

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 20998 號

案由：本院委員許毓仁等 17 人，有鑑於數位及其他資通科技應用之普及，資通安全議題日益受到重視，且公務機關所承擔之公共任務對國家安全、民眾生活及經濟活動有重大影響，如未能考量自身資通安全風險，進而逐步提升自身資通安全保護機制，一旦遭受駭客惡意攻擊，恐造成難以回復之損害，為縝密我國公務機關整體資通安全維護機制及資通安全意識，以保障國家安全與公共利益，爰增訂資通安全管理法草案予以規範。至於非公務機關部分，參酌美國聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014）對於非公務機關並無予以管制規範，為尊重民間自律，本草案僅以公務機關作為管制對象，以鼓勵民間企業對於資通安全保護之自律及自主。是否有當？敬請公決。

提案人：許毓仁

連署人：王育敏 廖國棟 林麗蟬 孔文吉 張麗善
鍾佳濱 管碧玲 劉權豪 江永昌 李彥秀
鄭天財 Sra Kacaw 盧秀燕 楊鎮浚 許淑華
蔣萬安 洪慈庸

資通安全管理法草案總說明

- 一、公務機關所承擔之公共任務對國家安全、民眾生活及經濟活動有重大影響，如未能考量自身資通安全風險，進而逐步提升自身資通安全保護機制，一旦遭受駭客惡意攻擊，恐造成難以回復之損害，為縝密我國公務機關整體資通安全維護機制及資通安全意識，以保障國家安全與公共利益，爰增訂資通安全管理法草案予以規範。
- 二、參酌美國聯邦資訊安全現代化法（Federal Information Security Modernization Act of 2014）對於非公務機關並無予以管制規範，為尊重民間自律，本草案僅以公務機關作為管制對象，以鼓勵民間企業對於資通安全保護之自律及自主。
- 三、鑒於資通安全之提升須以全民重視為前提，並須佐以先進之資通安全技術、軟硬體、專業人才等資源，政府應與民間共同提升全民資通安全意識，推動資通安全產業，以利先進資通安全技術、軟硬體、專業人才等之發展，爰參考日本網路安全基本法第十九條產業之振興及國際競爭力強化、第二十條研究開發之推動、第二十一條人才之確保等規定，為第三條之規範。
（草案第三條）
- 四、考量我國有關資通安全政策之推動所涉範圍甚廣，為利相關業務之推動，爰明定行政院應考量國家資通安全相關事務發展之需求，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等相關事宜，並要求行政院應定期公布國家資通安全情勢報告。（草案第四條）
- 五、考量公務機關之業務有其重要性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質有所不同，故要求行政院應衡酌公務機關之不同情勢，訂定資通安全責任等級，並針對其分級基準、等級變更申請、義務內容、專責人員之設置，訂定相關辦法。（草案第五條）
- 六、為增進與改善我國境內面對資通安全威脅與風險之應變能力及策略擬定，應建立相關資通安全情資分享機制，爰為第一項賦予行政院應建立資通安全情資分享機制。（草案第六條）
- 七、為確保公務機關之資通安全，避免因人為疏失、蓄意或自然災害等風險，致機關資通系統或資訊遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務，公務機關應符合第五條所定資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫，爰為本條規定。公務機關訂修及實施上開計畫，應衡酌機關資源之合理分配，並依循上級或監督機關之相關資通安全規定為之。（草案第八條）
- 八、參考日本網路安全基本法第十二條有關促進地方公共團體確保網路資訊安全相關事項之規定，及同法第三十條規定相關行政機關之首長應適時提供與網路資訊安全相關之資料或資訊，以

立法院第 9 屆第 4 會期第 1 次會議議案關係文書

利執行所掌事務之精神，明定公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形，以確認其實施成效，並使上級或監督機關得了解及稽核所屬或受監督機關之年度資通安全維護情形。（草案第十條）

九、公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形；受稽核機關之資通安全維護計畫實施有缺失或待改善者，應向稽核機關及上級或監督機關提出改善報告，以確保資通安全維護計畫之落實及政府資通安全維護之強度。（草案第十一條）

十、為即時掌控資通安全事件，並有效降低其所造成之損害，爰於第一項規定公務機關應建立資通安全事件之通報及應變機制；且公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院。（草案第十二條）

十一、公務機關所屬人員於踐行本法要求事項成果優良或卓越時，應予獎勵；如因故意或過失，未踐履本法所定資通安全義務時，應受懲戒或懲處；如有其他違反資通安全義務而涉及民事或刑事責任之情形時，仍應依各該相關法律處理之。（草案第十三條）

