各政府機關（構）落實資安事件危機處理具體執行方案

壹、目的：

「國家資通安全會報」（以下簡稱本會報）為明確各政府機關（構）作業權責及通報與應變作業流程，特訂定「各政府機關（構）落實資安事件危機處理具體執行方案」以加強資通安全事件之危機通報及緊急應變作業，並協助各單位做好應變措施，以降低資安事件之危害。

貳、具體作法：

為確實掌握各政府機關（構）之資訊及網路系統遭受入侵或不當使用時，能迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害；故有必要策訂一套整體性的危機處理具體執行方案，達成國家資通安全的具體防護目標，確保我國擁有安全、可信賴的資通訊環境，以加速台灣實現高科技服務島的理想，提昇國家競爭力。因此，本會報特提具相關執行作法如下：

一、作業面：

（一）為強化政策擬訂，使資安事件通報與應變處理上作法一致，本會報組織架構已奉行政院

院長核定調整，其中有關「會報組織架構圖」如附件一，「會報各工作組職掌」如附件二，「通報與應變作業流程」如附件三，希望藉由組織的強化，完善資安管理作業。

（二）為使各單位落實執行本會報所律訂之各項作業，各政府機關（構）首長應負該管單位全盤資安成敗之責，以期確實推動，「政府機關首長資通安全作業權責」如附件四。

二、管理面：

（一）組織管理：

1. 在政府基層單位一般缺乏足夠的資訊專業人力情況下，資通安全所能獲得的資源經常有限，因此，各政府機關（構）主管資通安全業務之副首長應負起兼任資訊安全長一職之工作，協助首長做好資安維護的責任制度，方能真正貫徹執行資安的各項要求。

2. 各政府機關（構）應肩負起自身管理及技術上的責任，並強化自我防護作為，建立資安專業制度，培育相關人才，全面提升國家資通安全防護水準。

3. 配合本院訂頒之「建立我國通資訊基礎建

設安全機制計畫」，於不違背預算法前提下，各政府機關(構)在建置資訊系統時，應考量資通安全設施經費及維護費用的需求，資通安全預算應採一定比例方式編列，以確保資訊系統運作安全無虞。

（二）安全控管：

1.資訊委外服務的各政府機關(構)，由於欠缺資安專業人力監督廠商，時而流於放任，因此各政府機關（構）首長應指派專人負責安全管控。在資訊委外服務時，更應要求廠商提供資通安全相關服務，包括電腦主機弱點掃描、漏洞修補、防毒軟體等工作項目。

2.各政府機關（構）對極重要、重要之敏感文件、資料、檔案等之處理，應採取檔案加密方式儲存，並除非常必要之連網外，均兼採實體隔離等防護措施，以防止被侵入破壞、竄改、刪除或未經授權之存取動作。

（三）通報機制：

1.各政府機關（構）發生資安事件時務必通報，絕對不能有「不需要協助就不必通報」

的錯誤心態，而導致資安事件擴大之重大損害。

2. 資通安全通報體系除依循本會報通報應變組「通報與應變作業流程」運作外，於緊急狀況應變或任務需要時，由本會報綜合規劃組負責籌劃運作，處理資通安全危機相關事宜，並落實資通安全事件之危機通報及緊急應變作業。

3. 為確保各政府機關（構）組織功能正常運作，應依據組織風險評估界定，針對遭遇內部危害（如人為破壞）、外力入侵（如病毒感染、駭客攻擊、非法入侵）、天然災害或重大意外（如水災、火災、地震、資通訊網路系統骨幹中斷）等事件，訂定資通安全危機通報緊急應變計畫暨復原處置作業程序。

4. 各政府機關（構）應主動積極建立事前安全防護、事中預警應變、事後復原鑑識等機制，於資訊及網路系統遭受入侵或不當使用時，能作到預先防制、應變處理及事後復原的基本要求。

（四）稽核管考：

1.為了確保國家生存發展，各政府機關（構）應帶頭示範做好資通安全工作，妥善保護政府通資訊系統，提升資通安全管理水準，健全資訊安全管理制度（ISMS），Ａ、Ｂ級單位應積極培育稽核人才，於九十七年底前Ａ級單位應獲得主導稽核證照至少二張，Ｂ級單位應獲得主導稽核證照至少一張，Ａ、Ｂ級單位每年至少執行一次以上內部稽核，並編列預算爭取通過所律定資安範圍之第三者(BSi7799-2/CNS17800)資安管理之認證；Ｃ、Ｄ級單位應有自我完成資通安全檢視作業之能力，確實執行單位內、外稽核之檢核作業，各政府機關（構）應以自身的經驗作為所屬單位的借鏡，推動資訊安全管理制度之施行，以確保政府各級單位能落實推動資通安全工作。

2.配合本會報稽核服務組之年度稽核計畫，對於經常發生資安事件及漏洞之單位，或於演練作業表現較差的單位，稽核服務組應將其納入外部稽核實施外部考核，考核結果除告知受稽核之單位外，應另行通知該單位所屬主管機關，並考量列入年度考

核作業中。

（五）教育認知：

1.由本會報技術服務中心訂定資安認知教育之學程內容及目標，以訓練各政府機關（構）資安之種子人員，並訂定績效指標，加強訓練後之成效追蹤及列管。

2.為提高各政府機關（構）資通安全之危機意識，應持續加強對所屬單位的宣導及推廣，使所屬了解各種可能的資通安全風險，俾能建立資通安全的共識與危機意識。

3.本會報應研訂政府重點機關及重要民生體系單位之風險規劃、風險評估、風險分析、風險處理等資通安全管理制度之政策，持續推動國家重要基礎設施資訊系統之資通安全管理制度，並評估其具體成效，以落實政府各單位之資通安全管理制度。