立法院議案關係文書 （中華民國41年9月起編號）
中華民國105年9月29日印發

# 院總第 1570 號　委員提案第 19537 號

案由：本院時代力量黨團，鑑於全球透過網路或其他通訊設備之攻擊事件頻傳，爰參酌美國、德國等資通安全發展較為先進之國家之立法歷程、內容與實作經驗，以及國內自 2001 年以來所有關於資通安全之政策及作為，特制定本法，將原先業務職掌分散於各部會之資通安全等業務之制定及執行，整合至行政院資安處，以綜理我國資通安全業務、輔導及考核中央及地方各級政府及一定規模以上、具有關鍵基礎設施屬性的民間企業制定並執行資通安全管理規定；給予資安處專業人員專業技術加給、定期技能培訓與檢驗及必要人員須受特殊考核之義務；納入通訊保障及監察紀錄之資通安全管理，使我國能在事前防護資通安全系統及偵測針對系統之各種威脅、於事中得以迅速回應、縮小損害規模甚至回擊、在事後也可以盡早回復、保全及蒐集相關證據，提升我國資通安全之防禦能力、維護我國國家安全及國民權益。是否有當？敬請公決。

提案人：時代力量立法院黨團
林昶佐　徐永明　黃國昌
高潞・以用・巴魕剌 Kawlo・Iyun・Pacidal
洪慈庸

# 資通安全管理法草案總說明

鑑於全球透過網路或其他通訊設備之攻擊事件頻傳，例如 2016 年 7 月國內的第一銀行盜領案、2015 年 1 月法國 1.9 萬個包含商業、宗教、學校、政府的網站遭到 ISIS 攻擊、2014 年 6 月香港大學民意網遭受大規模阻斷服務攻擊、2013 年 12 月美國國內第二大連鎖零售商店 Target 也遭到駭客入侵，在其門市 POS 系統植入惡意程式、竊取高達 1.1 億筆消費者資料；此外，美國 2013 年統計顯示，美國國內之水、電、油、核電廠等關鍵基礎設施曾遭 257 次外部駭客攻擊，我國 2012 至 2014 年每年也有 244 至 401 起的通報資安事件數。

以上案例，均顯示出國際資安風險日益提高，不論其目的在於竊取個人隱私、公務、國防及商業機密，或破壞國家關鍵基礎設施（如能源、水利、金融、交通、醫療等）、甚至是發動網路戰以癱瘓國家網路運作，都在在威脅各國之國家安全及國民權益。

因此，爰參酌美國（美國聯邦資訊安全管理法，Federal Information Security Management Act）、德國（德國聯邦資訊科技安全加強法案，Act to Strengthen the Security of Federal Information Technology of 14 August 2009）等資通安全發展較為先進之國家之立法歷程、內容與實作經驗，以及國內自 2001 年以來所有關於資通安全之政策及作為，特制定本法，期使我國能在事前防護資通安全系統及偵測針對系統之各種威脅、於事中得以迅速回應、縮小損害規模甚至回擊、在事後也可以盡早回復、保全及蒐集相關證據，提升我國資通安全之防禦能力、維護我國國家安全及國民權益。

本草案之特色如下：

一、權能集中：將原先業務職掌分散於各部會（如經濟部、教育部、科技部、通傳會、行政院資安辦等）的(1)國家資通安全政策、法令、標準作業流程、技術規範；(2)系統及設備等軟、硬體產品或服務之測試及審驗；(3)各部會及單位之稽核、檢驗、測試、資安事件演練；(4)市場發展、監督、管理；(5)人才培育、全民資通安全意識及知識推廣；(6)境外事務及國際交流合作等業務之制定及執行，整合至行政院資安處，改變過去資安辦、資安會報將不同業務指定給不同部會，由各部會另行編制人力及預算予以執行的結構，將我國資通安全業務全數納編至行政院資安處，綜理我國資通安全業務。（草案第一條至第六條）

二、中央及地方各級政府及一定規模以上、具有關鍵基礎設施屬性的民間企業，要有資通安全管理規定，依其業務屬性分級管理，並由資安處負責輔導制定、實施與稽核。（草案第七條）

