國家資通安全通報應變作業綱要

目　錄

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事件通報應變及管控能力。

第 2 章 整體作業

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。

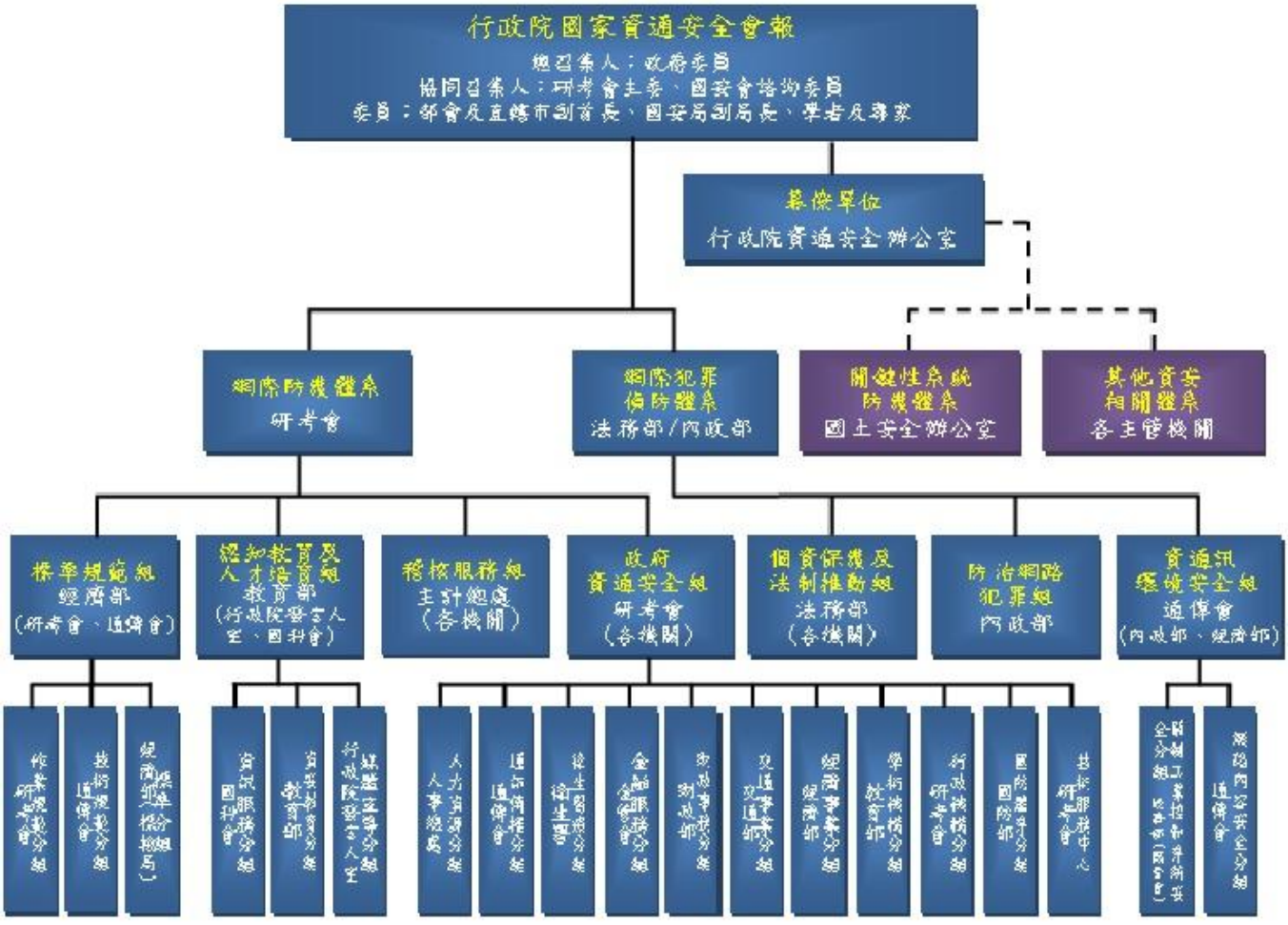

圖 1　行政院國家資通安全會報組織架構圖

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

資通安全分組	主責機關	轄管範圍
國防體系分組	國防部	國防體系
行政機構分組	研考會	行政機關
學術機構分組	教育部	學校及研究機構
經濟事業分組	經濟部	電力、石油、自來水及瓦斯等事業機構
交通事業分組	交通部	郵政及交通運輸等事業機構
財政事務分組	財政部	財稅及關貿等事務機構
金融服務分組	金管會	金融服務業
衛生醫療分組	衛生署	衛生醫療機構
通訊傳播分組	國家通訊傳播委員會	電信及通訊傳播業
人力資源分組	人事行政總處	人力資源相關

