立法院法制局法案評估報告　　編號：1896

本報告僅供委員參考

資通安全管理法修正草案評估報告

法制局　楊蕙如　撰

中華民國 113 年 10 月

資通安全管理法修正草案評估報告

目　次

摘　要

為因應數位發展部於111年8月27日成立，修正本法之主管機關為數位發展部，並定明國家資通安全業務由數位發展部資通安全署辦理掌理國家資通安全業務；強化各機關委外辦理資通系統服務提供之監督管理機制；增訂限制對危害國家資通安全產品之下載使用；增訂對資通安全專職人員之適任性查核及調度支援等規定，使本法規範事項更符合實務運作，行政院爰擬具「資通安全管理法修正草案」，於113年7月4日函請本院審議。經本報告研析相關內容，並檢視性別與人權影響評估結果，提出相關建議，俾供本院委員問政及審查法案參考。

資通安全管理法修正草案評估報告

壹、前言

資通安全管理法(以下簡稱本法）於民國[1]107年6月6日制定公布，並於108年1月1日施行，迄今未曾修正。為因應數位發展部（以下簡稱數位部）於111年8月27日成立，掌理國家資通安全業務，並下設數位發展部資通安全署(以下簡稱資安署），掌理國家資通安全之規劃、推動與執行，以及為使本法規範事項更符合實務運作，行政院爰擬具「資通安全管理法修正草案」(下稱本草案)，並於113年7月4日以院臺安字第1135013826號函請本院審議。茲就行政院提案之相關內容進行研析，並就其性別及人權影響評估報告結果加以檢視，提出相關建議，俾供本院委員問政及審查法案參考。

貳、草案重點

本草案計修正 25 條，新增 9 條，謹就本報告納入研析與建議修正條文摘錄修正要點如下：

一、修正資通安全、資通安全事件、特定非公務機關、關鍵基礎設施、特定關鍵基礎設施提供者及特定財團法人之定義。(草案第3條)

二、強化各機關落實委外辦理資通系統建置、維運、服務提供之監督管理機制。(草案第10條)

三、增訂公務機關及特定非公務機關對於危害國家資通安全產品有關下載、安裝或使用之相關規定。(草案第11條及第27條)

四、定明公務機關及特定非公務機關應配合辦理資通安全事件通報

[1] 本報告有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

及應變機制之演練作業授權項目。(草案第17條及第24條)

五、增訂強化資通安全人員專業知能及重大資通安全事件之調度支援等規定。(草案第18條)

六、增訂中央目的事業主管機關應依資安署指定之方式將稽核結果及改善報告送交資安署之規定。(草案第20條及第21條)

參、問題研析與建議

一、關鍵基礎設施應宜於本法明定主要領域，以符法律保留原則（草案第 3 條第 7 款）

國家關鍵基礎設施(Critical Infrastructure, CI)係指「公有或私有、實體或虛擬的資產、生產系統以及網絡，因人為破壞或自然災害受損，進而影響政府及社會功能運作，造成人民傷亡或財產損失，引起經濟衰退，以及造成環境改變或其他足使國家安全或利益遭受損害之虞者。」關鍵基礎設施提供者之指定，其作業流程係依「關鍵基礎設施盤點作業須知」辦理，其具體之篩選準則為：基礎設施遭攻擊或災損時，有造成「足以直接或間接造成大規模人口傷亡或避難遷徙者；足以直接或間接造成重大經濟損失者；足以直接或間接影響其他關鍵基礎設施營運之能力者；足以影響政府功能持續運作、民心士氣、社會安定者[2]。」之一者，應列為關鍵基礎設施。

國家關鍵基礎設施依三層架構分類為：(一) 主領域：依功能屬性分為能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等共 8 項主要領域；(二) 次領域：各主領域之下再依功能業務區分次領域，例如能源領域下再區分為電力、石油、天然氣等次領域；(三) 功能設施與系統：指維持次領域重要

[2] 行政院國土安全政策會報，《關鍵基礎設施盤點作業須知》，111 年 3 月 30 日，頁 1。

功能業務運作所必須之設施設備、運輸網絡、資通訊系統、控制系統、指管系統、維安系統、關鍵技術等[3]。

本草案第3條第7款雖參照《國家關鍵基礎設施安全防護指導綱要》(下稱防護指導綱要)對於關鍵基礎設施之定義，指稱該等資產若功能一旦停止運作或效能降低，對國家安全等有重大影響之虞者，卻未說明該等資產之範疇，僅為原則性或抽象式之概括規定。本草案納管部分非公務機關（例如特定關鍵基礎設施提供者），加諸其通報等義務並定有罰則，因此包含哪些產業別，相關構成要件或領域宜直接於資安法中明確規範，以符合法律保留原則，並強化其位階性及法律之明確性；故建議宜將關鍵基礎設施分類之第一層「主領域」在定義中明確敘明，將關鍵基礎設施安全防護之範圍予以明確規定，以利於預算分配及法規執行。基於法律之位階與明確性，爰建議修正本草案第3條第7款：「關鍵基礎設施：指能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等行政院定期檢視並公告之領域中，該領域服務所依賴之實體或虛擬資產、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者。」

