立法院議案關係文書 （中華民國41年9月起編號）
中華民國106年9月20日印發

院總第 1570 號　委員提案第 21026 號

案由：本院委員余宛如、鍾佳濱等 18 人，因積極推動我國資通安全，除行政院現已實施之各項措施外，尚須建構一套完整資安治理架構，以統整資安政策法令，提供資安防護標準及資安最低必要控制，並透過政府採購帶動資安產業，協助市場建立資安解決方案，爰提出「資通安全法」草案。是否有當？敬請公決。

說明：

一、資通安全之重要性已無庸贅述，反倒是在制定「資通安全法」之前，首先要確立幾個前提：

1. 沒有 100%的資通訊安全，100%的資通訊安全只存在於完全封閉的體系，在這種體系之中，資通訊對於開放社會無任何積極意義，也無須立法管制。規範資通安全，首重正視風險，方能管理風險。
2. 因此，資通訊安全強調的是最大比較利益，將有限資通防護資源投注於對於資通安全影響最大的地方，以求得最大防護效果。
3. 在開放社會中，資通訊防護能量最強大者有二：民間資通安全專業服務提供者以及軍方。如何整合這二大動能，使其各自發揮最大效能，對於資安政策之能否有效，實具有決定性的影響。
4. 資安防護工作的推動義務，依據被防護對象遭受攻擊時，對於資通訊體系的完整有效性，以及開放社會的安定秩序的影響程度，呈現「光譜式」的強度模式。影響越大者，推動義務越高，反之亦然。
5. 資安作業絕非僅限於「軟體之間的戰爭」，而是一整套「政策、原則、標準、指引、指令」的綿密鋪陳（參考 FISMA 之定義）。
6. 資安作業是一套龐大的分工合作體系，因此，精準的治理架構是決定資安作業能否有效的最重要關鍵。

二、國內現存資通安全法相關草案總共有行政院版、陳亭妃委員版，及時代力量黨團版「資通

安全管理法」計三個版本，三個版本都是以美國《聯邦資訊安全現代化法》（Federal Information Security Modernization Act，簡稱 FISMA）做為範本。而 FISMA 其實緊扣著國際標準 ISO 27001，差別之處在於 ISO 的目的在於提供標準，為了實踐 ISO 標準，各國會考慮其特殊國情佈局其人力物力，而一國之規劃是否能夠達成其國家資源與政策目標之間的最適均衡，是評價該國資安政策及立法設計是否良好的依據。

三、FISMA 之成為國內現存三個版本的參考架構，其因在於美國在公共政策規劃上採取嚴謹的政策開發程序，佐以實作經驗的反覆探討，且該法於 2002 年完成立法以來，已經經過 2012 年及 2014 年二次修正，針對實務中所發現的不足之處予以更新。我國因在公共政策規劃上向來投資不足，無法自行開發如該法一般嚴謹的法律，因此，借鏡先進國家經驗，是後進國家成本效益最高的立法捷徑。唯仍須注意者，在於借鏡時仍應注意是否能夠達成我國國家資源與政策目標之間的最適均衡，斷不可一味照抄，或引喻失義，否則大鞋小腳，畫虎類犬，仍非良好公共政策設計之所應為。

四、然經檢視行政院版之規劃，令人捏一把冷汗，僅以作用法之第一核心要項「主管機關」之設計而論，便已見出不妥適之處。FISMA 所設計的組織架構包含以下數個部分，詳如表一：

表一　FISMA 所設計的資安組織架構

業　務　性　質	單　位
資安防護標準之制訂	NIST（國家標準技術研究所）
政策制訂及業務監督	1. 國土安全部部長 2. 國家情報總監
政策執行單位	各級行政單位依規模大小分設資安長或資安工作人員
技術支援單位	聯邦資安事件中心
稽核單位	檢察總署，或總署指派之獨立外部稽核人員
上級監督或業務協調	國會、國家情報總監、國土安全部部長、政府改革委員會、國土安全委員會、參議院科學委員會、參議院國土安全暨政府事務委員會、參議院商業科學暨交通委員會、國會撥款委員會、審計總長、執法機關、檢察總長及總法律顧問辦公室、總統指派處理國安系統問題的辦公室、國會重大事件委員會、任何依法成立或由總統指揮的機關（構）

製表：立法委員余宛如辦公室

權責分工，清清楚楚。我國雖因政府規模較小，未必可以照本宣科，但必要之分權分工仍應釐清，尤其 report line 事涉指揮體系之統一，若含糊無可辨識，將於嚴重或鉅量資安

攻擊事件發生時，陷入指揮調度困難。

五、在行政院版「資通安全管理法草案」中，非常特殊的是並沒有看到主管機關的設定，而是採用模糊的「政府」（第三條）、「行政院」（第四至第七條）、「公務機關」（第八至第十四條）及「中央目的事業主管機關或直轄市、縣（市）政府」（第十五條至第二十一條）這樣的架構，依據這些條文，上述四種「主管機關」的職責如表二：

表二　行政院版「資通安全管理法草案」主管機關職責表

機　關　類　型	職　責
政府	1. 資通安全專業人才之培育 2. 資通安全科技之研發、整合、應用、產學合作及國際交流之推動 3. 資通安全產業之發展及推動 4. 資通安全軟硬體技術規範、相關服務與審驗機制之發展及推動
行政院	1. 規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護、定期公布國家資通安全情勢報告及資通安全發展方案 2. 委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務 3. 訂定資通安全責任等級之分級及相關辦法、稽核非公務機關之資通安全維護計畫實施情形 4. 建立資通安全情資分享機制 5. 公告重大資通安全事件相關必要內容及因應措施
公務機關	1. 訂定、修正及實施資通安全維護計畫 2. 置資通安全長 3. 每年向上級或監督機關提出資通安全維護計畫實施情形 4. 稽核其所屬或監督機關之資通安全維護計畫實施情形 5. 訂定通報及應變機制 6. 獎勵資通安全維護績效優良者
中央目的事業主管機關或直轄市、縣（市）政府	1. 指定關鍵基礎設施報行政院核定 2. 稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形 3. 接受關鍵基礎設施提供者之資通安全維護計畫缺失改善報告 4. 要求非關鍵基礎設施提供者之非公務機關提出資通安全維護計畫 5. 稽核非關鍵基礎設施提供者之非公務機關資通安全維護計畫實施情形，並限期要求改善 6. 公告重大資通安全事件相關必要內容及因應措施 7. 派員攜帶執行職務證明文件進入非公務機關場所檢查 8. 罰則之執行

製表 立法委員余宛如辦公室

僅從主管機關之設計便可以看出台美二種設計之差異，從「課責性」的角度而論，FISMA 的分工清清楚楚，我國《資通安全管理法草案》的分工有不少問題。

六、即以「政府」而言，依據憲法的設計，中央政府採五院制，莫非每一院都肩負「資通安全專業人才培育」、「資通安全科技研發、整合、應用、產學合作及國際交流推動」、「資通安全產業發展」、「資通安全軟硬體技術規範、相關服務與審驗機制之發展及推動」的義務？何況政府還包括地方政府？

