資通安全管理法草案總說明

隨著網際網路及其他資通科技之快速發展與普及，資通科技相關應用，已被世界各國視為協助產業經濟轉型及有效解決社會發展議題之關鍵，各國亦紛紛致力於資通政策之規劃，期能建構公開、有效率之數位環境，並希望藉由科技化服務，提升民眾生活品質、維護公共利益、帶動產業發展及國家整體競爭力。

政府資通政策之擘劃，除應重視促成產業轉型、解決社會發展議題等成就特定目標之面向外，亦應讓資通科技應用所代表之科技創新思維，能真正滲透、深入民眾生活，並與社會脈絡動態共生，進而延伸啟發更多元、寬廣且不受限於框架之創新。政府資通政策如要成為此類循環、突破式創新之沃土，必須向最基礎、最根本處，即確保資通安全去尋求。唯有透過系統化之資通安全風險管理，消弭足以破壞資通安全之因素或削弱其影響力至可接受之範圍，民眾與整體社會才能屏除對資通科技之疑慮，投入其應用與創新，促成資通科技之持續進展與突破。

資通安全之確保除能塑造鼓勵持續創新之環境外，對國家安全及社會公益之確保亦有其重要性。近年來，對於公務機關或關鍵基礎設施等進行網路攻擊之情形時有所聞，由於公務機關所承擔之公共任務，及關鍵基礎設施提供者等非公務機關所維運或提供之服務，均對國家安全、民眾生活、經濟活動等有重大影響，該等機關如未能考量自身資通安全風險，進而決定資通安全管理之作法，逐步提升自身資通安全能量，一旦其遭受惡意攻擊，恐造成難以回復之損害。

參諸國際近年資通安全之政策，許多先進國家係以制定專法之方式對資通安全議題加以規範，例如：美國有聯邦資訊安全現代化法、網路安全法，日本則制定網路安全基本法，在國際組織部分，歐盟亦訂定網路與資訊系統安全指令；透過專法之制定，協助公務機關及關鍵基礎設施提供者等非公務機關，認知自身資通安全責任、進而理解並因應資通安全風險，增進自身資通安全能力。

我國目前與資通安全相關之規範，適用於公務機關者，除適用對象較為廣泛之刑法妨害電腦使用罪罪章及個人資料保護法等外，另有行政

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、國家資通安全通報應變作業綱要等規定。上述規定中，屬法律者，其規範目的各異，而適用時或僅就實害之結果進行處罰，或其保護客體僅以特定類型之資料為限，並非針對資通安全管理為整體考量而制定；其餘規定對資通安全管理雖定有較細節之規範，但其位階較低，且規定分散，適用上難免不足。至於適用於非公務機關之規定，因其立法目的不同，其適用範圍、保護客體與規範對象亦有差異，無法作為各非公務機關共通遵循之標準，難以帶動其整體資通安全能量。此外，無論是適用於公務機關或非公務機關之規定，均無以資通安全為主要考量，並要求以風險管理為核心，建立完整資通安全維護計畫及通報應變相關機制者，此現況與國際上目前資通安全管理之趨勢尚有落差。

綜上說明，制定一部協助公務機關及受規範之非公務機關認知自身資通安全風險並加以因應，訂定及實施資通安全維護計畫以確保其資通安全、逐步提升自身資通安全能量之專法，遂成現階段建構、提升資通安全環境最有效率之規範面政策選擇。為達成上述目的，並使行政院統籌分配資源、整合民間力量，提升我國整體資通安全環境及資通安全意識，保障國家安全與公共利益，爰擬具「資通安全管理法」（以下簡稱本法）草案，其要點如下：

一、本法之立法目的及用詞定義。（草案第一條及第二條）

二、政府應整合民間力量推動資通安全相關事項。（草案第三條）

三、行政院應規劃及推動國家整體資通安全政策等事宜、公告國家資通安全情勢報告及資通安全發展方案;並得委任或委託其他公務機關、法人或團體辦理資通安全相關事務。（草案第四條及第五條）

四、行政院應訂定資通安全責任等級分級辦法，並得稽核非公務機關之資通安全維護情形；受稽核機關應就缺失或待改善事項完成改善報告，送交行政院、中央目的事業主管機關或直轄市、縣（市）政府。（草案第六條）

