國家資通安全通報應變作業綱要修正規定對照表

103 年 6 月 23 日修訂

章節	修正規定	現行規定	說明
第 1 章 前言	行政院國家資通安全會報(以下簡稱本會報)為有效掌握我國政府機關(構)及公民營事業之資通訊系統遭受破壞、不當使用等資通安全事件(以下簡稱資安事件)，能迅速雙向通報及緊急應變處置，並在最短時間內回復，以確保國家利益與政府之正常運作，特訂定國家資通安全通報應變作業綱要(以下簡稱本綱要)。	行政院國家資通安全會報(以下簡稱本會報)為有效掌握我國政府機關及公民營事業機構之資通訊及網路系統遭受破壞、不當使用等資通安全事件(以下簡稱資安事件)，能迅速雙向通報及緊急應變處置，並在最短時間內回復，以確保國家利益與政府之正常運作，特訂定國家資通安全通報應變作業綱要(以下簡稱本綱要)。	文字酌作修正。
第 2 章 2.1 行政院國家資通安全會報組織架構	圖 1　行政院國家資通安全會報組織架構圖	圖 1　行政院國家資通安全會報組織架構圖	因應行政院組織改造，將國科會修正為科技部、研考會修正為國發會；另，召集人改為科技部部長、稽核服務組改由資安辦主責。
	網際防護體系下之政府資通安全組由資安辦主責，負責規劃、推動政府各項便民資通訊應用服務之安全機制，輔導政府機關資安技術服務、資安防護及應變，統合政府機關資安人力充實及運用，其下包括國防體系分組、電子化政府分組、學術機構分組、經濟事業分組、交通事業分組、財政事務分組、金融服務分組、衛生醫療分組、通訊傳播分組及人力資源分組等10個分組，並成立行政院國家資通安全會報技術服務中心(以下簡稱技術服務中心)，為執行國家資通安全通報應變作業之技術幕僚單位。前揭政府資通安全組下各分組主責機關及轄管業務範圍如下表。	網際防護體系之政府資通安全組由資安辦主責，負責規劃、推動政府各項便民資通訊應用服務之安全機制，輔導政府機關資安技術服務、資安防護及應變，統合政府機關資安人力充實及運用，其下包括國防體系分組、電子化政府分組、學術機構分組、經濟事業分組、交通事業分組、財政事務分組、金融服務分組、衛生醫療分組、通訊傳播分組及人力資源分組等 10 個分組，並成立行政院國家資通安全會報技術服務中心(以下簡稱技術服務中心)，為執行國家資通安全通報應變作業之技術幕僚單位。各分組之主責機關及轄管範圍如下表：	文字酌作修正。

章節	修正規定	現行規定	說明
	政府資通安全組各分組主責機關及轄管範圍表	表1 政府資通安全組各分組主責機關及轄管範圍表	表標題文字酌作修正。
第2章 2.3資安事件影響等級	資安事件影響等級分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。 （一） 4級事件 符合下列任一情形者，屬4級事件： 1. 國家機密資料遭洩漏。 2. 關鍵資訊基礎設施系統或資料遭嚴重竄改。 3. 關鍵資訊基礎設施運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。 （二） 3級事件 符合下列任一情形者，屬3級事件： 1. 密級或敏感資料遭洩漏。 2. 核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改。 3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。 （三） 2級事件 符合下列任一情形者，屬2級事件： 1. 核心業務（含關鍵資訊基礎設施）一般資料遭洩漏。 2. 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄	資安事件影響等級分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。 （一） 4級事件 符合下列任一情形者，屬4級事件： 1. 國家機密資料遭洩漏。 2. 國家重要資訊基礎建設系統或資料遭竄改。 3. 國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。 （二） 3級事件 符合下列任一情形者，屬3級事件： 1. 密級或敏感公務資料遭洩漏。 2. 核心業務系統或資料遭嚴重竄改。 3. 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。 （三） 2級事件 符合下列任一情形者，屬2級事件： 1. 非屬密級或敏感之核心業務資料遭洩漏。 2. 核心業務系統或資料遭輕微竄改。 3. 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。 （四） 1級事件 符合下列任一情形者，屬1級	1. 文字酌作修正。 2. 增加「關鍵資訊基礎設施」在3級事件的判斷標準。