七、「行政院」或許比較清楚，因為行政院設有資安處，可以由該單位代表行政院執行相關業務，可是資安處的預算、人力及專業度有龐大到可以執行那麼多業務嗎？FISMA 的設計中將「資安防護標準之制訂」、「技術支援單位」、「稽核單位」分由「NIST」、「聯邦資安事件中心」及「檢察總署」擔任，既分工又分權，行政院版《資通安全管理法草案》將這四大功能攬於資安處，分工、事權不清，且資安處將因此和經濟部標準檢驗局分工不清，因為目前任何資通訊設備都有可能內建資安軟體，試問應由行政院資安處或是標檢局來把關防護標準？

八、還有一個隱藏的議題，就是行政院國家資通安全會報技術服務中心。立《資通安全管理法》有很大一部份原因，是替技服中心的合法性解套。但是有一個技術性問題，行政院版將辦理資通安全整體防護、國際交流合作及其他資通安全相關事務委託給法人或團體，所委託事項包含很大的公權力行使，且涉及保密義務，絕對不適合採用逐年招標的方式辦理委託，以免業務斷斷續續。雖然大家都知道這一條是為技服中心所量身訂製，但是既然可以委託技服中心，其他法人（例如工研院、國家實驗研究院等，甚至中華電信、趨勢科技等私法人）或是團體具不具備接受委託資格呢？如果技服中心是長期委託，且委託事項有高於一般委託案件的代行公權力義務，就應該讓受委託機構入法，比照聯邦資安事件中心之入 FISMA，或者是比照英國設立 FCA 或是 OFCOM 這種 Authority 的合法流程；同時其代行公權力的部分也應該要入法，權力義務交代清楚為宜。

九、行政院版對於「公務機關」的規範，跟 FISMA 對於政策執行單位的規範差不多，這一部份較無問題。比較有問題的地方是「中央目的事業主管機關或直轄市、縣（市）政府」，它們可以：

1. 指定關鍵基礎設施報行政院核定。

2. 稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。

3. 接受關鍵基礎設施提供者之資通安全維護計畫缺失改善報告。

4. 要求非關鍵基礎設施提供者之非公務機關提出資通安全維護計畫。

5. 稽核非關鍵基礎設施提供者之非公務機關資通安全維護計畫實施情形，並限期要求改善

。

6. 公告重大資通安全事件相關必要內容及因應措施。

7. 派員攜帶執行職務證明文件進入非公務機關場所檢查。

8. 罰則的執行。

其權力與政策正當性嚴重不對稱。須知，「中央目的事業主管機關」是目的事業的主管機關，並非資安主管機關，比方說，公路總局是公路主管機關，但是公路總局擁有資安專業嗎？怎麼能讓目的事業主管機關或地方政府來指定關鍵基礎設施，再由行政院核定呢？如果指定方和核定方意見不一時，請問該怎麼辦？如果有指定方不願指定，但是核定方認為確有必要者，依據行政院版草案將無法發動核定。如果發生行政爭訟，由哪一方來擔任訴訟人？國賠時由哪一方擔任賠償方？還有，一定要搞到這麼複雜嗎？從 FISMA 及美國總統政策指引 PPD—21「關鍵基礎設施之安全及復原 Critical Infrastructure Security and Resilience」所規範者觀之，關鍵基礎設施的指定者，就是資安作業的政策制訂及業務監督者，是不是比較合理？

十、因此，必須要有一部起碼可以釐清各單位之權責的「資通安全法」草案用以修正目前行政院版機關權責不明確的問題，否則一旦實施，問題將會層出不窮。

十一、至於資安法應該具備哪些內容？先檢視 FISMA 2014 所設計的資安運作方式，大致分為以下數個核心要素，詳如表三：

表三　國 2014「聯邦資訊安全現代化法」（Federal Information Security Modernization Act，FISMA）核心要素及內容表

要　　素	內　　容
防護目標及標的物、威脅種類	1. 目標：資訊系統的完整性、機密性及可用性 2. 標的物：資訊、資訊系統及關鍵基礎設施 3. 威脅種類：未經授權的存取、利用、揭露、干擾、修改、毀壞
組織架構	見表一
資安防護業務內容	1. 政策制訂 2. 各機關資安政策之整合與協調 3. 資安事件通報 4. 年度資安報告 5. 緊急資安狀態緩解 6. 操作支援及技術支援 7. 聯邦資安事件中心之運作 8. 編輯並分析各機關之資安資料（data）

	9. 資安系統的弱點評估 10. 確保資安管理與機關的戰略、運作、計畫及預算流程整合一致 11. 定期測試及評價 12. 人員訓練：含資安人員及一般人員
年度報告	向國會、國家情報總監、國土安全部部長、政府改革委員會、國土安全委員會、參議院科學委員會、參議院國土安全暨政府事務委員會、參議院商業科學暨交通委員會、國會撥款委員會、審計總長提報年度資安政策實施狀況
資安通報	1. 聯邦資安中心 2. 執法機關、檢察總長及總法律顧問辦公室 3. 總統指派處理國安系統問題的辦公室 4. 國會重大事件委員會 5. 任何依法成立或由總統指揮的機關（構）
獨立稽核	檢察總署，或總署指派之獨立外部稽核人員為之
聯邦資安事件中心	1. 技術協助 2. 編輯及分析威脅資安事件之情資 3. 提供機關資安威脅及弱點的相關情資 4. 與 NIST 共同
利害關係人	1. 機關直屬資安人員 2. 機關合約包商 3. 機關委任其他實體代為運作資安業務者

製表：立法委員余宛如辦公室

這是一套基於 ISO 27001 標準，且經過「實作→檢驗→修正」後的實戰制度；且包含我國立法例應具備之「立法目的」、「名詞定義」、「組織架構」、「業務範疇」、「業務推動」、「考績稽核」、「利害關係人」等方方面面，實已具足。