五、行政院應建立資通安全情資分享機制，並訂定相關事項之辦法。（草案第七條）

六、公務機關及非公務機關，於本法適用範圍內，委外辦理資通系統或資通服務事宜時，應就受託者之資通安全維護為監督。（草案第八條）

七、公務機關應考量其所屬資通安全責任等級之要求及保有或處理之資訊種類等條件，訂定、修正及實施資通安全維護計畫，並向上級或監督機關提出該計畫之實施情形。（草案第九條及第十一條）

八、公務機關應由其首長指派副首長或適當人員擔任資通安全長，負責推動及監督機關內資通安全相關事務。（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；受稽核機關應就缺失或待改善事項完成改善報告，送交稽核機關及上級或監督機關。（草案第十二條）

十、公務機關應訂定資通安全事件之通報及應變機制，於知悉事件時，向上級機關、監督機關或行政院通報，並分別向上級機關、監督機關或行政院提出事件之調查、處理及改善報告。（草案第十三條）

十一、公務機關所屬人員就資通安全維護之獎懲。（草案第十四條）

十二、中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，報請行政院核定。關鍵基礎設施提供者應訂定、修正、實施資通安全維護計畫，並向中央目的事業主管機關或直轄市、縣（市）政府提出該計畫之實施情形；如經稽核發現缺失，應提出改善報告送交中央目的事業主管機關或直轄市、縣（市）政府。（草案第十五條）

十三、關鍵基礎設施提供者以外之非公務機關，應訂定、修正、實施資通安全維護計畫；中央目的事業主管機關或直轄市、縣（市）政府得要求該等非公務機關提出計畫實施情形，並得進行稽核，發現有缺失者，應要求受稽核機關提出改善報告。（草案第十六條）

十四、非公務機關應訂定資通安全事件之通報及應變機制，於知悉事件時向中央目的事業主管機關或直轄市、縣（市）政府通報，並應向中央目的事業主管機關或直轄市、縣（市）政府提出事件之調查、處理及改善報告；如為重大資通安全事件者，其報告並應送行政院。行政院、中央目的事業主管機關或直轄市、縣（市）政府，於適當時機得公告與重大資通安全事件相關之必要內容及因應措施，並提

供協助。（草案第十七條）

十五、中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護計畫發現重大缺失，或遇重大資通安全事件，認有必要時，得進入受稽核或發生重大資通安全事件之非公務機關場所檢查；非公務機關及相關人員無正當理由不得規避、妨礙或拒絕；參與檢查之人員就因而知悉之他人秘密資訊，應負保密義務。（草案第十八條）

十六、非公務機關違反本法相關規定之罰則。（草案第十九條至第二十一條）

資通安全管理法草案

條　　文	說　　明
第一章　總則	章名。
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。	一、明定本法之立法目的。 二、隨著數位及其他資通科技(Information Communication Technology)應用之普及，資通安全議題日益受到重視。為有效規劃我國之資通安全管理政策，落實於公、私部門，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。
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。 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。 五、非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 六、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，並經行政院公告者。 七、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，依第十五條第一項規定經中央目的事業主管機關或直轄市、縣（市）政府指定，並報行	一、第一項明定本法用詞定義： (一)參考美國國家標準技術研究所（National Institute of Standards and Technology）SP800-60 Volume I: Guild for 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。 (二)第四款及第五款規定公務機關及非公務機關。公務機關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；該等機關之範圍，將於施行細則中規範。非公務機關則包括關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 (三)參考美國 31 CFR 800.208 所定關鍵基礎設施（critical infrastructure)、日本網路安全基