三、資安處專業人員另給予專業技術加給；也需定期技能培訓與檢驗。必要人員另需依法進行忠誠考核，以防護我國資通安全系統與業務。（草案第九條）

四、重視資通安全教育與研發。（草案第十條）

五、政府重大施政計畫要有資通安全影響評估。（草案第十一條）

六、納入通訊監察紀錄的管理。（草案第六條）

# 資通安全管理法草案

| 條　　文 | 說　　明 |
| --- | --- |
| 第一章　總　　論 | 章名 |
| 第一條　（立法目的）<br>為提升國家資通安全之防護、應變及復原能力，加強資通安全政策、法令、技術及市場之研究、發展及應用，扶植國家資通安全人才、組織及產業，以維護國家安全及國民權益，特制定本法。 | 鑑於全球透過網路或其他通訊設備之攻擊事件頻傳，導致各國、企業或個人之機敏性資料落入具有特定負面意圖之人或組織手中，造成國家安全或國民權益之重大損害，爰參酌美國、德國等資通安全發展較為先進之國家之立法歷程、內容與實作經驗，特制定本法，期使我國能在事前防護資通安全系統及偵測針對系統之各種威脅、於事中得以迅速回應、縮小損害規模甚至回擊、在事後也可以盡早回復、保全及蒐集相關證據，提升我國資通安全之防禦能力、維護我國國家安全及國民權益。 |
| 第二條　（名詞定義）<br>本法所稱資通安全，謂硬體設備、軟體系統、軟體應用服務等有關網路與通訊事項之可用性、完整性及保密性，並遵循一定之標準，避免未經授權之存取、使用、洩漏、破壞、修改或銷毀等不利於國家安全及國民權益之行為。<br>前項所稱有關網路與通訊事項，準用通訊保障及監察法第三條之定義。 | 一、根據美國前總統柯林頓第 63 號總統決策令（Presidential Decision Directive）及美國聯邦資訊安全管理法（Federal Information Security Management Act），資訊安全管理的目標在於保護資訊及資訊系統以避免未經授權的存取、使用、洩漏、破壞、修改或銷毀等行為，以確保資訊的可用性（Availability）、完整性（Integrity）及保密性（Confidentiality）；德國聯邦資訊科技安全加強法案（Act to Strengthen the Security of Federal Information Technology）亦指出，資訊安全指透過安全防範的方式，確保資訊之可用性、完整性及保密性。<br>二、另再參酌我國通訊保障及監察法等相關規定，界定需加以防護之範疇，包含利用電信設備發送、儲存、傳輸或接收符號、文字、影像、聲音或其他信息之有線及無線電信、郵件、書信、言論及談話等，以確保處理及傳輸訊息之各式科技及記錄均在本法指涉範疇中。 |
| 第三條　（編列預算）<br>政府每年應編列預算，執行資通安全之相關法令及政策。 | 政府發展資通安全相關研究、發展及應用之工作，需大量人力及經費之挹注，方有成效。然我國資訊相關預算占公務總預算之比例，卻呈現逐年下降、不到 1%之情形；對照美國聯邦政府，不僅資訊相關預算占總預算比例超過 |

| | |
|---|---|
| | 2%，近五年來亦逐年成長中。爰此訂定編列預算之條文，賦予政府編列資通安全預算之法源，據此補充我國資通安全發展之所需資源。 |
| 第四條　（獎勵均衡研發及應用）<br>政府應協助學校、研究機關（構）、法人或團體，充實人才、設備及技術，以促進資通安全之研究、發展及應用。<br>政府於推動資通安全之研究、發展及應用時，應注意與資通安全相關之人文社會科學及其他資通安全技術之均衡發展。 | 政府發展資通安全相關研究、發展及應用，在有限之資源下，必須整合產、學、研各界能量，針對技術、管理、政策、法律、倫理等不同面向，投注資源進行研發與應用。為確保我國研發不致偏頗於技術面，爰此參酌科學技術基本法第二條之規定，擬具均衡發展之條文，期使我國資通安全相關研發及應用得以平衡。 |
| 第五條　（主管機關）<br>為有效辦理資通安全相關事項，行政院應設置資通安全處（以下稱本處），依法行使職權。 | 明定主管機關為行政院資通安全處。 |
| 第二章　業務職掌 | 章名 |
| 第六條　（業務職掌）<br>本處掌理下列事項：<br>一、資通安全政策之訂定、法令之訂定、修正、廢止及執行。<br>二、資通安全標準作業流程及技術規範之訂定、修正、廢止、執行、監督及管理。<br>三、資通安全系統及設備等軟、硬體產品或服務之測試及審驗。<br>四、協助中央政府各級機關、地方政府及一定規模以上、具有國家關鍵基礎設施屬性之民間企業訂定、修正、廢止、執行、監督及管理第七條所稱之資通安全管理規定。<br>五、協助中央政府各級機關、地方政府及一定規模以上、具有國家關鍵基礎設施屬性之民間企業預防、偵測、處置、復原、證據保全及鑑識資通安全事件。<br>六、定期或不定期稽核、檢驗、測試及演練中央政府各級機關、地方政府及一定規模以上、具有國家關鍵基礎設施屬性之民間企業其資通安全管理規定及資通安全相關業務之執行情形。<br>七、資通安全市場之發展、監督及管理。<br>八、資通安全人才培育及認證政策之訂定、修正、廢止、執行、監督及管理。<br>九、全民資通安全意識及知識推廣策略之訂 | 一、參考美國聯邦資訊安全管理法、德國聯邦資訊科技安全加強法案等規定，以及我國歷年資通安全發展計畫（如建立我國通資訊基礎設施安全機制計畫、國家資通訊安全發展方案等），訂定我國資通安全相關業務之主管機關之任務。<br>二、根據最新一期國家資通訊安全發展方案（2013-2016 年）揭櫫之願景：「建構安全資安環境，邁向優質網路社會」及其四大策略目標：「強化國家資安政策」、「完備資安防護管理」、「奠基資安技術能量」、「擴大資安人才培育」等政策，爰將：<br>1. 研訂資安政策、規範（如資安管理要點及相關規範）、指引（如手冊）、標準（如品項規範、服務水準協議、資安服務需求說明書範本）及法規；<br>2. 落實資安管理及稽核制度（如資安治理評核系統、資安治理成熟度評估、資訊系統分級、資安防護部署計畫、機關分級及定期內部與外部稽核等）；<br>3. 資訊分析與分享；<br>4. 提升全民資安意識；<br>5. 培訓專業人才；<br>6. 資安演練（包含弱點檢測、滲透測試、情境演練、實兵演練、電子郵件社交工 |

