資通安全管理法施行細則草案總說明

「資通安全管理法」（以下簡稱本法）業於一百零七年六月六日制定公布，為落實及明確定義本法相關規定，爰擬具「資通安全管理法施行細則」（以下簡稱本細則）草案，其要點如下：

一、本細則訂定之依據。（草案第一條）

二、軍事機關及情報機關之定義。（草案第二條）

三、針對資通安全維護計畫實施情形稽核有缺失或待改善者，應提出改善報告之內容、方式及時間。（草案第三條）

四、委外辦理資通系統之建置、維運或資通服務之提供，於選任及監督受託者時應注意事項。（草案第四條）

五、本法及本細則之書面，依電子簽章法之規定，得以電子文件為之。（草案第五條）

六、資通安全維護計畫及其實施情形之內容應載明事項；該計畫之訂定、修正、實施及其實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關辦理。（草案第六條）

七、本細則所定核心業務及核心資通系統之範圍及定義。（草案第七條）

八、資通安全事件調查、處理及改善報告應載明之事項。（草案第八條）

九、中央目的事業主管機關指定關鍵基礎設施提供者應前，應給予其陳述意見之機會。（草案第九條）

十、重大資通安全事件之定義。（草案第十條）

十一、重大資通安全事件之公告方式、內容及相關限制。（草案第十一條）

十二、特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。（草案第十二條）

十三、本細則之施行日期。（草案第十三條）

資通安全管理法施行細則草案

條文	說明
第一條　本細則依資通安全管理法(以下簡稱本法)第二十二條規定訂定之。	明定本細則訂定之依據。
第二條　本法第三條第五款所稱軍事機關，指國防部及其所屬機關（構）、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款規定之機關。	參考國家情報工作法及檢察機關辦理刑事案件與軍事機關聯繫要點之規定，明定本法第三條第五款所稱軍事機關及情報機關之範圍。
第三條　公務機關或特定非公務機關（以下簡稱各機關）依本法第七條第三項、第十三條第二項、第十六條第五項或第十七條第三項提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形： 一、 缺失或待改善之項目及內容。 二、 發生原因。 三、 為改正缺失或補強待改善項目所採取管理、技術、人力或資源等層面之措施。 四、 前款措施之預定完成時程及執行進度之追蹤方式。	明定公務機關或特定非公務機關（以下簡稱各機關）之資通安全維護計畫實施情形經稽核發現缺失或待改善時，所提改善報告應包含之內容，以及後續執行情形之提出，說明如下： 一、第一款及第二款為該缺失或待改善事項之具體項目與內容及發生原因。 二、第三款所定措施，指因應缺失或待改善項目所採取之機關組織、作業程序、應變機制、人員管考、教育訓練、實體或虛擬設備等管理、技術、人力或資源等層面之相關措施。 三、第四款所定預定完成時程及執行進度之追蹤方式，指因應缺失或待改善項目所規劃採行相關措施之時程評估，及為確認其效果所進行之追蹤、管考。
第四條　各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項： 一、 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。 二、 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。 三、 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。 四、 受託業務涉及國家機密者，執行	一、依本法第九條規定，各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。為利執行，爰於第一項明定相關注意事項，說明如下： (一)為確保受託者辦理受託業務之程序及環境具安全性，並得妥善執行受託業務，爰為第一款及第二款規定。 (二)委託機關應依受託業務之性質，決定是否允許受託者就受託業務為複委託；如允許複委託，應注意得複委託之範圍與對象，及複

受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。 五、 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；如該資通系統屬委託機關之核心資通系統，或委託金額達一千萬元以上，委託機關並應自行或另行委託第三方進行安全性檢測；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。 六、 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。 七、 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。 八、 受託者應採取之其他資通安全相關維護措施。 九、 委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。 委託機關辦理前項第四款之適任性查核，應考量受託業務所涉及國家機密之機密等級、內容，就執行該業務之受託者所屬人員及可能接觸該國家機密之其他人員，於必要範圍內查核有無下列事項： 一、 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。 二、 曾任公務人員，因違反相關安全保密規定受懲戒或記過以上行政懲處。 三、 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。	委託之對象應具備之資通安全維護措施，爰為第三款規定。 (三)考量國家機密牽涉國家之安危或重大利益，應嚴加保護，爰於第四款明定受託業務涉及國家機密時，受託者辦理該項業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境，以利各機關謹慎審酌其辦理受託業務之合宜性及維護國家機密。 (四)為確保受託業務執行之適法性與安全性，受託業務如包含客製化資通系統之開發，應確保該資通系統之安全性，如委託金額達政府採購法勞務採購查核金額以上，或該資通系統為委託機關核心資通系統時，應由委託機關自行或委託公正之第三方進行安全性檢測之複測；且該業務如涉及利用非自行開發之系統或資源，受託者並應標示與揭露該系統或資源之內容與其來源，及提供授權證明，爰為第五款規定。 (五)受託者執行受託業務，有違反資通安全相關法令之情形，或知悉資通安全事件時，為避免損害擴大，應立即將相關情狀通知委託機關，並採行諸如啟動備援、回復運轉、損害管制等適當之補救措施，爰為第六款規定。 (六)為確保對於受託業務相關資料及系統之保護，受託者於委託關係結束時，應返還、移交、刪除或銷毀為履行契約所持有之資料，爰為第七款規定。 (七)委託機關就委外辦理之業務，得要求受託者依業務之性質及內容，調整其須具備之資通安全相關維護措施，爰為第八款規定。 (八)為確保受託業務執行之妥適性，委託機關應定期檢視執行狀況；於知悉受託者發生可能影響受託業務之資通安全事件時，亦應確

