求，爰擬具本辦法修正草案，其修正要點如下：

- 一、配合本法及其施行細則條次變更，修正本辦法援引條次。（修正條文第一條及第三條）
- 二、定明資通安全維護計畫實施情形應包含之內容。（修正條文第五條）
- 三、修正稽核計畫應包含之內容、訂定稽核計畫及擇定受稽核者之考量因素及資通安全維護計畫實施情形之稽核方式、程序。（修正條文第六條至第八條）
- 四、修正稽核小組成員人數及公務機關代表比例。（修正條文第九條）
- 五、修正稽核結果報告應包含之內容，並刪除現行辦理稽核後，應於次年一月底前彙整稽核結果報告送數位發展部資通安全署之規定。（修正條文第十條）
- 六、定明改善報告應包含之內容，及受稽核者提出改善報告後，應依指定之方式及時間送交改善報告之執行情形。（修正條文第十一條）
- 七、增訂得委任或委託團體辦理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。（修正條文第十二條）
- 八、配合電子簽章法第五條第二項明定書面內容得以電子文件為之，為免重複規範，爰刪除現行條文第十二條。

數位發展部所管特定非公務機關資通安全管理作業辦法修正草案條文對照表

修正條文	現行條文	說明
第一章 總則	第一章 總則	章名未修正。
第一條 本辦法依資通安全管理法（以下簡稱本法） <u>第二十二</u> 條規定訂定之。	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。	本法原第十六條第六項及第十七條第四項合併修正移列為第二十二條，爰配合修正本辦法之授權依據。
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 <u>第二十</u> 條第一項規定指定，經行政院核定者。	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。	本法原第十六條移列為第二十條，爰配合修正。
第二章 資通安全維護計畫必要事項及實施情形之提出	第二章 資通安全維護計畫必要事項及實施情形之提出	章名未修正。
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 <u>第九</u> 條第一項規定辦理。	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。	本法施行細則原第六條移列為第九條，爰配合修正。
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。	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。	本條未修正。

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。 <u>關鍵基礎設施提供者以外之特定非公務機關</u>，經本部依本法<u>第二十一條第二項</u>規定要求提出資通安全維護計畫實施情形者，應於<u>收受</u>本部通知後二個月內，依本部指定之方式提出。 <u>前二項資通安全維護計畫實施情形應依本法施行細則第九條第二項規定辦理。</u> <u>有特殊情形無法依第一項、第二項指定之方式提出者，得經本部同意以其他適當方式為之。</u>	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、第一項未修正。 二、第二項定明適用對象並配合本法原第十七條移列為第二十一條，修正援引條次，另酌作文字修正，以資明確。 三、定明資通安全維護計畫實施情形應包括本法施行細則第九條第一項各款之執行成果及相關說明，爰增訂第三項。 四、考量實務上或有特殊情形無法依指定之方式提出，為兼顧周延及彈性，爰增訂第四項。
第三章 資通安全維護計畫實施情形之稽核	第三章 資通安全維護計畫實施情形之稽核	章名未修正。
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<u>實地稽核或其他適當之方式</u>，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，<u>其內容至少包括稽核依據、稽核目的、稽核範圍、作業期程、稽核小組組成方式、保密義務、受稽核者遴選原則、稽核基</u>	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<u>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。</u>	配合資通安全維護計畫實施情形稽核辦法第五條第一項及第六條規定，爰予修正。

準、稽核方式及項目。 本部<u>訂定前項稽核計畫</u>時，應綜合考量我國資通安全政策、國內外資通安全趨勢、過往稽核計畫之內容與稽核結果，<u>及其他與稽核資源之適當分配或稽核成效相關之因素</u>。 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<u>業務之重要性與機敏性、資通系統之規模及性質、資通安全事件發生之頻率及程度、資通安全演練之成果、歷年受主管機關或本部稽核之頻率及結果或其他與資通安全相關之因素</u>。	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<u>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</u>。	
第七條 本部辦理前條第一項之稽核時，應於一個月以前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。	第七條 本部辦理前條第一項之稽核，應於一個月以前<u>將稽核計畫</u>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、第一項配合資通安全維護計畫實施情形稽核辦法第七條第一項規定，爰予修正。 二、第二項及第三項未修正。
第八條 本部辦理第六條第一項之稽核，得要求受稽核者<u>為資通安全維</u>	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	一、配合資通安全維護計畫實施情形稽核辦法第八條第一項、第二