政院核定之非公務機關。 前項第五款所稱政府捐助之財團法人，其範圍於施行細則中定之。	本法（サイバーセキュリティ基本法）第三條所定重要社會基礎業者、韓國情報通信基礎保護法(정보통신기반보호법)第二條所定情報通信基礎設施等定義，於第六款明定關鍵基礎設施之內涵，並考量關鍵基礎設施因應環境與時代變遷，其範圍可能調整，故規定由行政院公告之。依據行政院訂定之「國家關鍵基礎設施安全防護指導綱要」，關鍵基礎設施之範圍分為能源、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、高科技園區等八大功能領域，其下並各分為數項次領域及重要元件設施；因前揭指導綱要每兩年將定期檢視調整，關鍵基礎設施之範圍，亦將配合修正調整。 (四)考量關鍵基礎設施對國家安全、社會公共利益、國民生活及經濟活動有重大影響，然各維運關鍵基礎設施之非公務機關其屬性及重要性仍有不同，爰於第七款規定關鍵基礎設施提供者為由中央目的事業主管機關或直轄市、縣（市）政府指定其中具重要性者，並報行政院核定之非公務機關。 (五)提供或維運關鍵基礎設施之全部或一部者，如屬本法所定義之公務機關，應遵循本法有關公務機關之規定；至其他關鍵基礎設施之提供者，則應遵循本法有關關鍵基礎設施提供者之規定。 (六)非提供或維運關鍵基礎設施功能或重要元件設施，而僅提供關鍵基礎設施所需用之其他設備或服務者，雖非本法所稱關鍵基礎設施提供者，但如其係受關鍵基礎提供者委託辦理資通系統之建置、維運或資通服務之提供時，仍應依本法第八條規定，受委託者之監督。 二、有關本法規範之政府捐助之財團法人,其範圍宜與財團法人相關規定內涵一致，爰為第二項規定；未來將參

	考財團法人法草案第二條第二項及第三項規定,於施行細則中定明其範圍。
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： 一、 資通安全專業人才之培育。 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。 三、 資通安全產業之發展及推動。 四、 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。	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。 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。
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。	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。 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，另配合國家資通安全政策之推動，原則以四年為一期，公布資通安全發展方案。
第五條　行政院得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。	一、 除政策制定等本質上不宜委任或委託辦理之事務外，行政院為推動資通安全業務，如有需要，得依行政程序法第十五條或第十六條規定，委任或委託其他公務機關、法人或團體辦理。為利實務運作，爰為本條規範。又委外事務倘不涉及公權力之移轉，例如國際法規或國際政策之研析，或雖為資通安全整體防護或國際交流等事項而未有公權力移轉之情形時，則仍應依政府採購法等規定辦理。 二、 行政院依本條規定為委任或委

	託，因涉及公權力之移轉，應考量事務之性質、對象之屬性等事項，先行評估委任或委託辦理之適當性後，再行為之。
第六條　行政院應衡酌公務機關及非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。 行政院得稽核非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由行政院定之。 非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向行政院提出改善報告，並送中央目的事業主管機關或直轄市、縣（市）政府。	一、 考量公務機關與非公務機關之規模及業務性質不一，其應遵行之資通安全責任等級亦應有不同，此外，資通安全責任等級宜因機關調整、裁撤、業務變動或運用之資通系統發生重大變更等事由，而有所調整，以達到資通安全防護之最適效果。就此，目前有「政府機關（構）資通安全責任等級分級作業規定」可作為遵循之參考；於資通安全管理法制化後，上述諸事宜亦應加以規定，爰於第一項明定行政院應衡酌公務機關及非公務機關業務等事項，訂定資通安全責任等級之分級，並就其分級基準、等級變更申請、義務內容及專責人員之設置及其他相關事項，授權該院訂定辦法規範。 二、 為監督非公務機關實施資通安全維護計畫之情形，爰為第二項規定，並授權行政院訂定稽核頻率、內容與方法及其他相關事項之辦法。行政院依本項進行稽核時，應考量稽核對象之責任等級、其過往資通安全維護狀況、歷來接受行政院、中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率、結果及其他相關情形，決定最適之受稽核者名單。至於公務機關資通安全維護計畫實施情形之稽核，則於第十二條規範。 三、 考量非公務機關依第二項規定接受稽核後，經發現其資通安全維護計畫實施有缺失或待改善情形，宜由行政院及相關機關進行監督，確認改善之狀況，爰為第三項規定。
第七條　行政院應建立資通安全情資分享機制。 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	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，爰為第一項規定。

關事項之辦法，由行政院定之。	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。
第八條　公務機關或非公務機關，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。	考量公務機關或非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。
第二章　公務機關資通安全管理	章名。
第九條　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。	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）應符合第六條第一項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。 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。
第十條　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。	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（Federal Information Security Modernization Act of 2014）§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。
第十一條　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。	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。
第十二條　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。 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。	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。 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。
第十三條　公務機關為因應資通安全事件，應訂定通報及應變機制。 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。 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	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

告，並送交行政院；無上級機關者，應送交行政院。 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。	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。 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。 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。 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。
第十四條　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。 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。	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　非公務機關資通安全管理	章名。