十二、然需注意之處有二：

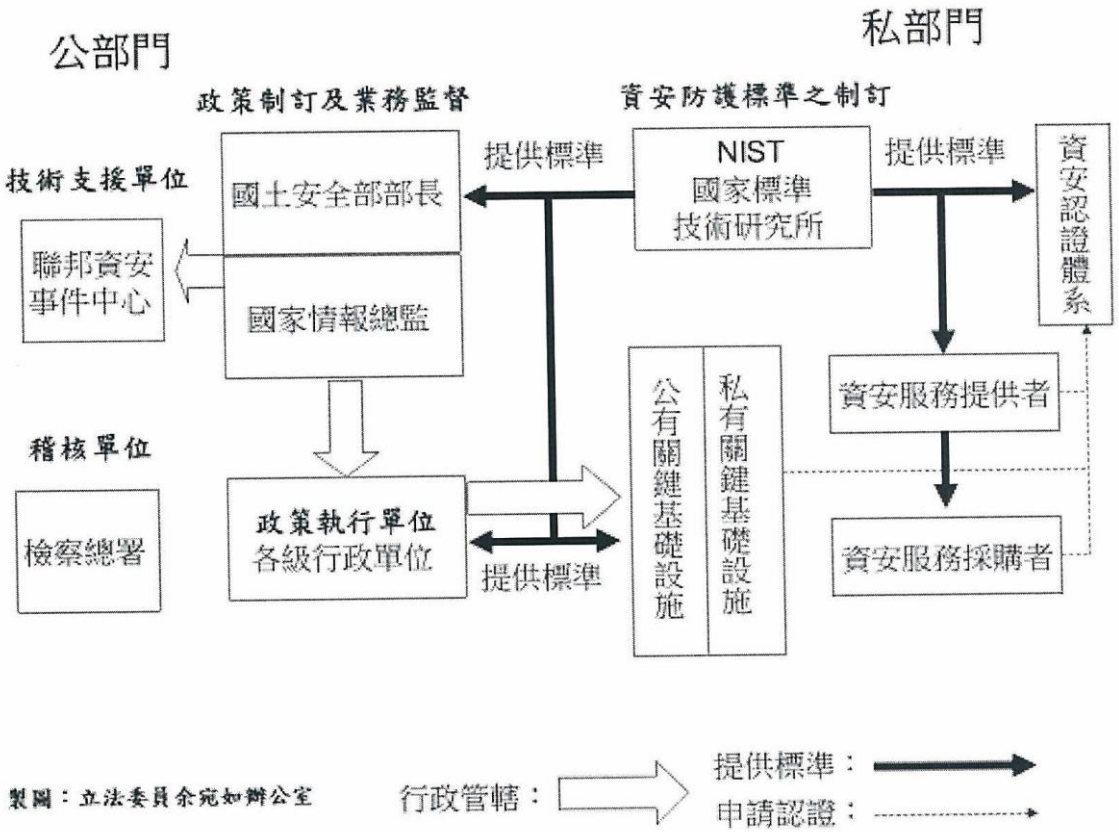
1. 我國政府規模較小，資源較少，且單位專業程度不及美國政府，未必能夠完全比照美國聯邦政府的資安防護架構，仍須做適度之調整及遷就現實；
2. 我國為五院制，某些功能已由監察院（包含審計部）執行。

十三、美國的資通安全架構，其特色概略如下：

1. 公部門及私部門分開處理，FISMA 只規範公部門應盡之職責。
2. 「資安防護標準之制定」與「資安政策之制定與監督」分由二單位負責，其好處是負責標準制定的單位可以免受政策績效之影響，中立客觀地制定標準。而政策負責單位能夠在一個標準之下，依不同單位之屬性設計專屬的單位政策，各司其職。且資安與國安可相互支援。
3. NIST 可以作為各方最新資安技術交流的平台。

4. 透過認證體系，民間資安由商業市場提供不同等級的資安服務，政府僅需公告私有關鍵基礎設施擁有者適用的資安等級，由民間認證體系自行提供認證服務，避免公權力負擔太重以及侵犯私權。

美國的資通安全架構簡示如圖一：

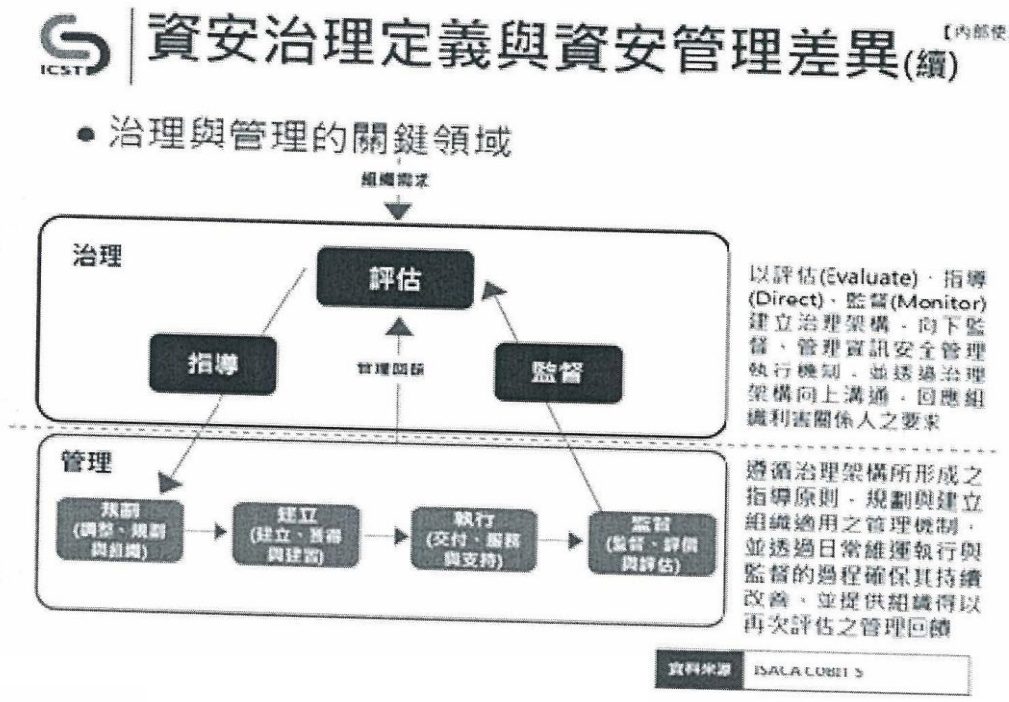


圖一　美國資通安全治理架構

十四、在仿行這一套制度時，須注意台灣在許多方面與美國不同。首先，經濟部標準檢驗局沒有美國 NIST 那種專業能量，未來勢必需要藉助技服中心以及民間和軍方，甚至是國外的專業能量，否則沒有可能制定資安防護標準。其次，由於我國資安內需市場太小，技術等級也還不是全球領先，建立認證機制成本太高，維護不易，恐怕也難以取得國際社會認可。如果直接以國際認證作為認證標準，對於國內中小型業者而言，認證成本太高，且將會發生未來國內需要通過頂級資安認證的產品及服務可能只有國際大廠符合投標資格的情形，對於輔助我國資安產業不利，其中權衡，尚須另作安排，但架構之精神及主要結構，仍取法 FISMA。第三，我國並無「國土安全部」及「國家情報總監」這樣的部會設計，性質比較接近者為國安會及國安局，行政院版「資通安全管理法草案」也因國情因素，將軍方及國安方面的資安排除於外，因此若要配合我國現狀，政策制定及業務監督機關也需另作安

