國家資通安全通報應變作業綱要修正規定對照表

102 年 9 月 9 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)。 本綱要分為 6 章，除前言外依整體作業、通報作業、應變作業、資安演練作業、獎懲及減責標準等逐項規範或說明。其中整體作業含本會報組織架構、主管機關職掌、資安事件影響等級定義及作業流程等，明確律定於資安事件發生時通報應變作業程序；通報作業含各級政府機關(構)、主管機關及本會報通報作業方式及要求；應變作業含各級政府機關(構)事前安全防護、事中緊急應變、事後復原作業及主管機關應變作業檢討等；資安演練含本會報所辦理及資通安全處理小組應辦理之相關資通安全演練作業，據以檢測各級政府機關(構)資通安全防護及應變管控能力；獎懲及減責標準含提報獎勵標準、懲處規定及減責規定等。 本綱要務請各級政府機關(構)落實執行，俾配合推動提升通報應變時效、健全資安防護能力、深化資安認知及教育等措施，以全面強化政府資安防護機制，確認政府擁有安全、可信賴的資通訊環境。	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)。 本綱要架構，分為整體作業、通報作業、應變作業、資安演練作業、獎懲及減責標準等項目，整體作業項目含本會報組織架構、主管機關職掌、及資安事件影響等級定義及作業流程，明確律定於資安事件發生時通報應變作業程序。 通報作業，含各級政府機關(構)、主管機關、行政院資通安全辦公室、國家資通安全辦公室及本會報通報作業方式及要求；應變作業含事前安全防護、事中緊急應變、事後復原作業及主管機關應變作業檢討之相關項目。 資安演練作業含本會報所辦理相關資通安全演練作業及資通安全處理小組演練作業，據以檢測各級政府機關(構)資通安全防護及應變管控能力；獎懲及改善含提報獎勵標準、懲處規定及建議改善要求。 本綱要可增進本會報確保政府擁有安全、可信賴的資通環境，推動提升通報應變時效、健全資安防護能力、深化資安認知及教育等多項行動方案，逐步落實政府的資安防護機制，以強化各相關機關對資安	文字酌作修正。

章節	修正規定	現行規定	說明
		事件通報應變及管控能力。	
第 2 章 2.1 行政院國家資通安全會報組織架構	本會報負責國家資通訊安全相關事項之政策諮詢審議、協調及推動，其幕僚作業由行政院資通安全辦公室(以下簡稱資安辦)辦理，本會報下設網際防護及網際犯罪偵防等二體系，下設相關組，組織架構如圖 1。	本會報負責國家資通訊安全相關事項之政策協調、聯繫及推動，其幕僚作業由本院資通安全辦公室辦理(以下簡稱資安辦)，會報下設網際防護及網際犯罪偵防等二體系，分別由本院研究發展考核委員會、法務部及內政部共同主辦，下設相關組，組織架構如圖 1。	配合 102 年 1 月 1 日生效之行政院國家資通安全會報設置要點，修正相關文字。
	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	更新為 102 年 1 月 1 日生效之行政院國家資通安全會報組織架構圖。

章節	修正規定	現行規定	說明
	網際防護體系由資安辦主辦，負責整合資安防護資源，推動資安相關政策；網際犯罪偵防體系由法務部及內政部共同主辦，負責防範網路犯罪、維護民眾隱私及建立資通訊基礎建設安全等工作。 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： 表 1　政府資通安全組各分組主責機關及轄管範圍表	本會報網際防護體系(由行政院研究發展考核委員會主責)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、行政機構分組、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 個分組及技術服務中心，各分組之主責機關及轄管範圍如下表。 表 1　網際防護體系分組主責機關及轄管範圍表	1.配合 102 年 1 月 1 日生效之行政院國家資通安全會報設置要點，修正相關文字。 2.修改表 1 內主責機關名稱為全銜，並文字酌作修正。 3.刪除本節部份內容 (含表 2)。