第十五條　中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，並報請行政院核定之。 關鍵基礎設施提供者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。 關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形。 中央目的事業主管機關或直轄市、縣（市）政府應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。 關鍵基礎設施提供者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，送交中央目的事業主管機關或直轄市、縣（市）政府。 第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。	一、 第一項規定關鍵基礎設施提供者之指定。關鍵基礎設施提供者之資通安全維護，乃現今國際針對資通安全保護所重視之議題，爰參考歐盟二〇一六年「網路與資訊系統安全指令」(The Directive on security of network and information systems)第五條關於關鍵服務營運商之清單、第十四條關於關鍵服務營運商用以提供關鍵服務之網路與資訊系統，如有影響其安全之事件，關鍵服務營運商須採取適當措施及最小化事件之影響，以確保服務之持續性、美國 6 USC §132 指定關鍵基礎設施保護計畫(Designation of critical infrastructure protection program)及第一三六三六號行政命令有關改善關鍵基礎設施網路安全（Executive Order 13636）、日本網路安全基本法第六條重要社會基礎業者之職責、韓國情報通信基礎保護法第八條中央行政機關長官有權指定主要資訊通信基礎設施及同法第五條主要資訊通信基礎設施保護措施之制定等立法例，將關鍵基礎設施提供者納入本法之適用範圍。 二、 因關鍵基礎設施涉及國家安全、社會公共利益、國民生活及經濟活動，爰於第二項規定關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並訂定、修正及實施資通安全維護計畫，以確保其資通安全。 三、 為使中央目的事業主管機關及直轄市、縣（市）政府掌握所管關鍵基礎設施提供者之資通安全維護計畫實施狀況，爰於第三項規定關鍵基礎設施提供者應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫實施情形，以利中央目的事業主管機關或直轄市、縣（市）政府監督，並適時提

	供相關建議或協助。 四、 為確保資通安全維護計畫之落實，於第四項規定中央目的事業主管機關或直轄市、縣（市）政府應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。稽核時，宜考量受稽核者歷來接受行政院、中央目的事業主管機關或直轄市、縣（市）政府稽核之頻率與稽核結果等因素，決定最適之受稽核者名單與頻率。 五、 第五項規定關鍵基礎設施提供者之資通安全維護計畫實施情形有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關或直轄市、縣（市）政府，以確保資通安全維護計畫之落實。 六、 考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利關鍵基礎設施提供者適用與遵循，爰於第六項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 七、 中央目的事業主管機關宜訂定非公務機關資通安全維護計畫之範本，以供非公務機關參考；行政院並得提供必要之協助。
第十六條　關鍵基礎設施提供者以外之非公務機關，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。 中央目的事業主管機關或直轄市、縣（市）政府得要求所管前項非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關或直轄市、縣（市）政府得稽核所管第一項非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之非公務機關提出改善	一、 考量關鍵基礎設施提供者以外之非公務機關亦應負相當之資通安全責任，仍應訂定安全維護計畫並提出計畫實施情形，爰參考日本網路安全基本法第三條賦予重要社會基礎業者配合政府資通安全政策之協力義務之規定，於第一項明定該等非公務機關應符合其所屬資通安全責任等級之要求，並修訂及實施資通安全維護計畫。 二、 鑒於資通安全維護事項與事業之經營管理關係密切，對於非公務機關資通安全維護之指導、監督、管理及稽核，宜由各非公務機關之中央目的事業主管機關或直轄市、縣

報告。 前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請行政院核定之。	（市）政府執行，爰為第二項及第三項規定。 三、 考量資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，其內容宜有一致性，以利第一項之非公務機關適用與遵循，爰於第四項規定，由中央目的事業主管機關擬訂，並報請行政院核定之。 四、 中央目的事業主管機關宜訂定非公務機關資通安全維護計畫之範本，以供非公務機關參考；行政院並得提供必要之協助。
第十七條　非公務機關為因應資通安全事件，應訂定通報及應變機制。 非公務機關於知悉資通安全事件時，應向中央目的事業主管機關或直轄市、縣（市）政府通報。 非公務機關應向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交行政院。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由行政院定之。 知悉重大資通安全事件時，行政院、中央目的事業主管機關或直轄市、縣（市）政府，於適當時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。	一、 為使中央目的事業主管機關、直轄市、縣（市）政府及行政院即時掌握非公務機關之資通安全事件，監督及協助該等非公務機關進行緊急應變處置，並在最短時間內回復業務正常運作，爰參考歐盟二〇一六年「網路與資訊系統安全指令」第十四條事件通知、日本網路安全基本法第十四條促進重要社會基礎業者確保網路資訊安全、韓國情報通信基礎保護法第十六條於金融、通信等領域別之情報通信基礎設施業者得依法成立及運作情報共有、分析中心，作為有侵害事故時之即時警報與分析體系等規定，為第一項至第三項規定。有關資通安全事件之內涵，同第十三條說明一；重大資通安全事件之認定，將於施行細則中規範。 二、 第四項明定第一項至第三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由行政院定之，以利非公務機關依循。 三、 考量重大資通安全事件可能影響多數人民之生命、身體或財產安全，宜由行政院、中央目的事業主管機關或直轄市、縣（市）政府於知悉後，分別或共同公告必要之內容(例如發生原因、影響程度及目前控制