定、修正、廢止、執行、監督及管理。

十、資通安全境外事務及國際交流合作之執行。

十一、資通安全相關法令政策、市場動態、標準作業流程實務、工程技術報告及統計資料之蒐集、彙整、分析及發布。

十二、其他有關資通安全之事項。

前項第一款所稱資通安全政策及法令，應由本處每年諮詢及彙整有關機關代表、學者專家、產業部門及相關社會團體之意見後訂定及修正，並由行政院核定之。

前項諮詢及彙整之學者專家、產業部門及相關社會團體之人數，不得少於二分之一。

第一項第五款、第六款所稱國家關鍵基礎設施屬性，係指營運項目包含能源、電力、水利、金融、衛生、醫療、資通訊科技、交通運輸、國防軍事、電信、郵政、及其他特定專業領域。

前項所稱特定專業領域，及第一項第五款、第六款所稱一定規模，應由本處諮詢及彙整有關機關代表、學者專家、產業部門及相關社會團體之意見後訂定，並由行政院核定之。

第一項第六款所稱資通安全相關業務，包含勾稽通訊保障及監察法所稱監察通訊所得資料、傳送至臺灣高等法院通訊監察管理系統之資料，及由監察設備執行通訊監察作業後自動生成之指令記錄檔，以確認通訊監察執行機關之資通安全。

程演練等）；

7. 緊急應變及處理復原；
8. 加強國際交流合作；
9. 推升產業能量（如每年進行商業服務重點產業個資管理、資安應用調查、法令規範及需求盤點等）等項目納入本處業務職掌。

三、在美國法規中，規定白宮管理與預算辦公室（Office of Management and Budget）負責：

1. 制定資訊安全政策、標準與指南，並監督其實作，如電腦安全事件處理指引（Computer Security Incident Handling Guide）等；
2. 要求聯邦各機關（構）建置資訊安全保證措施；
3. 監督聯邦各機關（構）之資訊安全計畫；
4. 向國會提出聯邦各機關（構）之資安工作執行狀況；
5. 確保聯邦資訊安全事件處理中心（Federal Information Security Incident Center）有效運作，提供各機關（構）即時性的技術服務，協助偵測、處理、分析資通安全事件。