章節	修正規定	現行規定	說明
		本會報網際犯罪體系(由法務部、內政部主責) 負責規劃、推動個資保護及法制推動及防治網路犯罪等資通訊應用服務之安全機制，輔導政府機關個資保護及法制推動服務、預防網路犯罪及偵防業務，統合政府機關法制、偵防人力充實及運用，其下包括個資保護及法制推動組、防治網路犯罪組、資通訊環境安全組，各組之主責機關及轄管範圍如下表。 表 2 各網際犯罪偵防體系主責機關及轄管範圍表	
第 2 章 2.2 主管機關	應由機關之副首長兼任資安長(無副首長者由首長指派)，並設置「資通安全處理小組」，由資安長擔任召集人，負責制定資安事件通報應變作業計畫，執行資通安全預防、危機通報及緊急應變處理相關措施，並納入機關(構)業務永續運作計畫之一部分；同時亦須協助所屬機關(構)之資安事件通報及應變處理作業，主管機關列表詳如附件。	應由機關之副首長兼任資訊安全長(無副首長者由首長指派)，並設置「資通安全處理小組」，由資訊安全長擔任召集人，負責制定資安事件通報應變作業計畫，執行資通安全預防、危機通報及緊急應變處理相關措施，並納入機關(構)業務永續運作計畫之一部分；同時亦須協助所屬機關(構)之資安事件通報及應變處理作業，主管機關列表詳如附件。	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.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。	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。	本節無調整。

章節	修正規定	現行規定	說明
	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。	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2章 2.4通報及應變作業流程	資安事件通報及應變作業流程如圖2所示，相關作業程序請參見「第3章 通報作業」及「第4章 應變作業」 圖 2 資安事件通報及應變作業流程	資安事件通報應變流程如圖2所示，相關作業程序請參見「第3章 通報作業」及「第4章 應變作業」。 圖 2 資安事件通報與應變作業流程	酌修圖2內容並於綱要各項次配合修正。
	各級政府機關(構)通報資安事件或進行結案，以及主管機關審核所屬機關(構)資安事件通報或結案時，均須至國家資通安全通報應變網站(以下簡稱通報應變網站)登錄作業，該網站營運維護、資安事件通報管理、技術諮詢及支援等服務，由本會報委託技術服務中心負責，聯繫資訊如下： （一）網址：https://www.ncert.nat.gov.tw （二）聯絡電話：(02)2733-9922 (24		1.新增通報應變網站聯絡資訊。 2.為建構整體資通安全聯繫網絡，增列資安長及資訊主管。

章節	修正規定	現行規定	說明
	小時專線電話) （三）傳真：(02)2733-1655 （四）電子郵件：service@icst.org.tw 依本網要進行資安事件通報、處理及聯繫等相關作業，各級政府機關(構)須至通報應變網站登錄並定期更新資訊主管及資安聯絡人(至少2位，並以資安專責人員為優先)等相關資訊；倘屬主管機關，則另須登錄並定期更新資安長及資安審核人等相關資訊，以確保資安通報流程之順利運作。		
第3章 3.1各級政府機關(構)	(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	(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，至國家資通安全通報應變網站(https://www.ncert.nat.gov.tw)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，需橫向通知相關應變分組。 (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，與本會報資通安全組聯繫，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。本會報資通安全組聯繫資訊如下： 1.聯絡電話：(02)2733-9922(24小時專線電話) 2.傳真：(02)2733-1655 3.電子郵件：service@icst.org.tw (三)進行資安事件處理，「4」、「3」級事件須於36小時內復原或完成損害管制；「2」、「1」級事件須於72小時內復原或完成	1 刪除第(二)項內容部份文字。 2. 第(三)項文字內容調整為完成復原或損害管制。

章節	修正規定	現行規定	說明
	損害管制。 (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。	損害管制。 (四)完成資安事件處理後，須至國家資通安全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。	

章節	修正規定	現行規定	說明
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。	(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。 (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，視需要向資安辦申請技術支援。如通報事件屬「4」、「3」級事件，須於通報後 1 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)通報應變網站(技術服務中心)接獲通報，不管任何等級應即時通報資安辦。	1.新增通報資安事件如屬「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。 2.主管機關如接獲所屬機關(構)「4」、「3」級資安事件，完成審核時間由1小時調整為 2 小時。 3.如接獲所屬機關(構)「4」、「3」級資安事件結案申請後，新增主管機關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。