	之情形等)及因應措施,並提供相關協助,以利防範、避免損害之擴大,爰為第五項規定。
第十八條　中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護情形發現重大缺失，或遇重大資通安全事件，而認有必要時，得派員攜帶執行職務證明文件，進入非公務機關場所檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料。 對於前項之檢查，非公務機關及其相關人員無正當理由不得規避、妨礙或拒絕。 參與檢查之人員，對於因檢查而知悉之他人應秘密之資訊，負保密義務。	一、為落實非公務機關資通安全之維護，應賦予監督機關有命令、檢查及處分權，爰參考日本網路安全基本法第十五條第二項政府為促進民間業者採取自發性之措施得採取必要措施，與同法第十七條政府為取締犯罪及防止傷害之擴大得採取必要措施之規定，為第一項及第二項規定，以強化中央目的事業主管機關與直轄市、縣（市）政府之權責。 二、為保護個人資料及其他他人應秘密之資訊，爰於第三項明定因檢查而知悉他人應秘密之資訊者，應負保密義務。
第四章　罰則	章名。
第十九條　非公務機關有下列情形之一者，由中央目的事業主管機關或直轄市、縣（市）政府令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰： 一、未依第十五條第二項或第十六條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十五條第六項或第十六條第四項所定辦法中有關資通安全維護計畫必要事項之規定。 二、未依第十五條第三項或第十六條第二項規定，向中央目的事業主管機關或直轄市、縣（市）政府提出資通安全維護計畫之實施情形，或違反第十五條第六項或第十六條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。 三、未依第六條第三項、第十五條第五項或第十六條第三項規定，提出改善報告送交行政院、中央目的事業主管機關或直轄市、縣（市）政府，或違反第十五條第六項或第十六條第四項所定辦法中有關改善報告提出之規定。	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對非公務機關未依本法規定訂定、修正、實施資通安全維護計畫、提出資通安全維護計畫之實施情形、改善報告送交中央目的事業主管機關或直轄市、縣（市）政府、訂定資通安全事件之通報及應變機制、向中央目的事業主管機關、直轄市、縣（市）政府或行政院提出資通安全事件之調查、處理及改善報告，或違反資通安全事件通報內容之規定等情形，明定所課予之行政裁罰。

四、未依第十七條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十七條第四項所定辦法中有關通報及應變機制必要事項之規定。 五、未依第十七條第三項規定，向中央目的事業主管機關、直轄市、縣（市）政府或行政院提出資通安全事件之調查、處理及改善報告，或違反第十七條第四項所定辦法中有關報告提出之規定。 六、違反第十七條第四項所定辦法中有關通報內容之規定。	
第二十條　非公務機關未依第十七條第二項規定，通報資通安全事件，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十萬元以上一百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對非公務機關未依第十七條第二項規定，通報資通安全事件之情形，明定所課予之行政裁罰。
第二十一條　非公務機關違反第十八條第二項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣十萬元以上一百萬元以下罰鍰。	參考歐盟二〇一六年「網路與資訊系統安全指令」第二十一條要求會員國必須針對違反相關國家法規之行為，制定有效罰則之意旨，並考量違反本法所定行政法上義務應受責難程度及其所生影響，針對非公務機關無正當理由妨礙、規避或拒絕行政檢查之情形，明定所課予之行政裁罰。
第五章　附則	章名。
第二十二條　本法施行細則，由行政院定之。	本法施行細則之訂定機關。
第二十三條　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。