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

網際犯罪偵防體系	主責機關	轄管範圍
個資保護及法制推動組	法務部	法務部（各機關）
防治網路犯罪組	內政部	法務部(調查局)、警政署、刑事警察局
通訊環境安全組	國家通訊傳播委員會	通傳會、內政部、經濟部
網路內容安全分組	國家通訊傳播委員會	通傳會
關鍵工業控制系統安全分組	經濟部（國營會）	經濟部(國營會)

2.2 主管機關

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。

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。
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。

2.4 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」。

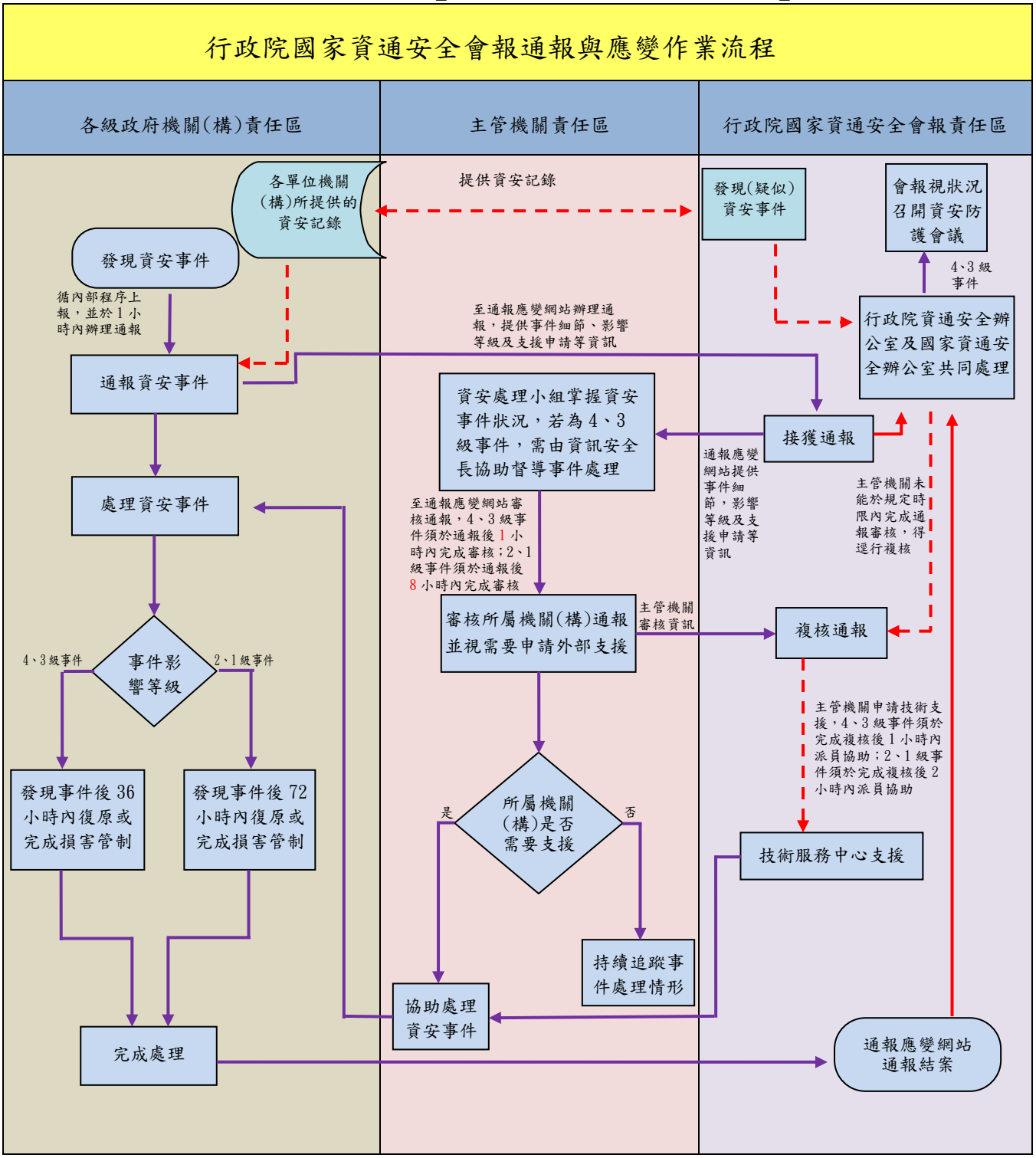

圖 2　資安事件通報與應變作業流程

第 3 章 通報作業

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。

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。

（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。

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。

第 4 章 應變作業

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錄。

（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。

（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。

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。

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 資安演練作業

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、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，依本會報年度內所訂定之計畫執行。