排。

十五、在規劃我國資通安全管理體系之前，先確立主管機關之治理架構有其必要，如果沒有一套精準的治理架構，這一套龐大的分工合作體系將難以運作。本草案的治理架構以三個主管機關及技服中心為主，主管機關區分為「資安治理主管機關」、「資安管理主管機關」及「資安標準主管機關」。如前所述，「資安標準主管機關」為經濟部標準檢驗局。至於「資安治理主管機關」及「資安管理主管機關」的差異，在於前者之主要職責在於建立治理架構，並透過評估（Evaluate）、指導（Direct）、監督（Monitor）等作為，督導資訊安全管理機關之執行，並透過治理架構進行溝通，以回應組織利害關係人之要求，其作為屬於「政策制訂及業務監督者」。後者則遵循治理架構所形成之指導原則，規劃並建立組織適用之管理機制，並透過日常維運執行與監督的過程確保其持續改善，並提供組織得以再次評估之管理回饋，其作為屬於「政策執行單位」。（參閱圖二）



資料來源：《資安治理概論與規劃》，行政院國家資通安全會報技術服務中心內部簡報

圖二 「資安治理定義與資安管理差異」

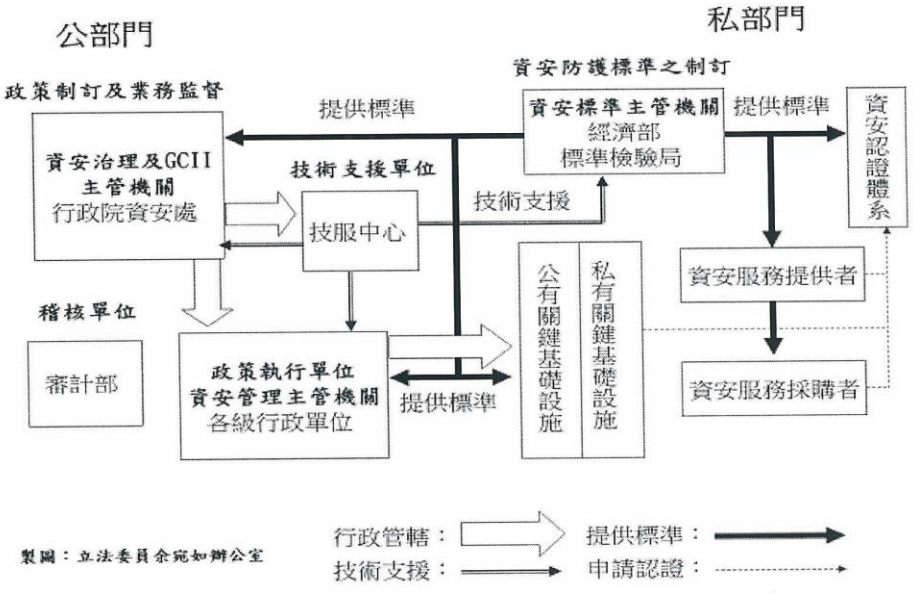
十六、這樣的設計所依循者為 NIST 所建議的組織型態，分為「管理層」、「業務層」及「維運層」。但因我國政府規模較小，因此將業務層及維運層整合於「資安管理主管機關」的管轄之下。（參閱圖三）

資料來源：「資安治理概論與規劃」，行政院國家資通安全會報技術服務中心內部簡報

圖三 「國際資安治理趨勢資安治理」

十七、本草案將「資安治理主管機關」訂為行政院資安處。雖然「處」屬於內部單位，本不適合扮演全國各級機關資安業務「政策制訂及業務監督者」，但是由於本席已提出「資訊長四法」草案，未來資安業務將納入專責部會級政府資訊單位管轄，在目前過渡期間，實不宜再另新設專責機構為之。至於「資安管理主管機關」，則為各行政機關（構）。

十八、在這一套治理架構之下，本草案所規劃的我國資通安全治理架構，如圖四所示：



圖四 本草案資通安全治理架構

十九、將主管機關區分為三種在我國立法例中並不常見，原因有：

1. 其業務性質本就不同，但是完整的資安作業需要這三套業務密切配合，缺一不可。如果將這三項業務整合於一，對於該單位而言，勢必無法以一兼三，另外二項業務將因此犧牲品質，整體資安效益將大打折扣，反不如尊重現實，依業務特性設立三個主管機關。
2. 成為主管機關，才有法源依據編足預算及人力，也才能被課以完整的行政及政治責任，落實課責性分明。如果整合於一機關又發生前述情形，勢必造成單位之間的推諉，監考機關也不易落實監考。

二十、此外，仍有一個問題需要澄清，資安工作之推動並非自立法完成後才依圖施工，前期運作經驗已累積及總結的心得，經證實為有效者，自應在其基礎上繼續努力，對此實無另闢蹊徑，自為創發的必要。綜整我國資通安全相關之法律規範，可劃分為網路犯罪、身分認證、通訊保障、資料保護、資訊公開與機密維護，及資安治理六大類；其所涉及之法律規範包含刑法、電子簽章法、電信法、通訊保障及監察法等 21 項，詳如表四，這些機制都是目前已經實施中的措施：

表四　我國資通安全相關之法律與規範

類別	法律及規範
網路犯罪	刑法第三十六章妨害電腦使用罪。
身分認證	電子簽章法、電子簽章法施行細則、憑證實務作業基準應載明事項準則、外國憑證機構許可辦法。
通訊保障	電信法、通訊保障及監察法、通訊保障及監察法施行細則。
資料保護	個人資料保護法、個人資料保護法施行細則、執行電腦處理個人資料保護事項協調聯繫辦法、濫發商業電子郵件管理條例草案。
資訊公開與機密維護	國家機密保護法、國家機密保護法施行細則、檔案法、檔案法施行細則、機密檔案管理辦法、檔案電子儲存管理實施辦法、政府資訊公開法。
資安治理	行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範。

資料來源：「資安法規面面觀」，劉建良

行政院國家資通安全會報也早自民國 90 年起便執行「建立我國通資訊基礎建設安全機制計畫」，積極推動政府機關落實執行資通安全相關工作，主要政策包含政府機關資訊安全長責任制度、資通安全責任等級分級作業，及機密資訊保護等，對強化政府機關之資通安全能力產生一定的影響。既然如此，這一套資通安全專屬法典還要達到什麼目標？如果要訂定一專法，必須要能夠達成以下目標，否則便不算符合立法目的：