章節	修正規定	現行規定	說明
	改。 3. 非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。 （四） 1級事件 符合下列任一情形者，屬1級事件： 1. 非核心業務一般資料遭洩漏。 2. 非核心業務系統或資料遭輕微竄改。 3. 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。	事件： 1. 非核心業務資料遭洩漏。 2. 非核心業務系統或資料遭竄改。 3. 非核心業務運作遭影響或短暫停頓。	
第3章 3.1各級政府機關（構）	（一） 各級政府機關(構)通報範圍應包含自建或委外之資通訊系統，以及委託民間興建營運後轉移(Build-Operate-Transfer，BOT)之關鍵資訊基礎設施。 （二） 各級政府機關(構)發現資安事件後除應循內部程序上報外，並須於1小時內，至通報應變網站通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或關鍵資訊基礎設施運作，需橫向通知本會報政府資通安全組相關分組。 （三） 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後1小時內，與技術服務中心聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄	（一） 各級政府機關(構)發現資安事件後除應循內部程序上報外，並須於1小時內，至通報應變網站通報登錄資安事件細節、影響等級及支援申請等資訊，並評估該事件是否影響其他政府機關(構)或重要民生設施運作，需橫向通知本會報政府資通安全組相關分組。 （二） 如因網路或電力中斷等事由，致使無法上網填報資安事件，須於發現資安事件後1小時內，與技術服務中心聯繫，先行提供事件細節，待網路通訊恢復正常後，仍須至通報應變網站補登錄通報。 （三） 進行資安事件處理，「4」、「3」級事件須於36小時內完成復原或損害管制；「2」、「1」級事件須於72小時內完成復原或損害管制。	1. 文字酌作修正。 2. 機關之通報範圍應包含自建、委外及BOT案。

章節	修正規定	現行規定	說明
	通報。 （四） 進行資安事件處理，「4」、「3」級事件須於 36 小時內完成復原或損害管制；「2」、「1」級事件須於 72 小時內完成復原或損害管制。 （五） 完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理辦法及完成時間。	（四） 完成資安事件處理後，須至通報應變網站通報結案，並登錄資安事件處理辦法及完成時間。	
第 3 章 3.2 主管機關	（一） 主管機關(資通安全處理小組)在接獲所屬機關(構)通報後，應主動掌握事件狀況、協助所屬機關(構)進行資安事件應變處理，並督導事件處理過程。如資安事件屬「4」、「3」級事件，技術服務中心將主動通知主管機關之資安長及資訊主管。 （二） 主管機關須至通報應變網站審核所屬機關(構)資安事件通報，並評估該事件是否影響其他政府機關(構)或關鍵資訊基礎設施運作以及事件影響等級之合理性，視需要申請技術支援。如資安事件屬「4」、「3」級事件，須於通報後 2 小時內完成審核；「2」、「1」級事件，須於通報後 8 小時內完成審核。 （三） 各級政府機關(構)完成資安事件處理後，至通報應變網站通報結案，如資安事件屬「4」、「3」級事件，主管機關將接獲所屬機關(構)結案申請後，須至通報應變網站審核所屬機關(構)資安事件結案內容，並針對該資安事件填寫所配合辦理或規劃相關作業。	（一） 主管機關(資通安全處理小組)在接獲所屬機關(構)通報後，應主動掌握事件狀況、協助所屬機關(構)進行資安事件應變處理，並督導事件處理過程。如資安事件屬「4」、「3」級事件，技術服務中心將主動通知主管機關之資安長及資訊主管。 （二） 主管機關須至通報應變網站審核所屬機關(構)資安事件通報，並評估該事件是否影響其他政府機關(構)或重要民生設施運作以及事件影響等級之合理性，視需要申請技術支援。如資安事件屬「4」、「3」級事件，須於通報後 2 小時內完成審核；「2」、「1」級事件，須於通報後 8 小時內完成審核。 （三） 各級政府機關(構)完成資安事件處理後，至通報應變網站通報結案，如資安事件屬「4」、「3」級事件，主管機關將接獲所屬機關(構)結案申請後，須至通報應變網站審核所屬機關(構)資安事件結案內容，並針對該資安事件填寫所配合辦理或規劃相關作業。	文字酌作修正。

