法務部及所屬機關資通安全事件緊急應變計畫

安全分級：□ 公開 ■ 一般 □ 限閱

文件編號：31602

版次：1.5

施行日期：中華民國 105 年 10 月 日

版本修訂紀錄表

文件版本	修訂日期	修訂內容	修訂單位	修訂人	文件管制員
1.0	98.6.10	修正發布名稱及全文 9 點（原名稱：法務部及所屬機關資通安全事件緊急應變計畫暨作業處理程序）。	二科	陳慶龍	郭俊祥
1.1	102.2.26	一、配合「國家資通安全通報應變作業綱要」之規範，修正通報單位名稱及通報後審查時間。 二、依「國家資通安全現況解析及因應作為」會議結論增訂獎懲標準。	設備網路科	陳慶龍	李國鋒
1.2	103.4.14	配合行政院國家資通安全會報組織調整，修正第一點、第四點、第七點。	設備網路科	陳慶龍	李國鋒
1.3	104.11.28	將文字內容調整成與現實實務作業一致	設備網路科	張景程	李國鋒
1.4	105.4.8	因應國家安全會報技術服務中心組織異動為行政法人國家資通安全科技中心，變更相關文字。	設備網路科	陳慶龍	李國鋒
1.5	105.10	因應行政法人國家資通安全科技中心組織異動為行政院國家資通安全會報技術服務中心，變更相關文字。	設備網路科	陳慶龍	蔡淑蕙

目　錄

一、依據及目的

（一）依行政院國家資通安全會報「國家資通安全通報應變作業綱要」辦理。

（二）目的：為利法務部（以下簡稱本部）及所屬機關於遭遇資通安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保本部及所屬機關各項業務之正常運作，特訂定本計畫。

二、適用對象及時機

（一）適用對象：本部及所屬機關。

（二）適用時機：本部及所屬機關於發生重大資通安全事件或其他災害涉及資通安全事件時，應立即依本計畫辦理。

三、資通安全危機處理組織

（一）為督導本部及所屬機關執行資通安全預防及危機通報、緊急應變處理等相關工作，本部應成立「資通安全處理小組」，負責督導所屬機關執行資通安全預防及危機通報、緊急應變處理等相關工作。

（二）所屬機關為辦理資通安全等相關作業，應成立跨單位之「資訊安全執行小組」，負責推動、協調及督導資訊安全管理事項，並負責資訊安全危機事項之通報及處理事宜。

四、安全防護機制

（一）本部依「行政院及所屬各機關資訊安全管理要點」及「行政院及所屬各機關資訊安全管理規範」，規劃建置資通系統及網路安全整體防護環境，含系統存取控管機制、連線紀錄資料庫、建構防火牆軟硬體、虛擬私人網路(VPN)、病毒掃描機制、入侵偵測系統(IDS)、外部弱點掃描、頻寬管理、系統內部安全漏洞檢測(更新、補強)、儲備必要之備份資料、程式或異地備援、重要文件資料檔案採取加密方式儲存等防護工具或措施。

（二）本部「資通安全處理小組」執行即時偵防、監測預警工作，藉由二十四小時之監測工具（如入侵偵測系統 IDS 等）或行政院國家資通安全會報技術服務中心通告等方式掌握最新的預警訊息，並適時對單位內發布告警及因應處理措施，以控制及降低資通安全事件受損程度。

（三）本部及所屬機關應依「法務部及所屬機關資訊安全政策」各項規定辦理資通安全管理工作。

（四）所屬機關依資通安全防護需要，經洽本部「資通安全處理小組」同意後，可協調行政院國家資通安全會報技術服務中心支援執行入侵偵測、安全掃瞄、漏洞檢測修復等安全體檢工作，以做好事前防禦準備。

五、資通安全事件定義及分類

（一）內部危安事件：發現或疑似遭人為惡意破壞毀損、作業不慎等危安事件。

（二）外力入侵事件：

1. 病毒感染事件。
2. 駭客攻擊或非法入侵事件。

（三）天然災害或重大突發事件：

1. 天然災害：颱風、水災、地震或其他天然災害。
2. 重大突發事件：火災、爆炸、核子事故或其他重大突發事件。

六、資通安全事件等級

（一）「4 級」：符合下列情形之一者：

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」：符合下列情形之一者：

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」：符合下列情形之一者：

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」：符合下列情形之一者：

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。

七、危機通報作業處理程序

（一）本部及所屬機關於確認發生資通安全事件時，應向該機關之「資通安全處理小組」或「資訊安全執行小組」反應，該小組應立即（最遲不得超過一個小時）填報「法務部及所屬機關資通安全事件通報

單」（文件電子檔置於本部內部網站，法務部資訊安全行政規則體系表）傳真本部資通安全處理小組並至國家資通安全通報應變網站（以下簡稱通報應變網站）（https://www.ncert.nat.gov.tw）通報登錄資通安全事件細節、影響等級及支援申請等資訊。

（二）本部及所屬機關於通報資通安全事件時，須如因網路或電力中斷等事由，致使無法上網填報資通安全事件，與行政院國家資通安全會報技術服務中心聯繫，先行提供事件細節，並於網路通訊恢復正常後至通報應變網站補登錄通報。行政院國家資通安全會報技術服務中心聯繫資訊如下：

