政府機關（構）資訊安全責任等級分級作業施行計畫

壹、 依據：

「國家資通安全會報」第十五次工作小組會議紀錄事項辦理。

貳、 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）資訊安全責任等級分級作業流程，特訂定「各政府機關（構）資訊安全責任等級分級作業研訂施行計畫」，透過有效的資訊安全管理，來防止資訊受到潛在威脅的破壞，進而全面提升國家資通安全防護水準，以管理手段考量主客觀之形勢，明確律定資安等級之規範。

參、 具體作法：

一、 **政策方向**

(一) **政策：**

建立以管理機制配合技術支援服務，要求各單位建立資訊安全長（CISO）責任制度（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，協助首長落實資安維護的責任制度)，應掌握重點保護標的確實作好資安防護。

(二) **目的：**

為強化政策擬訂，各單位之資安防護需不斷發展，各政府機關（構）應肩負起自身管理及建立資安專業制度，培育相關人才，並透過有效的**資訊安全管理**，針對潛在威脅有效保護資訊，以全面提升國家資通安全防護水準。

(三) **制定：**

為避免混淆及考量使用習慣，各單位仍以由高至低之 A、B、C、D 分級，事件則以由輕至重之 1~4 級區分，因各種標準所採用的評估方式與安全需求不同，故依照每個標準所劃分的安全等級亦有所不同；凡涉及國家安全及民眾權益之**敏感資料及相關重要資訊系統，皆為保護標的物，以防護單位作為區分等級之標準**。

（四）**規劃原則：**

1.以「建立管理機制並配合技術支援服務，要求各單位建立 CISO 責任制度，掌握重點保護標的確實保護」爲政策方向。

2.透過評估各單位的資訊能力、重要性、機敏性以及保護標的來明確區分其資訊安全責任等級。

二、 各政府機關(構)資通安全作業權責：

爲落實政府各資安責任等級區分，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)之資通安全作業權責之相關事項，請參考行政院 2004 年十月二十一日院台科字第 0930090197 號函送「各政府機關(構)落實資安事件危機處理具體執行方案」，各政府機關（構）首長應負該管單位全盤資安成敗之責，以期落實執行成效。

三、 資安等級區分方式：

(一) 政府機關

1. A 級(重要核心)：

（1）公務機關處理具國家安全機密性或重要敏感性之數位資料之中央一、二級機關(如總統府、行政院、考試院、審計部等)。

（2）凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療及重要民生基礎設施等重要機敏系統(如行政院施政跨部會平台、公文交換、稅務電子閘門、自然人憑證管理、刑案資訊整合等系統)。

2. B 級(核心)：

（1）各政府機關(構)具有影響社會秩序、民眾隱私之機敏資料或維運機關 (如部分之中央一、二級機關、各部會之署局單位、各縣市政府、警察局、地方稅捐單位)。

（2）全國或地方凡涉及社會秩序民生體系運作及民眾隱私等機敏系統(如各民生體系運作計費登錄、地政、犯罪、地方稅務查詢等系統)。

3. C 級(重要)：

（1）部分中央一、二級機關(如蒙藏委員會、消保會、體委會等)。

（2）涉及地方縣市社會秩序、人民財產安全之重要資訊維運單位。

（3）各部會之地方性作業單位(如各地區行政執行處)。

（4）氣象作業中心、管理處(如氣象預報中心、地震、海象測報中心)。

（5）各縣市議會、衛生局、文化局等。

4. D 級(一般)

（1）地方鄉、鎮、區公所、代表會、事務所、衛生服務中心、鄉村里民代表會等。

（2）地區性氣象站(如台北、新竹、台中、高雄、宜蘭、花蓮及台東氣象站)。

(二) **學研機關(構)**：

1. A 級(重要核心)：

（1）負責教育政策審定單位(如教育部等)。

（2）凡涉及各相關部會委託研究具國家安全機密性或重要敏感性之數位資料之執行單位。

（3）教學醫院。

2. B 級(核心)：

（1）凡涉及社會秩序運作及民眾隱私等機敏系統之學研機構。

（2）各大學(含科技大學)。

（3）台灣學術網路各區域網路中心暨各縣市教育網路中心。

3. C 級(重要)：

各技術學院及專科學校。

4. D 級(一般)：

各高中職(含)以下學校。

(三) **各事業分組**：

1. A 級(重要核心)：

事業(一)電力部份之核能發電廠、電力調度處、資訊系統處；自來水部份之省、市級自來水單位其資訊人員 40 人以上；石油部份之總公司、油品行銷事業部、天然氣事業部等其資訊人員 40 人以上。