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	**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，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。	**3.3 行政院資通安全辦公室** (一)資安辦依據通報機關（構）及其主管機關提供之資訊進行複核，如主管機關未能於規定時限內完成通報審核，資安辦得逕行複核。 (二)主管機關申請技術支援，如通報事件屬「4」、「3」級事件，資安辦須於完成複核後 1 小時內，派員協同技術服務中心人員以協助主管機關處理資安事件；「2」、「1」級事件，資安辦須於完成複核後 2 小時內，視須要協同技術服務中心人員協助主管機關處理資安事件。 (三)「4」、「3」級事件，由資安辦協同國家資通安全辦公室審核該資安事件是否需要變更事件等級，並陳報至本會報召集人，決定是否邀集相關單位召開資安防護會議。 **3.4 國家資通安全辦公室** 國家資通安全辦公室獲得「資安預警情資」經初步研析後，6 小時內會同資安辦督導相關單位成立專案小組，依「國安相關資安事件偵防處理應變作業流程」分析研處並於事件發生後 4 小時內召開資安防護會議。 **3.5 行政院國家資通安全會報** 本會報依據資安辦及國家資通安全辦公室審核提報資安事件，並陳報至本會報召集人，邀集相關單位召開資安防護會議。	考量本會報組織實務運作情形，將本節原 3.3、3.4 及 3.5 合併為 3.3 節行政院國家資通安全會報，並文字酌作修正。

章節	修正規定	現行規定	說明
第 4 章 4.1 各級政府機關(構)	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。 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。	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機制。 （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。 2.應規劃建置資通安全整體防護環境，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，以做好事前防禦準備。 4.應定期實施安全稽核、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，每半年定期實施內部稽核乙次，以儘早發現系統安全弱點並完成修復補強。 6.應對機關內所建置或委外管理等資安相關記紀錄定期提供資安辦。 7.委外管理機關（構）須於合約內，訂定承商提供相關資安記紀錄。	1.為強化資安事件處理能力，檢討修正各級政府機關(構)之應變作業。 2.文字酌作修正。 3.點次變更。 4.刪除第 6 點。 5.新增第 7 至 10 點，重點包括：各機關應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；每年定期規劃辦理資安認知教育訓練；配合建立 SOC 監控情蒐回傳機制，定期回傳予技術服務中心；建置並保存相關設備之系統日誌。

章節	修正規定	現行規定	說明
	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、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務中心，俾提供相關協助。	（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資安辦反應，請求提供相關技術支援。 3.依訂定之緊急應變計畫，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，應做好證據保全工作，以聯繫檢警調單位協助偵查。	1.文字酌作修正。 2.新增第7點。

章節	修正規定	現行規定	說明
	（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。	（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，應彙整事件之處置過程紀錄、解決方案及強化措施等資訊，並提送「資通安全處理小組」及資安辦檢討，以強化資通安全防護機制。	第 4 點文字酌作修正。
第 4 章 4.2 主管機關	主管機關(資通安全處理小組)應於資安事件處理完成後，針對以下項目進行應變作業檢討。 （一）人力資源：檢討執行人員是否充足與適當。 （二）作業程序：檢討人員辦理通報作業的熟悉程度與程序是否適當。 （三）事件處理：檢討人員事件應變處理措施是否適當。 （四）其他：其他須檢討事項。	主管機關(資通安全處理小組)應於資安事件處理完成後，針對以下項目進行應變作業檢討。 （一）人力資源：檢討執行人員是否充足與適當。 （二）作業程序：檢討人員辦理通報作業的熟悉程度與程序是否適當。 （三）事件處理：檢討人員事件應變處理措施是否適當。 （四）其他：其他須檢討事項。	本節無調整。