章節	修正規定	現行規定	說明
第 3 章 3.3 行政院國家資通安全會報	（一） 技術服務中心依據通報機關(構)及其主管機關提供之資訊，評估通報內容及事件等級合理性，並得視需要變更事件等級；如主管機關未能於規定時限內完成通報審核，得逕行複核之。 （二） 主管機關申請技術支援，如資安事件屬「4」、「3」級事件，技術服務中心須於完成複核後 1 小時內，派員協助主管機關處理資安事件；「2」、「1」級事件，技術服務中心須於完成複核後 2 小時內，派員協助主管機關處理資安事件。 （三） 本會報政府資通安全組應彙整各級資安事件，定期提供國家安全會議國家資通安全辦公室；如接獲「4」、「3」級資安事件，應通報國家安全會議國安資訊聯絡辦公室及國家資通安全辦公室，並轉知行政院國土安全辦公室，俾供研析相關因應作為。 （四） 如接獲「4」、「3」級資安事件通報，得視狀況邀集國家安全會議國家資通安全辦公室及相關機關(單位)召開緊急應變會議，並逐級陳報至本會報召集人決定是否召開資安防護會議。	（一） 技術服務中心依據通報機關（構)及其主管機關提供之資訊，評估通報內容及事件等級合理性，並得視需要變更事件等級；如主管機關未能於規定時限內完成通報審核，得逕行複核之。 （二） 主管機關申請技術支援，如資安事件屬「4」、「3」級事件，技術服務中心須於完成複核後 1 小時內，派員協助主管機關處理資安事件；「2」、「1」級事件，技術服務中心須於完成複核後 2 小時內，派員協助主管機關處理資安事件。 （三） 本會報政府資通安全組應彙整各級資安事件，並定期提供國家安全會議國家資通安全辦公室，俾供研析相關因應作為。 （四） 如接獲「4」、「3」級資安事件通報，得視狀況邀集國家安全會議國家資通安全辦公室及相關機關(單位)召開緊急應變會議，並逐級陳報至本會報召集人決定是否召開資安防護會議。	
第 4 章 4.1 各級政府機關(構)	各級政府機關(構)應建立資安事件之事前安全防護、事中緊急應變及事後復原作業之具體機制(含 BOT 之關鍵資訊基礎設施)，至少須包括下列各項： （一） 事前安全防護 1. 應依資訊系統分級作業相關規定，判定資訊系統安全防護等級，並據以落實資安防護基準。	各級政府機關(構)應自行建立資安事件之事前安全防護、事中緊急應變及事後復原作業之具體機制，至少須包含下列各項： （一） 事前安全防護 1. 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。	1. 文字酌作修正。 2. 項次順序調整。

章節	修正規定	現行規定	說明
	2. 應規劃建置資通安全整體防護環境，做好機關(構)及BOT廠商內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。 3. 應訂定災害預防、緊急應變程序、復原計畫等防護措施並定期演練，以建立緊急應變能量。 4. 應依資通安全防護需要，執行入侵偵測、安全檢測及弱點掃描等安全檢測工作，並訂定系統與資料備份管理辦法，以做好事前防禦準備。 5. 應實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。 6. 應保留資安紀錄與備份，如資訊系統屬委外(含BOT)建置管理者，應於合約內要求承商保留相關資安紀錄。 7. 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。 8. 無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予技術服務中心。	2. 應規劃建置資通安全整體防護環境，作好機關內部資料存取控制，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。 3. 應依資通安全防護需要，執行入侵偵測、安全掃描及弱點檢測等安全檢測工作，並制定系統與資料備份管理辦法，以做好事前防禦準備。 4. 應實施安全稽核、網路監控及人員安全管理等機制，以強化資通安全整體防護能力，降低安全威脅及災害損失。 5. 應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。 6. 委外管理機關(構)須於合約內，訂定承商提供相關資安紀錄，並制定資安紀錄備份管理辦法。 7. 應依資訊系統分類分級與鑑別機制，識別資訊系統安全等級，訂定資訊系統相關防護與復原措施。 8. 應每年定期規劃辦理資安認知教育訓練。 9. 各級政府機關(構)無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予技術服務	