事業(二)通信部份之中華電信數據分公司；郵政部份之中華郵政公司其資訊人員 100 人以上。

事業(三-1)財政部份之政策單位、總行其資訊人員 100 人以上。

事業(三-2)金管部份之政策單位、總行其資訊人員 100 人以上。

事業(四）醫院部份之醫學中心其資訊人員 30 人以上。

2. B 級(核心)：

事業(一)電力部份之火力發電廠、資料處裡中心、PC400 部及伺服器 30 部以上；自來水部份之管理處、營運所、水廠其資訊人員２0 人以上；石油部份之探勘事業部、煉油廠、天然氣；糖業部份之總公司資訊人員 30 人（含）以上；綜合部份之資訊人員 20 人（含）以上。

事業(二)通信部份之中華電信公司分公司、所其資訊人員 10 人（含）以上；鐵路管理局；船舶部份之各港務局、工程處；郵政部份之中華郵政各地郵局、投遞中心。

事業(三-1)財政部份之事業機構其資訊人員 50 人（含）以上。

事業(三-2)金管部份之事業機構其資訊人員 50 人（含）以上。

事業(四）醫院部份之區域醫院其資訊人員 5 人（含）以上。

3. C 級(重要)：

事業(一)電力部份之火水力發電廠、區營業處、總處、工程單位、PC100 部及伺服器 5 部以上；自來水部份之管理處、營運所、水廠資訊人員１0 人以上；石油部份之事業部、儲運處、營業處、管理處；糖業部份之各糖廠資訊人員 10 人（含）以上；綜合部份之委員會、公司、局、廠處及中國造船公司。

事業(二)通信部份之中華電信各營運處、研究所-分所 。

事業(三-1)財政部份之事業機構其資訊人員 20 人(含)以上。

事業(三-2)金管部份之政策單位、總行其資訊人員 20 人(含)以上。

事業(四）醫院部份之各地區醫院。

4. D 級(一般)：

事業(一)電力部份之火水力發電廠、區營業處、總處、工程單位

；自來水部份之管理處、營運所、水廠；石油部份之事業部、儲運處、營業處、管理處；糖業部份之營業處、所、訓練中心、服務處、工程處；綜合部份之分廠。

事業(二)通信部份之中華電信各地區服務中心；鐵路局部份之各地收費站、機務段、票務中心。

事業(三-1)財政部份之政策單位、總行其資訊人員 10 人(含)以上。

事業(三-2)金管部份之政策單位、總行其資訊人員 10 人(含)以上。

事業(四）醫院部份之其他醫院。

(四) **其他：**在資訊資產價值分類內容之區分

1. A 級(重要核心)：違反資訊安全保護政策，會對**國家安全**之重要機敏資訊或系統等造成工作營運停頓或嚴重之損害，影響**業務推動持續一個月(含)以上**之損害，有極高度潛在影響等級。
2. B 級(核心)：違反資訊安全保護政策，會對**社會秩序、民生體系運作及民眾隱私**之機敏資訊或系統，影響業務推動**持續一星期(含)以上**之損害，有高度潛在影響等級。
3. C 級(重要)：違反資訊安全保護政策，會對**地方縣市級之社會秩序、人民生命財產**之重要資訊或系統，影響業務推動**持續一天(含)**以上之損害，有中度潛在影響等級。
4. D 級(一般)：違反資訊安全保護政策，造成意外的事件不影響業務工作或營運，爲低度潛在影響等級。
5. 本次調整含蓋面更爲廣泛除行政機關外亦將協調其他機關配合參考辦理，使未來政府資安防護能更有效地全面提昇，各政府主責機關應負責本身及所屬資安防護，以建立 CISO 責任制度。

四、 各類資安系統等級應執行之工作事項：

作業內容 名稱 等級	防禦機制強度	防護縱深	ISMS 推動作業	稽核方式	資安教育訓練(主官、主管、技術、一般)	專業證照
A 級	強度等級 4(註一)	NSOC 直接防護/自建 SOC、IDS、防火牆、防毒	96 年通過第三者認証(註二)	每年至少執行二次內稽	每年至少（4,6,18,4 小時）	96 年資安專業鑑定二張(註三)
B 級	強度等級 3	SOC (Optional)、IDS、防火牆防毒	97 年通過第三者認証	每年至少執行一次內稽	每年至少(4,6,16,4 小時)	96 年資安專業鑑定一張
C 級	強度等級 2	IDS,防火牆防 毒	各單位自行成立推動小組規劃作業	自我檢視	每年至少(2,6,12,4 小時)	資安專業訓練
D 級	強度等級 1	防火牆防 毒	推動 ISMS 觀念宣導	自我檢視	每年至少(1,4,8,2 小時)	資安專業訓練