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。	**4.3 行政院資通安全辦公室** （一）當資安事件造成重大災害時，應依災害防救法規定，請各該災害之「中央災害防救業務主管機關」配合進駐本會報，協助處理重大災害(如發生資安事件擴大至通資訊骨幹中斷、能源輸送損壞、交通運輸系統故障或金融衛生體系癱瘓等)，以降低災損。 （二）當資安事件造成國家安全或重大事故時(如危及國家安全、人民生命或關鍵設施遭到破壞等涉及民、刑事案件，或因電腦犯罪事件而需檢警單位追蹤鑑識、偵查支援等)，應立即依「國家資通安全會報國安相關資安事件偵防處理應變作業流程」協調國家資通安全辦公室、國防部、法務部(調查局)、內政部警政署(刑事警察局)等單位組成專案小組，協助處理資安事件，並於事件結束後由專案小組，簽報處理情形及行文受害單位改善並副知資安辦。 **4.4 國家資通安全辦公室** （一）當接獲資安預警情資(含國防、外交、國安等)，依據「國家資通安全會報國安相關資安事件偵防處理機制」評鑑指標，初步研判涉及國安相關資安事件，立即會同資安辦督導成立專案小組，按「國家資通	1.考量本會報組織實務運作情形，原 4.3、4.4 及 4.5 節合併為 4.3 節行政院國家資通安全會報。 2.當資安事件分別涉及網路犯罪相關議題、對資通訊以外之關鍵基礎設施(Critical Infrastructure，CI)造成威脅或影響國家安全，即由資安辦立即協調或通報本會報網際犯罪偵防體系、行政院國土安全辦公室或國家安全會議(國家資通安全辦公室)查處。

章節	修正規定	現行規定	說明
		安全會報國安相關資安事件偵防處理應變作業流程」辦理。 （二）成立專案小組後，須立即針對各案蒐整相關情資，執行資料分析與研處，簽報處理情形及函知受害單位儘速改善，以完善處置作業順遂。 (三)「國家資通安全會報國安相關資安事件偵防處理機制」評鑑指標：(符合下列指標之一) 1.攻擊來源：是否為有組織、有計畫性的駭客團體所為。 2.受駭單位：是否為重要政府機關(構)。 3.受駭範圍：是否為單一個案或全面性。 4.遭竊資料：是否屬於“密”級以上機敏資料。 5.影響層面：是否影響重大民生事件。 **4.5 行政院國家資通安全會報** 本會報依據資安辦及國家資通安全辦公室提報資訊，將資安事件造成國家安全或重大事故（如危及國家安全、人民生命或關鍵設施遭到破壞等涉及民、刑事案件，或因電腦犯罪事件而需檢警單位追蹤鑑識、偵查支援等處理情形，陳報至本會報召集人。	
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)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、	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、	文字酌作修正

章節	修正規定	現行規定	說明
	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。	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，依本會報年度內所訂定政府機關(構)資安演練計畫執行。	
	5.1.2 資通安全通報演練 （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。	5.1.2 資通安全通報演練 （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，依本會報年度內所訂定之計畫執行。	文字酌作修正
	5.1.3 防範惡意電子郵件社交工程演練 （一）演練目的： 1.為提高人員警覺性以降低社交工程攻擊風險。 2.規範機關自訂社交工程防制目標、舉辦相關資安教育訓練與宣導，以強化公務人員資安意識並檢驗機關宣導社交工程防制成效。 （二）一般說明：演練範圍、總體目標、宣導要點、演練時間、對象、前置作業、結果陳報、作業要點及獎懲事項，將由本會報不定期辦理。	5.1.3 防範惡意電子郵件社交工程演練 （一）演練目的： 1.為提高人員警覺性以降低社交工程攻擊風險。 2.規範機關自訂社交工程防制目標、舉辦相關資安教育訓練與宣導，以強化公務人員資安意識並檢驗機關宣導社交工程防制成效。 （二）一般說明：演練範圍、總體目標、宣導要點、演練時間、對象、前置作業、結果陳報、作業要點及獎懲事項，依本會報年度內所訂定之防範惡意電	文字酌作修正