<u>護計畫實施情形之說明、協力或提出相關之文件、證明資料供稽核小組查閱，並執行下列事項，受稽核者及其所屬人員應予配合：</u> 一、稽核前訪談。 二、<u>實地稽核或其他適當之稽核方式。</u> 受稽核者依法律有正當理由，<u>未能為前項說明、協力或提出資料供稽核小組查閱者</u>，應以書面敘明理由，向本部提出，本部收受書面後，應進行審核。 <u>本部進行前項審核，認有理由時</u>，應將審核之依據及相關資訊記載於稽核結果報告，<u>並得停止稽核作業之全部或一部</u>；<u>認無理由時</u>，應要求受稽核者依第一項規定辦理。<u>經停止稽核作業者</u>，<u>本部得擇期續行辦理</u>，並於十日前以書面通知受稽核者。	維護計畫實施情形、提供相關佐證資料供現場查閱，並<u>配合執行下列事項：</u> 一、稽核前訪談。 二、<u>現場實地稽核。</u> 受稽核者依法律有正當理由，不能為前項說明、提供資料<u>或配合措施時</u>，應以書面敘明理由，向本部提出。 本部收受<u>前項書面後</u>，應進行審核，<u>依下列規定辦理，並得停止稽核作業之全部或一部：</u> 一、<u>認有理由者</u>，應將審核之依據及相關資訊記載於稽核結果報告。 二、<u>認無理由者</u>，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。	項規定，爰予修正第一項、第二項，並將第三項移列至第二項。 二、第三項考量實務執行情形，當受稽核者有正當理由未能為說明，協力或提出資料時，始得停止稽核作業之全部或一部。另配合資通安全維護計畫實施情形稽核辦法第八條第三項規定，整併第一款及第二款，並酌作文字修正。
第九條 本部為辦理第六條第一項之稽核，應依同條第四項<u>所定</u>考量因素，就各受稽核者分別組成<u>三人以上之</u>稽核小組。 <u>本部組成前項稽核小組時</u>，應考量稽核之需求，邀請具備資通安全政策或該次稽核所需之技術、管理、法律或實	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<u>成員三人至七人</u>，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	一、第一項及第三項配合資通安全維護計畫實施情形稽核辦法第九條第一項、第二項及第四項規定，酌作文字修正。 二、為使稽核小組組成人數更為彈性，以利本部得配合實務需要增列小組成員，爰將現行第二項稽核小組成

務專業知識之公務機關代表或專家學者擔任<u>小組成員</u>，其中公務機關代表不得少於全體成員人數之<u>四分之一</u>。 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，與受稽核者或其代表人、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，與受稽核者或其代表人、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、<u>本人</u>目前或過去二年內任職之機關（構）或單位，<u>曾</u>為受稽核者之顧問，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，<u>將對稽核結果之公正性造成影響</u>。 本部應以書面與稽核小組成員約定利益衝	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，<u>本人或任職之機關（構）或單位</u>，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<u>情形</u>。 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	員人數上限七人刪除，並整併至第一項。復考量實務上具備稽核專業、適合擔任稽核小組成員之人員未必屬公務機關人員，調整公務機關代表比例，爰修正第二項。 三、第四項未修正。
--	--	--

突之迴避事項及執行稽核之保密義務。	核之保密義務。	
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者未能為說明、<u>協力或提出資料供稽核小組查閱之情形、理由與同條第三項所定本部審核結果，及其他與稽核相關之必要內容。</u>	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、提供資料或配合措施之情形與理由及其他相關事項。 <u>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。</u>	一、第一項未修正。 二、第二項配合資通安全維護計畫實施情形稽核辦法第十條第二項規定，爰予修正。 三、因本法第二十條第六項及第二十一條第四項就送交稽核結果及改善報告已有明文，無重複規範必要，爰予刪除第三項。
第十一條 受稽核者經發現其資通安全維護計畫實施情形有缺失或待改善者，應於收受稽核結果報告後一個月內，依本法施行細則第六條第一項規定及本部指定之方式，向本部提出改善報告。 受稽核者提出改善報告後，應依<u>本法施行細則第六條第二項規定</u>，提出改善報告之執行情形<u>送交本部</u>。 本部認有必要時，得要求<u>該受稽核者就前二項之改善報告、改善報告之執行情形</u>進行說明或調整。	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<u>依前項規定</u>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、考量現行改善報告內容未臻明確，明定應依本法施行細則第六條第一項規定提出改善報告，爰修正第一項，並酌作文字修正。 二、受稽核者提出改善報告後，應依指定之方式及時間送交改善報告之後續執行情形，爰修正第二項，並酌作文字修正。 三、第三項由現行第二項後段移列修正。為確保監督效能，明定本部得要求受稽核者就改善報告、改善報告之執行情形進行說明或調整。
第四章 附則	第四章 附則	章名未修正。

	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。	一、<u>本條刪除</u>。 二、配合電子簽章法第五條第二項規定，現行條文已無規範必要，爰刪除之。
<u>第十二條</u> 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、<u>法人或團體</u>辦理。 前項受委任或委託之公務機關、<u>法人或團體</u>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。	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、條次變更。 二、考量實務執行情形需求，並參考本法第三十二條規定，增列本部得委任或委託團體辦理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。
<u>第十三條</u> 本辦法自發布日施行。	第十四條 本辦法自發布日施行。	條次變更，內容未修正。