政府領域聯防監控情資回傳作業常見問題

版本：111.12

問題分類

1 適用對象與資通安全責任等級

議題	回應
1.1 特定非公務機關是否納入政府領域聯防監控？	特定非公務機關請依循各領域主管機關與 N-ISAC 規範。
1.2 同時為一般機關與中央目的事業主管機關的雙重身分，如何處理填報？	機關請以一般政府機關身分處理政府領域聯防監控作業；如具備中央目的事業主管機關身分，請依循 N-ISAC 規範。
1.3 財團法人是否需配合執行政府領域聯防監控作業？	單位如非公務機關，請依循各領域主管機關與 N-ISAC 規範。
1.4 機關為 A 級，其下轄機關為 C 級，是否要納入回傳範圍？	A 級機關如有協助轄下 C 級機關執行資安監控業務，建議彙整相關資安防護項目，並回傳資安監控情資。 如 C 級機關自行具有 SOC 機制，也可自行回傳。
1.5 機關原屬 C 級機關，今年升為 B 級機關，因今年沒有編列預算，是否必須於今年建置完成並回傳？	建議機關無論有無 SOC 機制，皆須執行管考系統資安監控填報作業，填寫機關現行防護狀況。後續若無回傳資安監控情資，將列入觀察名單，明年加強觀察。

2 管考系統

議題	回應
2.1 機關資安監控中心收容多台相同型號設備或 AD 之日誌，請問於資安防護列表中只需寫 1 項，還是每一台設備都要寫 1 項？	請依 SOC 收容之設備代號區分，原則上每一設備均有唯一識別之設備代號，每 1 台設備均要填寫 1 項。 多個設備共用一個設備代號，則只需寫 1 項，惟此配置恐造成後續事件觸發時，難以識別實際觸發設備，不建議採行此作法。
2.2 設備代號由機關命名為主或有規則依循填寫？	設備代號無命名規則，請依機關內部命名規則填寫即可，原則上每一設備均有唯一識別之設備代號。
2.3 機關網路採內(向上收整)外(委外)網實體隔離，於管考填報資安監控作業是否只需填寫外網資訊？	機關建置之委外或向上收整架構，如有納入資安監控範圍皆需填寫，中於資安防護項目列表中，填寫相對應機關資安監控中心名稱。若向上集中之應用系統由收整機關代為監控，可填寫系統項目並於機關資安監控中心指定收整機關。

3 聯防監控情資格式與連通測試作業

議題	回應
3.1 單位本身將資安監控業務委外廠商，但不知廠商是否通過連通測試？	通過連通測試之廠商，皆公布於國家資通安全研究院官網聯防監控專區。
3.2 不知道連通測試作業是由機關或資安服務廠商執行？	自行監控之機關，請與國家資通安全研究院進行連通測試作業；如委外資安服務廠商，請機關責成廠商與國家資通安全研究院進行連通測試。
3.3 連通測試作業申請表格需至哪下載？	資安情資回傳連通測試申請單置於國家資通安全研究院官網聯防監控專區。
3.4 從國家資通安全研究院官網下載資安監控單，為甚麼瀏覽器打開是 JSON 格式？	新版資安監控單為 STIX 封裝格式，內容架構為 JSON 格式。

4 聯防監控情資回傳

議題	回應
4.1 機關委外資安服務廠商，執行資安監控業務，廠商將資安監控情資回傳予國家資通安全研究院。此外，機關做尚需辦理甚麼？	機關 108 年 9 月須於管考系統填寫資安監控作業辦理情形，同時責成資安服務廠商做連通測試並回傳監控情資。此外，機關需持續了解委外廠商是否確實回傳資料。
4.2 機關已加入六都的區域資安聯防中心，資安監控情資回傳是要給區域或是政府領域？	● 如公務機關兼具政府領域資安聯防與各區域資安聯防，請依政府領域聯防規定與各區域資安聯防中心規定進行回傳。 ● 六都區域資安聯防中心應依 N-SOC 規範將聯防監控情資回傳予 N-SOC。
4.3 資安監控情資回傳是否有對應的 FTPS 資料夾？	請見國家資通安全研究院官網文件「聯防監控資安情資回傳 STIX 格式規範」，資安監控情資放置於 FTPS 存放目錄位置，請以資安服務廠商或自建機關為單位，資安監控單放置於 incident 目錄；情資分析單放置於 ticket 目錄；監控設備狀況單放置於 status 目錄。
4.4 目前 N-ISAC 情資類型分類與 N-SOC 事件分類並不一致，能否將兩邊類型統一？	N-ISAC 情資交換分類為 5 大類，而 N-SOC 為事件類別，情資與事件類別互不牴觸。
4.5 實務上，攻防演練期間只會接收到攻防演練時程，無法獲得攻防演練資訊，該如何歸類攻防演練類？	事件分類依各機關資安監控中心判斷，如可獲得攻防演練資訊，建議可將其歸類到攻防演練類，國家資通安全研究院也會就所獲得的資訊確認其正確性。
4.6 情資分析單是否要通報？	若資安監控情資確認實屬資安事件，對機關內部造成機密性、完整性與可用性之實質影響，仍須依照通報應變辦法進行通報。