1. 聯絡電話：(02) 2733-9922 (24 小時專線電話)。
2. 傳真：(02) 2733-1655 。
3. 網址：https：//www.ncert.nat.gov.tw

（三）所屬機關發現疑似資通安全事件，但無法確認是否屬資通安全事件時，可填具「法務部及所屬機關資通安全事件通報單」（勾選協助研判欄位），請求本部協助研判，本部「資通安全處理小組」於確認發生資通安全事件後，立即將研判結果以傳真、電話、或電子郵件方式傳送至該機關之「資訊安全執行小組」據以執行通報程序。

（四）本部「資通安全處理小組」聯絡人於接獲所屬機關之資通安全事件通報或行政院國家資通安全會報技術服務中心之資通安全事件通報後，應至通報應變網站查詢事件細節，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，並視需要向國家資通安全會報申請技術支援。如資通安全事件屬 3 級、4 級事件，應於通報後二小時內完成審核；1 級、2 級事件應於通報後 八小時內完成審核。

（五）本部及所屬機關進行資通安全事件處理，3 級、4 級事件須於三十六小時內復原或完成損害管制；1 級、2 級事件應於七十二小時內復原或完成損害管制。

（六）本部及所屬機關資通安全事件處理完畢，系統恢復正常運作時，應透過「法務部及所屬機關資通安全事件通報單」（勾選解除欄位）以傳真、電話、電子郵件方式或上網將處理情形通報至行政院國家資通安全會報技術服務中心解除事件列管，並以傳真、電話、電子郵件（本部資安聯絡人公佈於內網）方式通報本部「資通安全處理小組」。

（七）本部及所屬機關如遇資通安全事件，危及人員生命或設備遭到破壞等涉及民、刑事案件時，應經洽本部「資通安全處理小組」同意後，立即通報檢調單位請求處理。如引發重大災害時，應向災害防救體系提報，請求支援處理。

（八）如發生災損，有關通報單之災害損失評估內容包括如下：作業影響

情況、是否影響其他政府機關運作、設備或系統損害情況、作業延誤情況、資料受損項目、估算資通訊系統作業及資料回復所需時間、備援中心設備及人員支援狀況等。

（九）本部「資通安全處理小組」於資通安全事件影響等級 1 級及 2 級時，由各分組視其影響程度通報執行秘書立即綜理全盤狀況，並依需要由執行秘書召集各分組及相關單位召開緊急會議；當資通安全等級達到 3 級（含）以上時，由資通安全處理小組執行秘書立即通報召集人（資訊安全長），並即刻召集各分組及相關單位召開緊急應變會議處理全盤。

八、緊急應變作業處理程序

（一）緊急應變優先順序：本部及所屬機關如遇發生重大資通安全事件或其他災害涉及資通安全事件時，有關緊急應變優先順序處理原則，參照「法務部資訊作業營運持續管理計畫」。

（二）資通安全事件分類緊急應變程序

1. 內部危安事件：發現或疑似遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備份資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。
2. 病毒感染事件：病毒入侵後，立即聯絡防毒維護廠商協助掌握電腦病毒感染最新動態，隔離病毒，避免疫情擴散；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。
3. 駭客攻擊或非法入侵事件

（1）發現攻擊或被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。

（2）全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

（3）紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反映。

4. 天然災害或重大突發事件應變程序

（1）如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，或儲存於防火保險櫃等設施內，以利爾後系統重置復原。

（2）如遇資通訊網路系統骨幹（主幹頻寬）中斷事件，應立即聯繫線路租用及網路維護廠商查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

九、復原追蹤鑑識

（一）因資通安全事件受損之本部或所屬機關（以下簡稱受損機關）應速依資訊系統回復作業計畫之災難損害回復處理步驟，實施災後復原重建工作。

（二）受損機關執行災後復原工作，應先檢驗資通安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，以及運轉測試等；並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相關事宜。

（三）當危機解除後，受損機關應將災害應變處置復原過程之完整紀錄（如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）建檔管制，以利爾後查考使用。

（四）受損機關如有需要，應保留事件發生之線索，經洽本部「資通安全處理小組」同意後，向行政院國家資通安全會報技術服務中心、法務部調查局資通安全處、檢警單位申請追蹤鑑識、偵查支援，藉研析稽核紀錄或入侵活動偵測等相關資料，釐清事件發生的原因與責任並找出防護系統之漏洞，尋求補強保護方法以避免事件再度發生。

十、獎懲標準

（一）有下列情事之一者，應為獎勵:

1. 通報之資安事件資料具時效性，足以提醒本部及所屬機關及早防範，防止資安事件之擴大。
2. 通報之資安事件資料所提供之解決辦法，可供本部及所屬機關使用並具時效者。
3. 於資安事件通報後，積極辦理相關回復工作，降低對機關影響程度，績效顯著者。
4. 提供本部分析之紀錄，具事先預防機關內資安事件發生，並提供其他機關事前應對及預防效益者，應從優獎勵。
5. 各機關積極推動資通安全防護及通報作業，績效卓著應從優獎勵。

（二）有下列情事之一者，應為懲處：

1. 本部及所屬機關通報之資安事件資料，經查明如有不實之處，將依法處置。
2. 未遵循本計畫進行資安事件通報、應變作業，致使政府或民眾權益損失情形嚴重者，除本部內部依法處置外，亦須依相關法令規章進行處分。