章節	修正規定	現行規定	說明
	9. 應建置並保存相關設備之系統日誌。 10. 應每年定期規劃辦理資安認知教育訓練。	中心。 10. 各級政府機關(構)應建置並保存相關設備之系統日誌。	
	(二) 事中緊急應變 1. 應就資安事件發生原因、影響等級、可能影響範圍、可能損失及是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。 2. 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。 3. 查詢通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，以尋求解決方案；如無法解決，應迅速向主管機關或技術服務中心反應，請求提供相關技術支援。 4. 評估資安事件對業務運作造成之衝擊，並進行損害管制。 5. 視資安事件損壞程度，遵循機關(構)及BOT廠商內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。 6. 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。 7. 各級政府機關(構)如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予技術服	(二) 事中緊急應變 1. 應就資安事件發生原因、影響等級、可能影響範圍、可能損失、是否需要支援等項目逐一檢討與處置，並保留被入侵或破壞相關證據。 2. 查詢國家資通安全通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，尋求解決方案。如無法解決，應迅速向主管機關或技術服務中心反應，請求提供相關技術支援。 3. 依訂定之緊急應變程序，實施緊急應變處置，並持續監控與追蹤管制。 4. 視資安事件損壞程度，遵循機關內部備份管理辦法，啟動備援計畫、異地備援或備援中心等應變措施，以防止事件擴大。 5. 評估資安事件對業務運作造成之衝擊，並進行損害管制。 6. 資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工作，以聯繫檢警調單位協助偵查。 7. 各級政府機關(構)如發生重大(「4」、「3」級)資安事件，應主動提供相關設備系統日誌予技術服	1. 文字酌作修正。 2. 項次順序調整。

章節	修正規定	現行規定	說明
	務中心，俾提供相關協助。	務中心，俾提供相關協助。	
	（三） 事後復原 1. 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份及資料復原等相關事宜。 2. 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。 3. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。 4. 資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊，並提送「資通安全處理小組」及本會報政府資通安全組檢討，以強化資通安全防護機制。	（三） 事後復原作業 1. 在執行復原重建工作時，應執行環境重建、系統復原及掃描作業，俟系統正常運作後即進行安全備份、資料復原等相關事宜。 2. 在完成復原重建工作後，應將復原過程之完整紀錄(如資安事件原因分析及檢討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。 3. 全面檢討網路安全措施、修補安全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊情事再度發生，並視需要修訂應變計畫。 4. 資安事件結束後，應彙整事件之歷程概述、損害情形、後續可能影響、應變措施及強化作為等資訊，並提送「資通安全處理小組」及本會報政府資通安全組檢討，以強化資通安全防護機制。	文字酌作修正。