四、 其他與國家機密保護相關之具體項目。 第一項第四款情形，應記載於招標公告、招標文件及契約；於辦理適任性查核前，並應經當事人書面同意。	認受託業務之執行情形，爰為第九款規定。 二、適任性查核之對象應包括受託者之辦理該受託業務之人員及可能接觸該國家機密人員。而查核之項目則應考量上開業務所涉及之機密等級、內容，於必要範圍內查核之。各機關於辦理受託業務之委外時，若有第一項第四款之情事者，應於招標公告、招標文件、委外契約中敘明受託者辦理該項受託業務之人員及可能接觸該國家機密人員，應接受查核之項目，使其知悉並以書面同意，爰為第二項及第三項之規定。
第五條　前條第三項及本法第十六條第一項之書面，依電子簽章法之規定，得以電子文件為之。	明定本辦法及本法所定書面，依電子簽章法之規定，得以電子文件為之。
第六條　本法第十條、第十六條第二項及第十七條第一項之資通安全維護計畫，應包括下列事項： 一、 核心業務及其重要性。 二、 資通安全政策及目標。 三、 資通安全推動組織。 四、 專責人力及經費之配置。 五、 公務機關資通安全長之配置。 六、 資訊及資通系統之盤點，並標示核心資通系統及相關資產。 七、 資通安全風險評估。 八、 資通安全防護及控制措施。 九、 資通安全事件通報、應變及演練相關機制。 十、 資通安全情資之評估及因應機制。 十一、資通系統或服務委外辦理之管理措施。 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。 十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。 各機關依本法第十二條、第十六條第三項或第十七條第二項規定提出資通安全維護計畫實施情形，應包括前項各款之執行成果及相關說明。	一、 為利各機關訂定、修正及實施資通安全維護計畫，爰於第一項明定該計畫應包括之內容，說明如下： （一）各機關為有效落實其資通系統之安全管理，應釐清其核心業務，並說明該業務之重要性為何，爰為第一款規定。 （二）各機關依其業務性質推動資通安全維護事項，應建立資通安全政策，並應於各內部單位建立與資通安全政策一致之資通安全目標，爰為第二款規定。 （三）第三款至第五款明定計畫應包括機關內部推動資通安全事務之組織，與為達成資通安全政策及目標，所配置之專責人力及資源，公務機關並應配置資通安全長。 （四）各機關為有效推動資通安全管理，應盤點其資訊、資通系統，並應標示核心資通系統及相關資產，以利執行風險評估等作業，爰為第六款規定。 （五）第七款明定資通安全維護計畫之內容應包括資通安全風險評估相關之資訊，例如：機關應建立相關之風險評估準則，並了解諸如

第一項資通安全維護計畫之訂定、修正、實施及前項實施情形之提出，公務機關得由其上級或監督機關辦理；特定非公務機關得由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關辦理。	資訊儲存區域、組織面、實體面、技術面及作業面等資通安全風險；風險評估之範圍，包含第六款規定盤點之資訊、資通系統及相關資產。 （六）第八款明定資通安全維護計畫之內容應包括機關針對其資訊、資通系統及相關資產，所應採取之防護及控制措施。 （七）第九款明定資通安全維護計畫之內容應包括機關資通安全事件之通報、應變及演練相關機制。 （八）為強化各機關對於資通安全情資之應用，第十款明定機關應訂定相關機制，例如於收受資通安全情資後，應評估情資之內容，據以決定是否就資通安全維護計畫、資通安全事件之通報、應變方式或其他資通安全維護事宜為調整及因應。 （九）第十一款明定資通安全維護計畫應載明委外辦理資通系統或服務時之管理措施，以利執行本法第九條所定對受託者進行之監督。 （十）公務機關所屬人員辦理業務涉及資通安全事項者，應適時予以考核，爰於第十二款明定資通安全維護計畫應包含公務機關所屬人員辦理業務涉及資通安全事項之考核機制。 （十一）第十三款明定資通安全維護計畫應包含該計畫與實施情形之持續精進及績效管理機制，例如計畫合宜性、適切性及有效性之持續改善方式，以及對於相關人員之績效管理機制。 二、 為利各機關依本法規定提出資通安全維護計畫實施情形，爰於第二項明定其提出資料應包括之必要內容。 三、 考量部分公務機關或特定非公務機關之人力等行政資源可能較為不足，其資通安全維護計畫之訂修、執行及實施情形之提出等事宜，倘