1. 要針對整體資通安全管理，且涵攝目前已經存在的法令。

2. 對於資安防護的設計，必須自事前至事後，完整銜接。

3. 全國各行政機關（構）適用同一個來源的標準規範。

4. 資安防護的設計應以風險管理為中心，且應列入通報應變機制。

5. 應賦予推動資安之完整行政支援，包括人事及預算。

這也是立法時必須謹慎為之之處。

二十一、除 FISMA 2014 以外，本草案另擇要參採下列法令，一併敘明：美國 2017 年 NIST 網路安全架構、評估及稽核法（NIST Cybersecurity Framework, Assessment, and Auditing Act of 2017）、美國總統政策指引 PPD—21「關鍵基礎設施之安全及復原 Critical Infrastructure Security and Resilience」、美國總統 13636 號行政命令「增強關鍵基礎設施資安能力 Improving Critical Infrastructure Cybersecurity」、美國 2008 年 NIST SP800-60 Volum 1：「資訊及資訊系統安全分類指引」（Guide for Mapping Types of Information and Information System to Security Categories）、國際標準 ISO 27001、中華民國國家標準 CNS 27001、行政院《國家關鍵基礎設施安全防護指導綱要》。

二十二、本草案計十四條，內容如下：

第一條：立法目的。

第二條：名詞定義。

第三條：資安治理主管機關。

第四條：資安管理主管機關。

第五條：資安標準主管機關。

第六條：行政院國家資通安全技術服務中心。

第七條：年度報告。

第八條：公務機關稽核。

第九條：關鍵基礎設施。

第十條：通報義務。

第十一條：認證機制。

第十二條：應通報未通報之罰則。

第十三條：資安治理機關市場協助義務。

第十四條：本法實施日期。

提案人：余宛如　　鍾佳濱

連署人：莊瑞雄　　陳賴素美　蔡適應　　陳曼麗　　姚文智

鄭寶清　劉世芳　郭正亮　吳焜裕　吳玉琴
蘇巧慧　江永昌　陳　瑩　蔡易餘　黃秀芳
邱泰源

資通安全法草案

條　　文	說　　明
第一條　本法立法目的為： 一、提供政府資通安全治理架構，以提升國家資通安全之防護、應變及復原能力。 二、透過管理及監察，以及與公民社會及國家安全機制之協作，以提供政府資通訊及資通系統安全保護之最低必要控制。 三、協助市場建立先進、高能、自動及有效的資安解決方案及認證機制，以協助民間建置資通安全能量。 四、提供資安防護標準，以作為政府全面性作業架構、資通系統安全保護最低必要控制，及關鍵基礎設施資安防護方案的依據。 五、統整資通安全政策、法令，以保障國家安全，維護社會公共利益。 六、透過提升政府採購軟體或硬體資安解決方案，以帶動資通安全產業發展，扶植國家資通安全人才。	一、明訂本法立法目的。 二、本法立法目的包含六大主題： 1. 提供治理架構 2. 提供資安最低必要控制 3. 協助市場建立資安解決方案 4. 提供資安防護標準 5. 統整資安政策法令 6. 以政府採購帶動資安產業 三、參考 FISMA 2014 之立法目的： 1. 針對支持聯邦運作及資產（operation& assets）的相關資訊，提供一個能夠提高資訊安全控制效能的全面性架構。 2. 認知到現行聯邦資訊環境已經高度網路化的事實，提供有效的政府管理，以及對於相關資訊安全風險的監察，包括透過與公司社會、國家安全機制及執法單位的協作。 3. 發展並維持對於聯邦「資訊及資訊系統」安全保護的最低必要控制。 4. 提供一套機制，用以改善對聯邦資訊安全計畫的監察，包括經由自動化安全工具以持續「斷定（diagnose）」資安狀態並改善安全。 5. 理解商業開發之資訊安全產品可提供先進、高能、自動及有效的資安解決方案，反映市場解決方案對於保護由私部門設計、建造及營運的關鍵基礎設施（對國安及自由經濟安全十分重要）十分重要。 6. 認知選擇軟體或硬體資安解決方案應由各機關自行自商業市場產品中挑選。 四、參考 ISO 27001 之制訂目的：「本標準之制定係為提供用以建立、實作、運作、監視、審查、維持及改進資訊安全管理系統之模型。」
第二條　本法用詞，定義如下： 一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處	一、明訂本法用詞定義。 二、資通系統及資通服務之定義參考美國 NIST 2008 年 SP800-60 Volum 1：「資訊

理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、資通安全：指保護資訊及資通系統，免除於未經授權的存取、利用、揭露、干擾、修改、毀壞，以及可能導致之實際違法行為，或對依法形成的安全政策、安全流程或資訊利用政策構成威脅，以確保資訊及資通系統之完整性、機密性及可用性。

四、資安事件：指系統、服務或網路經識別已發生違法或違反資訊安全政策的狀態，或是可能與資通安全相關，然先前未知的狀態，致資訊及資通系統喪失完整性及機密性，因而構成對於資安政策或安全流程或資訊利用的威脅。

五、公務機關：指依法行使公權力之中央、地方機關（構）、公法人、公營事業及政府捐助之財團法人。

六、資通安全管理系統：整體管理系統的一部份，以營運風險管理為基礎，用以建立、實作、運作、監視、審查、維持及改進資通安全。

七、人力資源安全：整體人力資源管理之一部分，依所接觸資安業務機密等級所進行之聘僱前角色與責任之釐清、篩選、聘僱條款與條件，聘僱期間之管理階層責任、資訊安全認知、教育及訓練、懲處，聘僱終止或變更時之終止責任、資產歸還、存取權限之移除等事項。

八、關鍵基礎設施：指能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等實體或虛擬資產之營運所需之重要資通訊系統或調度、控制系統或網路，其功能一旦停止運作或效能降低，對國民生活、經濟活動、公眾安全或國家安全有重大影響之虞者。

及資訊系統安全分類指引」附錄 A。

三、資安之定義參考 FISMA 2014 第 3552 條：資安是「保護資訊及資訊系統，免除於未經授權的存取（unauthorized access）、利用（use）、揭露（disclosure）、干擾（disruption）、修改（modification）、毀壞（destruction）」。

資安的目的在於提供：

1. 完整性（integrity），意指保護系統免除於不正當的資訊修改或毀壞，並包括確保資訊的「可追究性 nonrepudiation」及「真實 authenticity」。
2. 機密性，意指保護對於接取行為及揭露行為的限制性授權機制，包括對於個人隱私權及專屬性資訊的保護。
3. 可用性，意指確保及時可靠的網路接取及資訊利用。

四、另參考 ISO 27001 對於「資訊安全」之定義：保存資訊的機密性、完整性及可用性；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。

五、參考 FISMA 2014 第 3552 條：「事件 incident」意指發生：

1. 中樞失效（without lawful authority），喪失系統的完整性及機密性，「資訊及資訊系統」無法使用。
2. 構成違法，或對依法形成的安全政策、安全流程或可被接受的資訊利用政策構成實存威脅。

六、ISO 27001 對於「資訊安全事件」（information security event）之定義：系統、服務或網路發生一個已識別的狀態，顯示可能已發生資訊安全政策違例或保護措施失效，或是可能與安全相關，然先前未知的狀況等。

七、參考 ISO 27001 對於「資訊安全管理系統，ISMS」（Information Security Management System）之定義：整體管理系統的一部份，以營運風險導向（作法）為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。