章節	修正規定	現行規定	說明
		子郵件社交工程施行方案執行。	
	5.1.4 其他演練 配合本會報規劃，不定期辦理資安相關演練。	5.1.4 其他演練 配合資安辦規劃，不定期辦理資安相關演練。	文字酌作修正
第 5 章 5.2 資通安全處理小組演練作業	5.2.1 資通安全通報演練 （一）演練目的：檢驗「資通安全處理小組」及所屬機關(構)之資安通報機制及應變能力。 （二）演練時間：每年辦理 1 次，確實執行日期由各資通安全處理小組自行決定，惟須於每年 9 月底前完成。 （三）一般說明： 1.各資通安全處理小組在本項演練作業中，應分組分工執行各項任務。如規劃組(危機處理分組)負責規劃演練之各種模擬狀況及選出演練單位；管控組(安全預防分組)負責通知參演單位及支援處理作業；督察組(稽核分組)負責保管模擬狀況題庫及登錄各階段演練時間，組織架構如圖 3： 圖 3 資通安全小組組織架構 2.演練計畫應簽奉資通安全處理小組之召集人資安長核定後實施。 3.演練實施前，除應邀集所屬各單位實施作業講習外，亦請與本會報政府資通安全組聯繫。 4.遴選演練對象方式，由各資通安全處理小組之規劃組以無預警隨機方式選取所屬 1/3(含以上)之單位為演練對象。 5.演練前，資通安全處理小組之規劃組需先規劃資安影響等級分	5.2.1 資通安全通報演練 （一）演練目的：檢驗「資通安全處理小組」及所屬機關(構)之資安通報機制及應變能力。 （二）演練時間：每年辦理 1 次，確實執行日期由各資通安全處理小組自行決定，惟須於每年 9 月底前完成。 （三）一般說明： 1.各資通安全處理小組在本項演練作業中，應分組分工執行各項任務。如規劃組(危機處理分組)負責規劃演練之各種模擬狀況及選出演練單位；管控組(安全預防分組)負責通知參演單位及支援處理作業；督察組(稽核分組)負責保管模擬狀況題庫及登錄各階段演練時間，組織架構如下圖： 圖 3　資通安全小組組織架構 2.演練計畫應簽奉資通安全處理小組之召集人(資訊安全長)核定後實施。 3. 演練實施前，除應邀集所屬各單位實施作業講習外，亦請與本會報聯繫。 4.遴選演練對象方式，由各資通安全處理小組之規劃組以無預警隨機方式選取所屬 1/3(含以上)之單位為演練對象。 5.演練前，資通安全處理小組之規劃組需先規劃資安影響等級分	1.明訂資通安全通報演練結果提報期限、對象及方式。 2.酌修圖 3。 3. 文字酌作修正。

章節	修正規定	現行規定	說明
	別為 1、2、3、4 級演練之各種模擬狀況(至少 10 種以上)，用隨機選取方式，分配予所選出之參與演練單位，密封交督察組保管。 6.各種模擬狀況中，可明定該狀況是可由資通安全處理小組支援解決或須由技術服務中心支援解決，以檢驗不同流程之處理方式。 7.演練完成後將「演練成果報告」併「演練時間紀錄表」，於1個月內主動送本會報政府資通安全組備查，並由該組彙整各資通安全處理小組所報成果，視情況邀集相關單位研商辦理獎勵及改善事宜。 8.「演練成果報告」、「演練時間紀錄表」及「支援處理及回覆單」等相關表單請至通報應變網站下載。	別為 1、2、3、4 級演練之各種模擬狀況(至少 10 種以上)，用隨機選取方式，分配予所選出之參與演練單位，密封交督察組保管。 6.各種模擬狀況中，可明訂該狀況是可由資通安全處理小組支援解決或須由資通辦協同技術服務中心支援解決，以檢驗不同流程之處理方式。 7.演練完成後將「演練成果報告」併「演練時間紀錄表」，於2週內送本會報備查，每年 10 月由本會報彙整各資通安全處理小組所報成果，邀集相關單位評選辦理獎勵及改善事宜。 8.「演練成果報告」、「演練時間紀錄表」及「支援處理及回覆單」等相關表單請至國家資通安全通報應變網站(https://www.ncert.nat.gov.tw)下載。	
	5.2.2 防範惡意電子郵件社交工程演練 （一）演練目的：提高「資通安全處理小組」及其所屬機關(構)對社交工程攻擊防制認知。 （二）演練時間：每年不定期至少辦理 2 次，由資通安全處理小組自行規劃及執行，惟須於每年 4 月底前辦理第 1 次演練，並於 9 月底前辦理第 2 次演練。 （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須 1/4(含)以上具有公務電子郵件人員參與演練。	5.2.2 防範惡意電子郵件社交工程演練 （一）演練目的：提高「資通安全處理小組」及其所屬資安責任等級列 A、B 級機關(構)對社交工程防制認知。 （二）演練時間：每年不定期至少辦理 2 次，由資通安全處理小組自行規劃、執行，惟須於每年 4 月底前辦理第 1 次演練、於 9 月底前辦理第 2 次演練。 （三）一般說明： 1.演練對象由資通安全處理小組自行決定，惟主管機關或所屬機關之資安等級列 A、B 者，須 1/4（含）以上具有公務電子郵件人員參與演練。	1.刪除防範惡意電子郵件社交工程演練之對象為資安等級 A、B 級機關之規定。 2.明訂資通安全通報演練結果提報期限、對象及方式。 3.文字酌作修正。