另以德國法規為例，第三條「聯邦辦公室的職責（Tasks of the Federal Office）」包含：

1. 預防對聯邦資訊科技安全之威脅；
2. 蒐集、分析及研究資通安全風險與防範之資訊，並根據其他機關（構）之需要提供報告及協助；
3. 制定資通安全程序及設備之安全防範規則；
4. 制定標準、程序及工具以測試及評估資通安全系統之安全性；
5. 提供資訊、加密技術及安全管理系統等諮詢及支援給各級政府機關（構，且包含地方政府）；
6. 建立適當溝通管道，在事件早期即可予私人企業協調合作，保護關鍵基礎設施等。

| | |
|---|---|
| | 四、參考國際將資安通報的配合義務延伸至民間企業、並希望在公私部門間建立資訊共享機制的趨勢，如美國前總統柯林頓第 63 號總統決策令（Presidential Decision Directive）指出，一方面建立政府與民間之對口機關國家基礎建設保護中心（National Infrastructure Protection Center）外，也鼓勵私部門自發性設立資訊分享與分析中心（Infromation Sharing and Analysis Center），以促進公私部門間就資安業務之資訊分享，爰納入一定規模以上、具有國家關鍵基礎設施屬性之民間企業，為本法規範之範圍內。<br>五、鑑於資通安全相關議題攸關國家安全及國民權益，並考量民間企業普遍未能有效落實資通安全技術及管理制度於企業運作實務中，爰訂定相關規定，賦予主管機關提供技術諮詢與支援、人才培育、資通安全意識及知識推廣、相關法令政策等資料之蒐集、彙整及分析等任務，期使主管機關透過綜理相關業務，有效提升我國資安防禦能量及競爭力。<br>六、由於現行通訊保障及監察法第十八條規定「依本法監察通訊所得資料，不得提供與其他機關（構）、團體或個人」，為避免本法防護及稽核範圍受限，爰此特擬定第五項條文，將通訊監察所得資料納入本法規範。<br>另，法務部調查局通訊監察設備執行通訊監察作業後自動生成之指令記錄檔，目前僅依時序寫入伺服器硬碟中並保留 180 日，且僅由擁有資料庫管理者權限（Administrator）者可進行檢視與管理，並未供外部單位查核及比對，顯見其資通安全管理措施並未臻完善，有透過資通安全專業人員及機構介入協助之必要。<br>因此，為確保通訊監察執行機關之資通安全防護措施，有無徹底落實、達成資通安全三大目的（可用性、保密性及完整性），爰此特擬定本處除應稽核監察通訊所得資料之外，另應稽核通訊監察管理系統之系統紀錄檔並加以勾稽，以確認所有 |

| | |
|---|---|
| | 通訊監察資料均有受到完整防護。 |
| 第七條　（中央政府各級機關、地方政府及一定規模以上、具有國家關鍵基礎設施屬性之民間企業應訂定資通安全管理規定）<br>中央政府各級機關、地方政府及一定規模以上、具有國家關鍵基礎設施屬性之民間企業應依前條所稱之政策、法令、標準作業流程及技術規範等，訂定資通安全管理規定，並推動實施之。<br>前項所稱資通安全管理規定，應包含：<br>一、資通安全管理單位之組織、權責、分工及資源規劃。<br>二、資通安全管理人員之編制、評估、訓練及考核。<br>三、資訊系統購置、分級、維護、加密、授權、接觸、存取、傳輸、使用者註冊管理制度、密碼管理及監控等規範。<br>四、除前項規定之規範外，針對關鍵基礎設施及機密資料，應另定其認定標準、實體及虛擬環境管理之方式。<br>五、資通安全事件之分級、通報、證據保全、處置及相關程序。<br>六、其他有關資通安全之事項。<br>中央政府各級機關及地方政府應每年檢討資通安全管理規定之執行狀況，做成資通安全管理規定稽核報告，由本處彙整後提交立法院備查。<br>第一項所稱一定規模以上、具有國家關鍵基礎設施屬性之民間企業，應每年檢討資通安全管理規定之執行狀況，並依證券交易法及相關規定，納入年報。 | 一、參考美國聯邦資訊安全管理法規定，聯邦各機關（構）應：<br>1. 評估各自單位之資通安全風險、確定其等級、提供與其資訊系統相符之資通安全防護措施；<br>2. 部署資通安全之負責專人與組織，展開資通安全相關工作；<br>3. 遵循有關政策規定，將資通安全工作納入其機關（構）之規劃與運作等。<br>二、參考美國聯邦資訊安全管理法規定，所有聯邦機關（構）所使用之資訊系統，須符合其風險管理框架（Risk Management Framework）之安全生命週期（Security Life Cycle），投注足夠人力與預算，決定所使用之資訊系統與其處理、儲存、傳輸之資訊的敏感性；識別及規劃資訊系統之適當安全控制措施；訂定組織內資訊系統之安全控制措施；評估資訊系統安全控制措施之有效性；並持續監控及隨時通報資通安全系統變化等相關事項。<br>三、參考美國聯邦資訊安全管理法之要求，各機關（構）需每年評鑑其資訊安全計畫與實作之工作成果，並將評鑑報告送交白宮管理與預算辦公室，再由白宮管理與預算辦公室彙整後編制成總報告提交國會審查。<br>四、參考我國政府機關（構）資通安全責任等級分級作業規定，不同層級或業務單位因所持有之資料不同，其資安責任等級及其在政策面、管理面、技術面及人員之訓練要求等應辦事項均不同，爰特擬定資訊系統及資通安全事件之分級，以達資源有效利用之目的。<br>五、民間企業於一定規模以上、具有國家關鍵基礎設施之屬性者，因其資通安全措施與其經營成效有所關連，與投資人、員工、主管機關等利害關係人之關係甚密，故亦應比照政府機關設置資安專責機構及技術人員，並將其資安有關作為向利害關係人周知。 |
| 第三章　組　　織 | 章名 |