資通安全管理法草案

條	文	說	明
		章名。	
<p>第一章 總則</p> <p>第一條 為積極推動國家資通安全政策，加速建構國家資通安全環境，帶動資通安全產業發展，以保障國家安全，維護社會公共利益，特制定本法。</p>		<p>一、明定本法之立法目的。</p> <p>二、隨著數位及其他資通科技應用之普及，資通安全議題日益受到重視。為有效將我國之資通安全管理政策落實於公部門，以建構安全之資通環境，進而保障國家安全，維護社會公共利益，特制定本法。</p>	
<p>第二條 本法用詞，定義如下：</p> <p>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理、使用或分享之系統。</p> <p>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。</p> <p>三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。</p> <p>四、公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。</p>		<p>第一項明定本法用詞定義：</p> <p>一、參考美國國家標準技術研究所 SP800-60 Volume I：Guidfor Mapping Type of Information and Information System to Security Categories 及經濟部標準檢驗局公布國家標準 CNS 27001「資訊技術—安全技術—資訊安全管理—要求事項」等文件，於第一款至第三款規定資通系統、資通服務及資通安全之定義。</p> <p>二、第四款所規範之公務機關，係指依法行使公權力之中央、地方機關（構）或公法人，例如總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、公立社會教育機構、公立文化機構、公立醫療機構或行政法人等。另考量軍事機關及情報機關之性質特殊，其資通安全管理宜由該等機關另行規定，故定明非屬本法所稱公務機關。</p>	
<p>第三條 為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：</p> <p>一、資通安全專業人才之培育。</p> <p>二、資通安全科技之研發、整合、應用、產學合作及國際交流合作之推動。</p> <p>三、資通安全產業之發展及推動。</p> <p>四、資通安全軟體技術規範、相關服務與審驗機制之發展及推動。</p>		<p>一、鑒於資通安全之提升須以全民重視為前提，並須佐以先進之資通安全技術、軟硬體、專業人才等資源，政府應與民間共同提升全民資通安全意識，推動資通安全產業，以利先進資通安全技術、軟硬體、專業人才等之發展，爰參考日本網路安全基本法第十九條產業之振興及國際競爭力強化、第二十條研究開發之推動、第二十一條人才之確保等規定，為本條規範。</p> <p>二、關於租稅優惠措施，因事涉國家稅收，且現行已有產業創新條例、科學技術基本法等法律相關規定可資運用，爰不另於本法規範，併予敘明。</p>	

立法院第 9 屆第 4 會期第 1 次會議議案關係文書

<p>第四條 行政院應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等相關事宜，並應定期公布國家資通安全情勢報告及資通安全發展方案。</p>	<p>一、考量我國有關資通安全政策之推動所涉範圍甚廣，為利相關業務之推動，爰明定行政院應考量國家資通安全相關事務發展之需求，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等相關事宜。</p> <p>二、為使各界了解國家資通安全趨勢，明定行政院應定期公布國家資通安全情勢報告。</p>
<p>第五條 行政院應衡酌公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由行政院定之。</p>	<p>考量公務機關之業務有其重要性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質有所不同，故要求行政院應衡酌公務機關之不同情勢，訂定資通安全責任等級，並針對其分級基準、等級變更申請、義務內容、專責人員之設置，訂定相關辦法。</p>
<p>第六條 行政院應建立資通安全情資分享機制。</p> <p>前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由行政院定之。</p>	<p>一、為增進與改善我國境內面對資通安全威脅與風險之應變能力及策略擬定，應建立相關資通安全情資分享機制，爰為第一項賦予行政院應建立資通安全情資分享機制。</p> <p>二、第二項定明資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由行政院定之，以資遵循。</p>
<p>第七條 公務機關於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。</p>	<p>考量公務機關於本法適用範圍內委外辦理資通系統建置、維運或資通服務之提供時，應依所委外項目之性質與資通安全需求，選任適當之受託者，並就受託者之資通安全維護為監督，以確保國家安全、社會公共利益或個人權益，爰為本條規定。相關監督事項之技術性及細節性內容，將於施行細則中規定。</p>
<p>第二章 公務機關資通安全管理</p>	<p>章名。</p>
<p>第八條 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p>	<p>一、為確保公務機關之資通安全，避免因人為疏失、蓄意或自然災害等風險，致機關資通系統或資訊遭不當使用、洩漏、竄改、破壞等情事，影響及危害機關業務，公務機關（包含總統府、行政院、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府與其所屬或監督之各級公務機關及直轄市議會、縣（市）議會等）應符合第五條所定資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，</p>