各單位仍需遵行政院及所屬各機關資訊安全管理規範另行政院研考會提供之教育訓練詳如註四；註一二三四說明如後

註一：資訊安全機制強度等級(Strength Mechanism Level，簡稱 SML)

強度等級 1	經由良好的資訊安全作業可達成的基本強度，用以防衛不複雜的威脅，應能保護低價的資訊資產。
強度等級 2	中等強度，可以抵抗諸如個人發動之攻擊活動的複雜威脅，能夠保護中等價值的資訊資產。
強度等級 3	高強度，用以防禦來自駭客組織的威脅，能夠保護高價值的資訊資產。
強度等級 4	極高強度，用以防禦來自國家級的威脅，能夠保護極高價值的資訊資產。

註二： ISMS 推動作業之範圍

以部門別定義	將部門資訊及業務定爲 ISMS 建置範圍(核心業務必須已涵蓋於所選定之部門內)，例如: 信用卡中心的核心業務爲核卡、發卡及相關後續服務, 其達成核心業務服務所依賴之關鍵資產可能包括: 核卡發卡電腦系統、客戶資料庫 、參與人員等，其範圍包含業務部、核卡部、發卡部、資訊部 。
以系統別定義	將與此系統業務有關之人員或部門全部納入，其範圍應涵蓋要保護之核心業務服務及所依賴之關鍵資產。
以產品/業務別定義	例如：以現金卡爲 ISMS 範圍,則相關牽涉此業務之活動、人員或部門便須納入 ISMS 範圍,此方式適合資源有限或分階段導入 ISMS 之組織。
以實體區域定義	以某機關或大樓(某樓層)爲 ISMS 建置範圍，此種定義方式應將此區域內所有系統業務有關之人員或部門全部納入，此方式適用於業務明確,且可於定義之區域內完全獨立作業者 。

註三：

資安專業證照獲得說明：資安專業證照是以獲得國內外第三者之認驗證單位頒發之證照，可分成特定產品與獨立證照二類，本會報係採用後者，因與廠商、產品無關，涵蓋面較廣，較具中立性，例如資安管理類之 BS7799LA、CISSP(電腦資訊系統安全專業証照)；資安技術類如從事駭客防護之 CEH(認證道德駭客)或從事網路鑑識工作之 GCFA(鑑識分析者)等相關證照證照。

註四：行政院研考會提供資安教育訓練：

1. 資訊安全管理系統主導稽核員訓練（對象：A、B 級機關，時數：40 小時）。
2. 資訊安全管理系統建置訓練（對象：A、B 級機關，時數：40 小時）。
3. 資通安全技術訓練（對象：A 級機關）：

(1) 資訊安全概論（時數：21 小時）。

(2) 通訊網路安全技術（時數：24 小時）。

(3) 系統安全技術（時數：30 小時）。

(4) 密碼學原理與應用（時數：18 小時）。

4. 警示系統教育訓練（對象：A、B 級機關，時數：3 小時）。
5. 弱點掃瞄教育訓練（對象：A、B 級機關，時數：6 小時）。
6. 政府資通安全技術研討會（對象：A、B 級機關，時數：3 小時）。
7. 國家資通安全事件通報應變機制說明會（對象：A、B、C、D 級機關，時數：3 小時）
8. e-learning 資安訓練（對象：A、B、C、D 級機關，時數：30 小時）。

五、資安等級分級修訂推動時程表

（一）資安等級分級修訂規範訂定自 94 年 1 月至 94 年 7 月止。

（二）資安等級分級修訂規範之宣導講習自 94 年 7 月至 94 年 9 月止。

（三)自 94 年 10 月至 94 年 11 月止,由各主管機關審核彙整提報修訂後其(含)所屬機關(構)資安等級。

（四）訂定各單位資安等級登錄與核定於 94 年 12 月。

（五）資安等級分級修訂規範預定於 95 年 1 月正式施行。