| | |
|---|---|
| 第八條　（組織法及編制表另定之）<br>本處組織、各職稱之官等職等及員額，另以組織法及編制表定之。 | 本條授權主管機關依本法所列業務項目及其需求，制定組織法及編制表，執行相關業務。為求資通安全工作之落實，主管機關應參考德國聯邦資訊安全辦公室（Federal Office for Information Security）或其他先進國家資通安全主管機關之組織及編制，充實其技術、政策、法規、倫理、市場等方向之研究、發展及應用能力。 |
| 第九條　（人員聘用相關規定）<br>本處因業務需要，得依聘用人員聘用條例之規定，另訂定公開、公平之資格審查方式，適度放寬公務人員任用之限制，聘用對資通安全有專門研究之專業或技術人員。<br>本處對於其所進用且從事稀少性、危險性、重點研究項目或於特殊環境工作之專業或技術人員，應優予待遇、提供保險或採取其他必要措施。<br>第一項所稱資格審查方式及聘用人員之教育培訓、技能檢定、績效評估及人事任免等相關規定，由本處訂定後送行政院核定之。<br>第一項聘用之專業或技術人員，必要時應由本處依公務人員任用法及相關規定辦理特殊查核，確保其品德及對國家之忠誠。 | 一、我國資訊人力約佔全國機關員額之 1.5%，相較於民間企業、學校在學及畢業生人數、以及美國聯邦政府（資訊人力佔約 5%）均顯著不均。<br>二、究其原因，受限於公務人員任用及銓敘等相關規定，民間企業往往提供較優之待遇及福利，造成政府不易招募及任用資通安全相關專業或技術人員。爰此於本條第一款及第二款，參酌科學技術基本法第十五條及第十七條之規定，賦予主管機關另訂聘用資格及待遇條件之權限。<br>三、然而，主管機關之業務涉及我國資通安全政策、技術等規範之制定、修正及執行，部分業務有其機密性，且其人員之能力須跟上國際最新技術演進，方可為我國設計與時俱進之資通安全防護機制，爰此於本條第三款、第四款訂定資格審查、教育培訓、技能檢定、績效評估、人事任免及必要時應辦理特殊查核之規定，有效確保我國負責資通安全業務之專業及技術人員之能力與忠誠。 |
| 第四章　附　　則 | 章名 |
| 第十條　（獎勵民間研發、教育及推廣之財政優惠措施）<br>為促進民間資通安全之研究、發展、應用、教育及推廣，政府得提供租稅、金融等財政優惠措施及必要之支助。 | 明定政府得提供財政優惠措施或其他必要之支助，提供民間投注資源研究、發展、應用、教育及推廣資通安全相關技術。 |
| 第十一條　（重大施政計畫應提出資通安全影響評估）<br>政府重大施政計畫應提出資通安全影響評估。<br>本處應協助中央政府各級機關及地方政府提出前項所稱資通安全影響評估。 | 明訂各級政府於推行重大施政計畫前，應一併提出資通安全影響評估，以便在主管機關之協助下，及早指認施政計畫中涉及資通安全之事項，並據以提出行動方案或修訂施政計畫。影響評估應包含事項及程序，由主管機關另定之。 |

| | |
|---|---|
| 第一項所稱資通安全影響評估應包含事項及程序等，由本處另定之。 | |
| 第十二條　（相關法令調適期限）<br>本處應於本法施行後兩年內，依本法之原則修正、制定或廢止相關法令。 | 本法施行後，相關法規之競合與調適問題，應由主管機關於兩年內予以盤點及研議，適時提出法律修正、制定或廢止案。 |
| 第十三條　（施行日期）<br>本法自公布日施行。 | 本法施行日期。 |