	<p>訂定、修正及實施資通安全維護計畫，爰為本條規定。公務機關訂修及實施上開計畫，應衡酌機關資源之合理分配，並依循上級或監督機關之相關資通安全規定為之。</p> <p>二、有關資通安全維護計畫之內容，將由行政院訂定範本，提供各公務機關參考，以利執行。</p>
<p>第九條 公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。</p>	<p>為確保有效推動資通安全維護事項，公務機關應置資通安全長，由其成立相關推動組織及督導推動相關工作。考量資通安全長如由副首長擔任，更能提升資通安全於機關中之重要性，並參考美國二〇一四年聯邦資訊安全現代化法 § 3554 關於資訊長應指定資深資安專責人員負責相應事務規定之意旨，爰為本條規定。</p>
<p>第十條 公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交行政院。</p>	<p>參考日本網路安全基本法第十二條有關促進地方公共團體確保網路資訊安全相關事項之規定，及同法第三十條規定相關行政機關之首長應適時提供與網路資訊安全相關之資料或資訊，以利執行所掌事務之精神，明定公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形，以確認其實施成效，並使上級或監督機關得了解及稽核所屬或受監督機關之年度資通安全維護情形。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應將資通安全維護計畫實施情形送交行政院。行政院收受上開計畫實施情形後將予以備查，並得視情形提供必要協助。</p>
<p>第十一條 公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。</p> <p>受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。</p>	<p>一、第一項規定公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。各公務機關對於其所屬或監督之各級公務機關，應依其機關層級、業務及其他相關情形，就稽核之基準、頻率、內容與方法訂定相關行政規則，以利執行。稽核時，宜考量受稽核者歷來接受行政院、上級或監督機關稽核之頻率與結果等因素，決定最適之受稽核者。</p> <p>二、第二項規定受稽核機關之資通安全維護計畫實施有缺失或待改善者，應向稽核機關</p>

	<p>及上級或監督機關提出改善報告，以確保資通安全維護計畫之落實及政府資通安全維護之強度。</p>
<p>第十二條 公務機關為因應資通安全事件，應訂定通報及應變機制。</p> <p>公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院；無上級機關者，應通報行政院。</p> <p>公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交行政院；無上級機關者，應送交行政院。</p> <p>前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由行政院定之。</p>	<p>一、為即時掌控資通安全事件，並有效降低其所造成之損害，爰於第一項規定公務機關應建立資通安全事件之通報及應變機制。所稱資通安全事件，係指資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，致有無法符合機密性、完整性及可用性之事件；其具體類型將於施行細則及本條第四項授權訂定之辦法中規範。</p> <p>二、參考日本網路安全基本法第十八條政府相關組織就有重大網路安全影響之虞之事件有相互合作、分享資訊並採取必要措施之義務之規定，於第二項明定公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報行政院。另因總統府、立法院、司法院、考試院、監察院、直轄市政府、縣（市）政府、直轄市議會及縣（市）議會等公務機關無上級機關，爰規定無上級機關者應通報行政院。</p> <p>三、考量公務機關於知悉資通安全事件後，應進行調查、處理及改善工作，爰於第三項規定公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交行政院，以利上級機關、監督機關或行政院監督，並得據以提供必要之協助。</p> <p>四、關於公務機關資通安全事件之通報及應變，目前有「國家資通安全通報應變作業綱要」可資遵循參考，於本法施行後，應檢視原有機制並依本法要求調整之，故第四項授權行政院訂定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，以利公務機關適用。</p>
<p>第十三條 公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。</p> <p>公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。</p>	<p>公務機關所屬人員關於資通安全事務之獎懲本有公務人員考績法、公務員懲戒法等規定加以規範，惟為促進該等人員對於資通安全工作之重視與投入，爰為本條規定。公務機關所屬人員於踐行本法要求事項成果優良或卓越時，應予獎勵；如因故意或過失，未踐履本法所定資</p>

立法院第 9 屆第 4 會期第 1 次會議議案關係文書

	通安全義務時，應受懲戒或懲處；如有其他違反資通安全義務而涉及民事或刑事責任之情形時，仍應依各該相關法律處理之。
第三章 附則	章名。
第十四條 本法施行細則，由行政院定之。	本法施行細則之訂定機關。
第十五條 本法施行日期，由行政院定之。	本法施行日期，考量配套子法作業時程，並為周延法制，以落實本法規定之執行，爰授權由行政院定之。