章節	修正規定	現行規定	說明
第 4 章 4.3 行政院國家資通安全會報	**4.3 行政院國家資通安全會報** （一） 當資安事件涉及網路犯罪相關議題時，資安辦應立即協調本會報網際犯罪偵防體系邀集相關機關(單位)組成專案小組協助處理，並於事件結束後，由專案小組陳報處理情形，副知本會報網際防護體系(政府資通安全組)，並要求受害機關(單位)改善。 （二） 當資安事件對資通訊以外之關鍵基礎設施(Critical Infrastructure, CI)造成威脅時，資安辦應立即通知行政院國土安全辦公室啟動相關應辦機制，以控管損害。 （三） 當資安事件對國家安全造成威脅時，資安辦應立即通報國家安全會議國家資通安全辦公室啟動相關應辦機制，以控管損害。	**4.3 行政院國家資通安全會報** （一） 當資安事件涉及網路犯罪相關議題時，資安辦應立即協調本會報網際犯罪偵防體系，邀集相關機關(單位)組成專案小組協助處理，並於事件結束後，由專案小組簽報處理情形，副知本會報網際防護體系(政府資通安全組)，並要求受害機關(單位)改善。 （二） 當資安事件對資通訊以外之關鍵基礎設施(Critical Infrastructure，CI)造成威脅時，資安辦應立即通報行政院國土安全辦公室啟動相關應辦機制，以控管損害。 **（三）** 當資安事件對國家安全造成威脅時，資安辦應立即通報國家安全會議(國家資通安全辦公室)啟動相關應辦機制，以控管損害。	文字酌作修正。
第 5 章 5.1 資通安全會報演練作業	5.1.1 資安攻防演練 （一） 演練目的： 1. 檢測政府機關(構)及轄管關鍵資訊基礎設施之資安防護能力。 2. 強化政府機關(構)在資安事件發生時之緊急應變、系統復原、協調管控等能力。 3. 檢討我國整體資安防護措施，並研討資安防護精進作為。 （二） 一般說明：演練範圍、時間、重點、編組、整備作業、防護作業、攻擊作業、評審監控、獎懲及注意事項，依本會報所訂定政府機關(構)資安演練計畫執行。	5.1.1 資安攻防演練 （一） 演練目的： 1. 檢測政府機關(構)之資安防護能力。 2. 強化政府機關(構)在資安事件發生時之緊急應變、系統復原、協調管控等能力。 3. 檢討我國整體資安防護措施，並研討資安防護精進作為。 （二） 一般說明：演練範圍、時間、重點、編組、整備作業、防護作業、攻擊作業、評審監控、獎懲及注意事項，依本會報所訂定政府機關(構)資安演練計畫執行。	將關鍵資訊基礎設施納入資安攻防演練範圍。
	5.1.2 資通安全通報演練	5.1.2 資通安全通報演練	文字酌作修正。

章節	修正規定	現行規定	說明
	（一） 演練目的： 1. 測試機關(構)資安審核人及聯絡人聯絡管道是否暢通。 2. 檢驗「通報應變網站」所登錄機關(構)資安審核人及聯絡人資料之正確性。 3. 測試各機關(構)於發現資安事件時，是否可正確、快速執行通報作業。 （二） 一般說明：演練範圍、方式、時間、獎懲及注意事項，將由本會報不定期辦理。	（一） 演練目的： 1. 測試機關資安審核人及聯絡人聯絡管道是否暢通。 2. 檢驗「國家資通安全通報應變網站」所登錄機關資安審核人及聯絡人資料之正確性。 3. 測試各機關於發現資安事件時，是否可正確、快速執行通報作業。 （二） 一般說明：演練範圍、方式、時間、獎懲及注意事項，將由本會報不定期辦理。	
第5章5.2資通安全處理小組演練作業	5.2.2 防範惡意電子郵件社交工程演練 （三） 一般說明： 1. 演練對象由資通安全處理小組自行決定，惟主管機關及所屬機關具有公務電子郵件人員，須1/4(含)以上參與演練。 2. 演練實施前須訂定演練計畫，簽奉機關資安長核定。 3. 完成演練作業後，機關應召開「檢討會議」，檢討辦理情形及演練結果；演練報告須經機關資安長核定，並於每次演練完成後1個月內主動送本會報政府資通安全組備查。	5.2.2 防範惡意電子郵件社交工程演練 （三） 一般說明： 1. 演練對象由資通安全處理小組自行決定，惟主管機關及所屬機關具有公務電子郵件人員，須1/4(含)以上參與演練。 2. 演練實施前須訂定演練計畫，簽奉機關資安長核定。 3. 完成演練作業後，須由機關資安長召開「檢討會議」，檢討辦理情形及演練結果，演練報告須經機關資安長核定，並於每次演練完成後1個月內主動送本會報政府資通安全組備查。	
附件	主管機關列表	主管機關列表	因應行政院組織改造，修正附件主管機關列表名單。