八、參考 ISO 27001 對於「人力資源安全」之

	定義。 九、關鍵基礎設施之定義，參考行政院「國家關鍵基礎設施安全防護指導綱要」、美國總統 13636 號行政命令「增強關鍵基礎設施資安能力」、美國總統政策指引 PPD—21「關鍵基礎設施之安全及復原」及美國 31 CFR 800.208 之定義。 十、關鍵基礎設施的定義不應以產業別作為分類基礎，而應仿歐盟作更精準的定義，免得過於浮濫而失焦。例如：歐盟關鍵基礎設施對於電業，只侷限於真正影響國安之「輸配電系統」，而非電廠或營業站。故本法僅限定於重要資通訊系統或調度、控制系統或網路。
第三條　本法所稱資安治理主管機關（本法簡稱資安治理機關），為行政院資通安全處。 資安治理機關掌理下列事項： 一、制訂與資安有關之法令、政策、原則。 二、依據資安法令、政策及原則建立資安治理架構。 三、整合與協調各公務機關之資安管理政策及程序。 四、監督各公務機關對於資安政策之執行及資安標準之遵守狀況。 五、與資安標準機關協作發展資安標準及相關作業辦法，並交付公務機關確認可行性。 六、依據資安標準機關公告之標準，與資安管理機關共同決定機關資通安全管理系統之最適資安防護等級及相關需求。 七、建立各公務機關資安治理評估系統並協助辦理資安治理評估系統試行與導入。 八、確保各公務機關依資安政策，於出現資安事件時，通報國家資通安全技術服務中心。 九、建立資安事件分級標準及公務機關資料分級標準，以供公務機關據以辦理通報。 十、確保各公務機關依資安政策提報年度資安報告。 十一、綜理國家資通安全技術服務中心之運作與管理。 十二、確保資安管理與各公務機關之政務運	一、明訂資安治理主管機關掌理事項。 二、參考 FISMA 2014 第 3553 條「國土安全部部長及國家情報總監的功能及權力」。 三、參考行政院國家資通安全會報技術服務中心內部簡報《資安治理概論與規劃》第 13 頁。 四、資安事件小自個人密碼被盜，大到機構遭到 DDoS 攻擊或大筆資料外洩，律定資安通報責任時應該要釐清何種等級的資安事件才需要通報，以免浪費行政資源。 五、參考美國 2008 年 NIST SP800-60 Volum 1：「資訊及資訊系統安全分類指引」，該指引之立法目的即在「協助聯邦各機關將資訊及資訊系統分類，以便將各種資安風險依衝擊等級及結果嚴重性細分，俾該機關正確執行資安防護政策」。故於第二項第九款明列資安治理主管機關應建立資安事件及公務機關資料分級標準，以利公務機關據以辦理通報作業及制訂相對應之資安措施。

作、政策計畫及預算流程整合一致。 十三、召集各公務機關資安長或資深資安人員會議，以確保資安政策得以有效執行。 十四、制訂與關鍵基礎設施有關之資安政策及原則，及辦理關鍵基礎設施之公告。 十五、定期公布國家資通安全情勢報告及資通安全發展方案。 十六、其他資安治理必要事項。	
第四條　本法所稱資安管理主管機關（本法簡稱資安管理機關），在中央為二級機關及行政院直屬三級機關，在地方為直轄市、縣（市）政府，公法人、公營事業及政府捐助之財團法人為該法人及事業。 資安管理機關掌理下列事項： 一、發展公務機關（構）資通安全管理系統，以確保資安作業能持續整個資訊系統週期，且計畫內容須以風險評估為基礎，並包含委外承包商管理。 二、確保資通安全管理系統之作為與機關的戰略、運作、計畫及預算流程整合一致。 三、依據資安標準機關公告之標準，與資安治理機關共同決定機關資通安全管理系統之最適資安防護等級及相關需求。 四、依據成本效益原則執行資安政策及程序，以降低資安風險至可接受的程度。 五、至少一年一次測試及評估資通安全管理系統之管控及技術，包括自動化工具之使用，以確保其有效執行。 六、提出年度資安報告，包含因資安事件所進行之系統修復行動。 七、依據前條第二項第九款之資安事件及公務機關資料分級標準，於資安事件發生時負責通報。 八、確保公務機關擁有質量足夠的資安人力及預算，以完成相關政策、程序、標準，及指引的落實。 九、訓練及監管資安人員擔負資安責任。 十、確保機關所有人員、委外承包商人員及委託其他機關代辦資安業務人員的能力皆得以執行資安計畫。 十一、指定一具備專業資格之資安官專責機關之資安作業。	一、明訂資安管理主管機關掌理事項。 二、參考 FISMA 2014 第 3554 條「聯邦政府的責任」。 三、數據安全是各國資通安全立法保護重點，但未必皆見於其資安專法。例如，美國在商業資訊安全方面透過《統一商業秘密法》、《經濟間諜法》對竊取商業秘密的行為進行相關刑罰。美國《電腦詐欺和濫用法》、英國《電腦濫用法》都規範了非法利用和竊取政府部門數據資訊行為的罰則。在個人數據方面，美國《反竊聽法》、《電信法》對資訊傳輸過程中非法攔截及竊取個人數據的行為加以管制。歐盟《1992 年資訊安全框架決定》、《1995 年數據保護指令》、《2002 年隱私與電子通信指令》、《2006 年數據留存指令》，都是歐洲保護個人數據的重要基本規範。資通安全管理機關本為各目的事業主管機關，肩負相關產業之監管輔導責任，在不抵觸資安政策之前提下，自然可以依據資安標準主管機關所提供之資通安全等級，辦理各機關監管或輔導之產業的資通安全協作事項。 四、我國現行資通安全相關之法律規範，可劃分為網路犯罪、身分認證、通訊保障、資料保護、資訊公開與機密維護，及資安治理六大類；其所涉及之法律規範包含刑法、電子簽章法、電信法、通訊保障及監察法等 21 項，於本法通過後依然有效，原目的事業主管機關也依然得依法辦理所轄業務。