	由其上級或監督機關、中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關統一辦理，較符合行政效率；為符合實務執行需求，以利資通安全維護業務之推展，爰於第三項明定資通安全維護計畫之訂定、修正、實施及其實施情形之提出，除由各機關自行辦理外，亦得由其上級或監督機關、中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機關辦理。
第七條　前條第一項第一款之核心業務，其範圍如下： 一、公務機關依其組織法規，足認該業務為機關核心權責所在。 二、公營事業及政府捐助之財團法人之主要服務或功能。 三、各機關維運、提供關鍵基礎設施所必要之業務。 前條第一項第六款之核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表八資通系統防護需求分級原則之規定，判定其防護需求等級為高者。	一、第一項明定第六條第一項第一款之核心業務之範圍。公務機關之核心業務，應視其組織法規之規定或業務是否係屬維運、提供關鍵基礎設施所必要進行判斷；於公營事業及政府捐助財團法人，則視其是否係屬主要服務或功能所在；各機關業務如涉關鍵基礎設施，則其維運、提供關鍵基礎設施所必要之業務亦屬各機關之核心業務，爰為第一項規定。另是否係屬核心業務，除由特定非公務機關自行認定外，中央目的事業主管機關亦得協助認定之，併予敘明。 二、第二項明定第六條第一項第六款之核心資通系統，指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表八資通系統防護需求分級原則之規定，判定其防護需求等級為高者，以利各機關辦理本法及相關法令要求之事項，並強化各機關之資通安全防護。
第八條　本法第十四條第三項及第十八條第三項之資通安全事件調查、處理及改善報告，應包括下列事項： 一、 事件發生、完成損害控制或復原作業之時間。 二、 事件影響之範圍及損害評估。 三、 損害控制及復原作業之歷程。 四、 事件調查及處理作業之歷程。	明定資通安全事件調查、處理及改善報告應包括之內容。

五、 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。 六、 前款措施之預定完成時程及成效追蹤機制。	
第九條　中央目的事業主管機關依本法第十六條第一項規定指定關鍵基礎設施提供者前，應給予其陳述意見之機會。	為保障人民權益，明定中央目的事業主管機關依本法第十六條第一項規定指定關鍵基礎設施提供者前，應給予其陳述意見之機會。
第十條　本法第十八條第三項及第五項所稱重大資通安全事件，指資通安全事件通報及應變辦法第二條第四項及第五項規定之第三級及第四級資通安全事件。	明定重大資通安全事件之定義。
第十一條　主管機關或中央目的事業主管機關知悉重大資通安全事件，依本法第十八條第五項規定公告與事件相關之必要內容及因應措施時，應載明事件之發生時間、原因、影響程度、控制情形及後續改善措施。 前項與事件相關之必要內容及因應措施有下列情形之一者，不予公告： 一、 涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或公開有侵害公務機關、個人、法人或團體之權利或正當利益。但法令另有規定，或為避免人民生命、身體之重大損害而有必要，或經當事人同意者，不在此限。 二、 其他依法令規定應秘密、限制或禁止公開之情形。 第一項與事件相關之必要內容及因應措施含有前項不予公告之情形者，得僅就其他部分公告之。	為利相關機關辦理本法第十八條第五項重大資通安全事件之公告，使民眾了解其事件之必要內容及因應措施，並考量民眾權益之保護及公共利益之維護，爰明定公告時應載明之事項及不予公告之情形。
第十二條　特定非公務機關之業務涉及數中央目的事業主管機關之權責者，主管機關得協調指定一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。	考量特定非公務機關之業務性質可能涉及數個中央目的事業主管機關之權責，為避免發生該等中央目的事業主管機關就本法所定事宜權責不清之情形，爰明定主管機關得協調指定其中一個以上之中央目的事業主管機關，單獨或共同辦理本法所定中央目的事業主管機關應辦理之事項。
第十三條　本細則之施行日期，由主管機關定之。	明定本細則之施行日期，由主管機關定之。