章節	修正規定	現行規定	說明
	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。	2.演練實施前須訂定演練計畫，簽奉機關資訊安全長(CISO)核定。 3.完成演練作業後，須由機關資訊安全長召開「檢討會議」，檢討辦理情形及演練結果，演練報告須經機關資訊安全長核定，並於每年 10 月底前送資安辦彙整。	
第 6 章 6.1 獎勵標準	具以下事蹟之一者，由本會報政府資通安全組主責機關(單位)建議相關機關(構)對所屬人員予以適度之獎勵： (一)所通報之資安事件資料完整且具時效性，足以警示其他機關(構)及早防範，防止資安事件擴大。 (二)完成資安事件處理後，通報結案時所提供解決辦法，可供其他機關(構)及時採用，防止資安事件擴大。 (三)於資安事件通報後，積極辦理相關回復工作，降低對機關(構)影響程度，績效卓著。 (四)提供技術服務中心分析之紀錄，有效預防機關(構)內發生資安事件，並可供其他機關(構)事前應對及預防之用。 (五)積極推動資通安全防護及通報至所屬機關(單位)，績效卓著。	(一)通報之資安事件資料具時效性，足以提醒其他機關（構）及早防範，防止資安事件之擴大。 (二)通報之資安事件資料所提供之解決辦法，可供其他機關（構）使用並具時效者。 (三)於資安事件通報後，積極辦理相關回復工作，降低對機關（構）影響程度，績效顯著者。 (四)提供資安辦分析之記錄，事先預防機關內資安事件發生，並提供他機關事前應對及預防，應從優獎勵。 (五)各級機關積極推動資通安全防護及通報至下屬單位，績效卓著應從優獎勵。	文字酌作修正。
第 6 章 6.2 懲處標準	具以下情事之一者，由本會報政府資通安全組主責機關(單位)建議相關機關(構)視情節輕重對所屬人員予以適度之懲處： (一)通報之資安事件資料，經查明不實。	(一)各級政府機關(構)通報之資安事件資料，經查明如有不實之處，將要求機關(構)內部依法處置。 (二)各受委託資安業者未依程序通	1.文字酌作修正。 2.第(二)項調整至本節末段。

章節	修正規定	現行規定	說明
	(二)未遵循本綱要規定落實資安事件通報應變作業及提供資安紀錄等，致國家或社會受有重大損害時，依法追訴行為人涉及湮滅證據等相關刑事責任；此外，另追究行為人、其主責機關資安長及相關人員之行政責任。 另，各受委託資安業者倘未依程序通報，將建議解除合約。	報，建議解除合約。 (三)未遵循本綱要進行資安預警情資、資安事件通報應變作業及提供資安紀錄等，致使政府或民眾權益損失情形嚴重者，除機關(構)內部依法處置外，亦須依相關法令規章進行處分，如造成國家安全重大危害，該機關(構)應加重處分。	
第 6 章 6.3 減責標準	遵循本綱要規定確實辦理資安事件通報及應變作業並提供資安紀錄，仍致政府或民眾權益受損時，本會報政府資通安全組主責機關(單位)應協助提供資料予相關機關(構)，並建議減輕其責。	遵循本綱要進行資安事件通報與應變作業及提供資安記錄，仍使政府或民眾權益損失時，資安辦或國家資通安全辦公室應提供完整資料予相關單位，並建議減輕其責。	文字酌作修正。
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。