十二、負責機關之人力資源安全，其範圍包括正式員工、包商以及委託其他機關執行資安相關業務人員，必要時得依業務機密等級進行不同等級之忠誠調查。 十三、在不抵觸資安政策之前提下，依據資安標準機關所提供之資通安全等級，辦理各機關監管或輔導之產業的資通安全協作事項。 十四、督導下級機關辦理本條所列事項。 十五、辦理資安軟體及服務之採購。 十六、其他資安管理必要事項。	
第五條　本法所稱資安標準主管機關（本法簡稱資安標準機關），為經濟部標準檢驗局。 資安標準機關掌理下列事項： 一、與資安治理機關協作制定全國統一性的標準與指引。 二、對公務機關所處理與保管的資訊進行分類，標示其資通安全等級。 三、提供資訊與資通系統相關之安全指引。 四、為公務機關制定資通安全準則。 五、資通安全軟硬體技術規範、相關服務與審驗機制之發展與推動。 六、其他與資安標準相關之業務。 資安標準機關於執行前項各業務時，應協同資安治理機關，並徵詢技服中心之技術支援。	一、明訂資安標準主管機關掌理事項。 二、參考 40 U.S . Code § 11331「聯邦政府資訊系統相關責任」，由國家標準技術研究所負責制定統一性的標準與指引，並對聯邦政府機關所處理與保管的資訊進行分類，標示其資訊安全等級，同時提供資訊與資訊系統相關之安全指引。目前美國國家標準與技術局制定的資通安全準則（NIST SP 800）系列文件已廣泛應用於聯邦政府所有的資訊系統。
第六條　行政院設行政法人國家資通安全技術服務中心（本法簡稱技服中心），辦理下列事項： 一、提供各公務機關於執行資安政策、原則、標準、指引上之操作支援及技術支援。 二、協助資安管理機關緩解緊急資安狀態。 三、辦理網路攻防演練，輔以定期稽核、健診及滲透測試等服務，及早發現資安問題。 四、針對資安人員及一般人員之資安訓練。 五、編輯並分析各機關之資安情資。 六、發展並指導公務機關資安系統的運作評估重點，包括資安系統所面臨之威脅，及資安系統的弱點評估。 七、維運政府資通安全防護監控中心及政府資安資訊分享與分析中心。	一、明訂行政院國家資通安全技術服務中心辦理事項。 二、參考 FISMA 2014 第 3556 條「聯邦資安事件中心」職權之相關規範如下： 1. 通則： I. 於機關資訊營運者面臨資安事件時，提供及時的技術協助，包括提供偵測技術協助及掌握資安事件的指引。 II. 編輯及分析威脅資安事件之情資。 III. 知會資訊營運者現存及潛在資安威脅，及易受攻擊之弱點。 IV. 提供機關適當的資安威脅及弱點的相關情資，以助機關進行風險評估。 V. 諮詢 NIST、資安體系各機關及辦公室（包括國安局），及其他依法及直

八、強化政府機關（構）資安聯防監控能量，建構巨量資料分析能量。 九、受理公務機關資安事件之通報。 十、協同資安治理機關及資安標準機關共同發展及執行基於風險管理基礎的資安標準。 十一、推動公務人員資安職能評量機制，持續培育資安專業人才，並推廣全民資安意識。 十二、推動資通安全科技之研發、整合、應用及國際合作交流。 十三、支援產業資通安全重大發展策略之需求。 十四、規劃及支援國家關鍵基礎設施之資通安全防護。 十五、其他與資通安全科技相關之業務。 國家資通安全技術服務中心之組織另以法律定之。	轄總統，並與資安業務有關之單位。 2. 國安系統：國安體系任何一機關皆須與聯邦資安事件中心分享資安事件、威脅及攻擊弱點等相關資訊，分享程度到符合國安體系應符合之標準，或指引所要求，且經法律授權，總統命令為之者。 三、參考「行政院國家資通安全會報技術服務中心」設置宗旨： 1. 研析國家資安法規體系，協助研議政府機關資安規範與指引，以完備國家資安基礎環境。 2. 維運政府資通安全防護監控中心（Government—Security Operation Center, G—SOC）、政府資安資訊分享與分析中心（Government—Information Sharing and Analysis Center, G—ISAC）等。 3. 協助各政府機關（構）處理重大資通安全事件，加強緊急應變及處理復原能力，並舉行大規模網路攻防演練，輔以定期稽核、健診及滲透測試等服務，及早發現政府與關鍵基礎設施資安問題。 4. 強化政府機關（構）資安聯防監控能量，建構巨量資料分析能量。 5. 推動資安治理與資安責任等級分級防護，加強各機關（構）資安防護縱深機制。 6. 推動公務人員資安職能評量機制，持續培育資安專業人才，並推廣全民資安意識。 7. 規劃關鍵資訊基礎設施之資通安全防護機制。 四、參考美國「網路威脅情報整合中心」（Cyber Threat Intelligence Integration Center—CTIIC）之功能，該中心扮演全美網路威脅情報中樞，匯總聯邦調查局、中央情報局及國家安全局等多部門的情報力量，提高美國防範和應對網路攻擊的能力。
第七條　資安管理機關應最遲於每年一月三十一日前，向資安治理機關提報前年度資安政策實施狀況，資安治理機關應於彙整後，最遲於三月一日前，向立法院提報前年度資安政策實施狀況。	一、明訂年度報告相關事項。 二、參考 FISMA 2014 第 3554 條「聯邦政府的責任」第三項「機關報告」。 三、「機關報告 Agency Reporting」分為「年度報告」及「其他計畫及報告」。「年度

前年度資安政策實施狀況報告應包含： 一、關於每一主要資安事件或相關事件群之描述。 二、資安事件總數，包括造成嚴重資安損害的事件數、系統衝擊等級、事件型態，及受損系統部位等資料。 三、個資侵權的資安事件描述。 四、依據第四條第二項第五款必須完成之年度評估結果摘要。 五、其他任何資安治理機關認為必要的資訊。 前年度資安政策實施狀況報告應同時提報國家安全會議及審計部。	報告」以「一般性報告」為主，須以非機密形式提報。另一種則是附件以機密形式提報。 四、「一般性報告」包含以下四主要主題： 1. 關於每一主要資安事件或相關事件群的描述。 2. 資安事件總數，包括造成嚴重資安損害的事件數、系統衝擊等級、事件型態，及受損系統部位等資料。 3. 個資侵權的資安事件描述。 4. 任何資安總監認為必要，或是部長諮詢資安總監後認為必要的資訊。 五、年度報告報告對象包括國家情報總監、國土安全部部長、政府改革委員會、國土安全委員會、參議院科學委員會、參議院國土安全暨政府事務委員會、參議院商業科學暨交通委員會、國會撥款委員會（appropriations committees）及審計總長（Comptroller General）。 六、每一公務機關（構）皆須提報年度報告，以陳述該機關對於資安政策、程序及實踐是否足夠且有效。
第八條　審計部應於資安治理機關提報前年度資安政策實施狀況報告後二個月內，完成對於公務機關資安政策實施狀況之稽核，並向立法院提出稽核結果報告。	一、明訂公務機關稽核相關事項。 二、參考 FISMA 2014 第 3555 條「年度獨立評價作業」第二項「獨立稽核 Independent Auditor」： 1. 檢查總署應該依據 1978 年檢查總署法之規定，指定部分機關受檢，受指定之機關，其依本條所定年度評價作業應由該檢察總署，或檢查總署指派之獨立外部稽核人員為之。 2. 不適用前款規定之機關，機關首長應聘任一外部稽核人員完成此評價作業。
第九條　關鍵基礎設施分為公有關鍵基礎設施及私有關鍵基礎設施。 公有關鍵基礎設施指公務機關（構）依據法律規定，或基於權利行使，或由於預算支出，或由於接受捐贈取得全部或部分所有權之關鍵基礎設施。非屬公有關鍵基礎設施之關鍵基礎設施為私有關鍵基礎設施。 關鍵基礎設施之防護應採用風險管理架構。	一、明訂關鍵基礎設施相關事項。 二、第一項關鍵基礎設施之區分為公有及私有，請參考行政院「國家關鍵基礎設施安全防護指導綱要」之肆「關鍵基礎設施定義及分類」。 三、第二項公有關鍵基礎設施之定義參考《國有財產法》。 四、第三項請參考行政院「國家關鍵基礎設施安全防護指導綱要」之貳「防護目標與風