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子郵件社交工程施行方案執行。

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。

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：

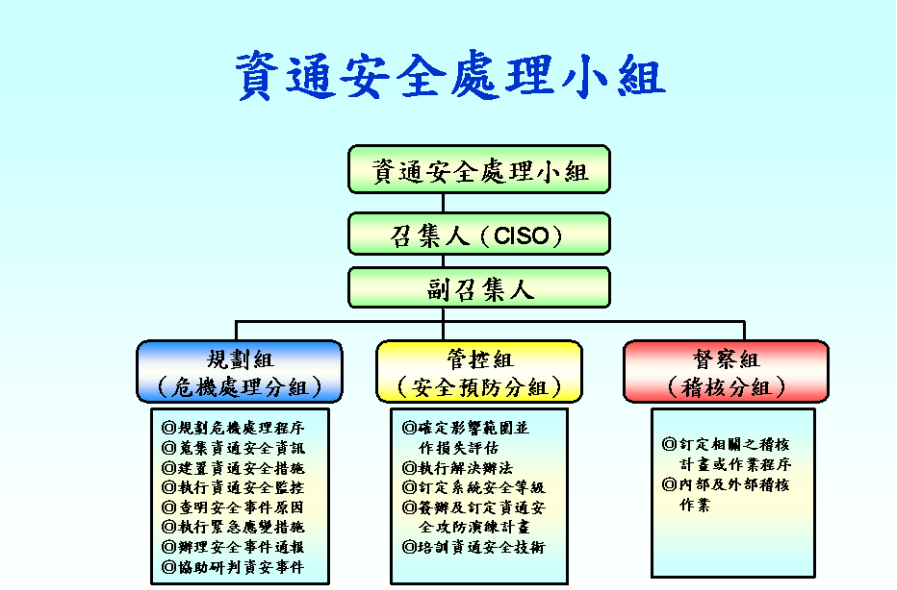

圖 3　資通安全小組組織架構

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。
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 獎懲及減責標準

6.1 獎勵標準

（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。

6.2 懲處標準

（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。

6.3 減責標準

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。

附件　主管機關列表

編號	機關名稱	編號	機關名稱
1	行政院	17	行政院衛生署
2	內政部	18	行政院環境保護署
3	外交部	19	行政院海岸巡防署
4	國防部	20	國立故宮博物院
5	財政部	21	行政院大陸委員會
6	教育部	22	行政院經濟建設委員會
7	法務部	23	行政院國軍退除役官兵輔導委員會
8	經濟部	24	行政院青年輔導委員會
9	交通部	25	行政院原子能委員會
10	文化部	26	行政院國家科學委員會
11	蒙藏委員會	27	行政院研究發展考核委員會
12	僑務委員會	28	行政院農業委員會
13	中央銀行	29	行政院勞工委員會
14	行政院主計總處	30	公平交易委員會
15	行政院人事行政總處	31	行政院公共工程委員會
16	行政院發言人辦公室	32	行政院體育委員會

編號	機關名稱	編號	機關名稱
33	中央選舉委員會	49	彰化縣政府
34	行政院原住民族委員會	50	南投縣政府
35	金融監督管理委員會	51	雲林縣政府
36	國家通訊傳播委員會	52	嘉義縣政府
37	飛航安全調查委員會	53	嘉義市政府
38	客家委員會	54	臺南市政府
39	福建省政府	55	高雄市政府
40	臺灣省政府	56	屏東縣政府
41	基隆市政府	57	宜蘭縣政府
42	新北市政府	58	花蓮縣政府
43	臺北市政府	59	臺東縣政府
44	桃園縣政府	60	澎湖縣政府
45	新竹縣政府	61	金門縣政府
46	新竹市政府	62	福建省連江縣政府
47	苗栗縣政府		
48	臺中市政府		