資安管理機關應為公有關鍵基礎設施提供防護架構，制訂防護執行策略及推動方針，執行資產調查及風險分析，決定防護優先等級，建立通報系統，實施防護演練、測試與檢討。

資安治理機關、資安管理機關及技服中心應透過下列措施，積極鼓勵私有關鍵基礎設施提供者參與資安防護工作：

一、透過即時預警資訊之提供，促進民間關鍵基礎設施擁有者自願參與資訊分享機制。

二、邀請私有關鍵基礎設施提供者參與公務機關或公有關鍵基礎設施舉辦之資安防護演練。

三、撰擬防護計畫時，結合相依性或替代性之私有關鍵基礎設施提供者資源，形成縱深應變體系。

四、透過輔導政策獎勵私有關鍵基礎設施提供者參與風險管理及應變機制。

私有關鍵基礎設施提供者應配合主管機關參與風險管理及應變機制。

險管理架構」。風險管理架構包括下列項目：

1. 設定安全目標
2. 辨識資產、系統與網絡
3. 風險評估
4. 決定防護強化優先次序
5. 實施防護計畫
6. 衡量實施成效

五、第四項請參考行政院「國家關鍵基礎設施安全防護指導綱要」之伍「防護規劃建置程序」。

六、第五項請參考行政院「國家關鍵基礎設施安全防護指導綱要」之壹拾肆「民營企業與民間組織之參與」。

七、美國總統政策指引 PPD—21「關鍵基礎設施之安全及復原 Critical Infrastructure Security and Resilience」中明確表示，對於關鍵基礎設施之防護，政府與民間共同承擔責任，然即便聯邦政府得以命令要求關鍵基礎設施業者配合建構資安防護，雙方仍應該是伙伴關係。

八、美國總統 13636 號行政命令「增強關鍵基礎設施資安能力」亦強調協同發展及執行風險管理標準，並特別指出增加資安情資供應質量及時效是美國政府的責任。

九、日本網絡安全策略依下列四個基本原則來規劃，包括：(1)保證資訊自由流通，並確保隱私與智慧財產權；(2)制訂法律，並參考國際規範；(3)開放；(4)自治；(5)與 CII 利害關係人共同協作。在關鍵資訊基礎設施的保護方面，公私機構間安全實務與發現的資訊分享，並且對 CIIP 的範圍定期審查。其中包括：由政府安全工作協調小組（Government Security Operation Coordination Team, GSOC）擔任監督與資訊分享的角色，分享網絡安全事件與偵測資訊給 CII 相關部門。

十、依據德國 2015 資訊科技安全法（IT—Sicherheitsgesetz），德國聯邦政府要求關鍵基礎設施的營運商，要滿足資訊科技安全的最低標準，且須向聯邦資訊安全局通報資訊安全事件。聯邦資訊安全局要對關

	鍵基礎設施營運商的資訊進行評估分析，並提供給關鍵基礎設施營運商彙整改善，以提高其基礎設施的保護。
第十條　資安事件發生時，公務機關及關鍵基礎設施提供者應即時通知並諮詢技服中心。 如發生之資安事件屬於重大資安事件，公務機關及關鍵基礎設施提供者並應即時通知資安治理機關、資安管理機關、國家安全會議秘書處。資安治理機關應於最遲七日內向立法院提出報告。 前項所稱重大資安事件之定義，由資安治理機關諮詢技服中心後訂之。	一、明訂公務機關稽核相關事項。 二、參考 FISMA 2014 第 3554 條「聯邦政府的責任」第二項第七款第三目「偵測、報告、反應資安事件的流程」。 三、依據該流程，遇資安事件發生時，除致力於在實質損害發生前緩和因資安事件所引起的風險外，公務機關有義務： 1. 通知並諮詢聯邦資安中心。 2. 在適當情況下，通知並諮詢 i. 執法機關、檢察總長及總法律顧問辦公室 ii. 總統指派處理國安系統問題的辦公室 iii. 國會重大事件委員會： I. 於合理判定已經發生重大事件之後 7 日內。 II. 在前述時間之後一段合理時間之後，又出現與該重大事件相關的新事證。 iv. 任何依法成立或由總統指揮的機關（構） 四、紐約州金融署要求公司必須在 2018 年 2 月 15 日以前向監理機關，提交一份遵循報告，其中包括以下內容：「若發生重大網絡安全事件，公司必須要在 72 小時內報告監理機關。」
第十一條　技服中心應比照國際主要規範，建立我國資通安全認證機制，以供公務機關、關鍵基礎設施及民間進行資安認證之用。 我國資通安全認證能量尚無法提供認證者，應以國際主要規範作為規範，以取得該等級規範之認證作為通過認證之依據。 國際主要規範之內容由技服中心訂定並公告。 資安治理機關應推動與他國之間資安認證互相承認。	一、明訂認證機制相關事項。 二、我國欲建立認證機制，應採取國際主流標準。國內認證能量不足者，應採納國際認證標準。 三、資安治理主管機關應推動與他國之間資安認證互相承認。
第十二條　關鍵基礎設施提供者違反第十條第二項之通報義務，由資安治理機關處新臺幣十萬元以上一百萬元以下罰鍰。	一、明訂違反通報義務之罰則。 二、德國於 2015 年 6 月 12 日通過資訊科技安全法案，德國重要企業遇到網絡攻擊必須

	申報，否則將被罰款，罰金最高十萬歐元。所謂重要企業是指能源公司、銀行、醫院等。 三、資安作業要能有效運作，最重要的是能建立聯防體系。資安聯防體系從攻擊事件發生、可疑事件偵測，到分析、處理、鑑識，最重要且必要的環節是通報，以便聯防體系之其他單位早期知悉攻擊發生，以避免事態擴大。
第十三條　資安治理機關應協調經濟部及技服中心，協助市場建立先進、高能、自動及有效的資安解決方案。 資安治理機關應協調經濟部及技服中心，政策獎勵自建關鍵基礎設施之資訊核心系統者。	明訂資安治理機關市場協助義務。
第十四條　本法自公布日施行。	明訂施行日期。