二、有關特定關鍵基礎設施提供者定義之「資通系統」宜修正為「資通系統或調度、控制系統」，以資明確並符實際（草案第3條第8款）

依據「防護指導綱要」，「國家關鍵基礎設施」(Critical Infrastructure, CI)及「國家關鍵資訊基礎設施」(Critical Information Infrastructure，CII)屬兩個相關但內涵不同之範疇。前者(CI)包含 8 項主要領域已如前述；後者「國家關鍵資訊基礎設

[3] 行政院，《國家關鍵基礎設施安全防護指導綱要》，107年5月18日訂正，頁3-4。

施」(CII)則係指「涉及核心業務運作，為支持國家關鍵基礎設施持續營運所需之重要資通訊系統或調度、控制系統(Supervisory Control and Data Acquisition，SCADA)，亦屬國家關鍵基礎設施之重要元件(資通訊類資產)，應配合對應之國家關鍵基礎設施統一納管者[4]。」

依行政院本草案第 3 條說明：「第八款用詞，考量本法係以維運或提供關鍵基礎設施全部或一部所依賴之『資通系統』者為規範對象，為避免混淆，爰由現行『關鍵基礎設施提供者』修正為『特定關鍵基礎設施提供者[5]』」，已敘明草案所提「特定關鍵基礎設施提供者」係指維運或提供關鍵基礎設施全部或一部所依賴之資通「系統」者。另依資安署訂定之關鍵基礎設施提供者指定程序（以下簡稱指定程序)，指定程序區分「辨識關鍵領域」、「辨識關鍵服務」、「辨識關鍵（資訊）基礎設施」及「核定關鍵基礎設施提供者」四大步驟，各步驟內之各分項工作依權責分由行政院、各中央目的事業主管機關及候選關鍵基礎設施提供者負責辦理[6]。故「特定關鍵基礎設施提供者」，係「經中央目的事業主管機關指定，送由主管機關報請行政院核定者。」。

現今工業自動化(Industrial Automation)時代，維運或提供關鍵基礎設施似難單僅依賴「資通系統」，爰第 3 條第 8 款指稱範圍尚宜包含支持關鍵基礎設施得以順利營運操作（Operation）之「調度及控制系統」，該等系統同屬國家關鍵基礎設施之重要元件(資通訊類

[4] 行政院，同前註，頁 3。

[5] 依行政院說明：「第八款用詞，考量本法係以維運或提供關鍵基礎設施全部或一部所依賴之『資通系統』者為規範對象，為避免混淆，爰由現行『關鍵基礎設施提供者』修正為『特定關鍵基礎設施提供者』，惟實質內涵並未變更，兩者具有同一性，不影響原經指定為關鍵基礎設施提供者之效力，不生重行指定之問題，並配合修正本法相關條文用詞。」

[6] 資安署網站/關鍵基礎設施資安防護，112 年 2 月 21 日，網址：https://moda.gov.tw/ACS/operations/ciip/650，最後瀏覽日期：113 年 10 月 2 日。

資產[7])。例如工業物聯網以三個維度的技術結合，其中包括資訊技術（Information Technology, IT）、操作技術（Operational Technology, OT）和通信技術（Communication Technology, CT[8]）。日本在2013年提出之「關鍵基礎設施的資訊安全措施」聚焦在電信、網路通訊部門，並指出資通訊設施在各個層面普及使用，若資通訊設施受到破壞，那麼以資通訊為「操作」基礎的電信、電力、金融服務等部門的運作，也將連帶造成衝擊，甚至造成難以恢復的損害。對此，日本內閣府網絡安全中心特別指出：「資訊技術（IT）與控制等操作技術（OT）融合，並傳播到社會經濟系統，除已實現的系統外，也可能成為網路攻擊目標的物聯網系統，也變得愈來愈普遍[9]」。因此，資通系統須與關注實際的工業操作和過程控制之操作技術（調度、控制系統）接軌合作，方能使關鍵基礎設施順利維運。綜上，建議修正本草案第3條第8款：「特定關鍵基礎設施提供者：指維運或提供關鍵基礎設施全部或一部所依賴之資通系統或調度、控制系統，經中央目的事業主管機關指定，送由主管機關報請行政院核定者。」

三、建議由中央主管機關訂定契約範本供參，減少因契約規範不明衍生之資通安全風險（增訂草案第10條第3項）

本草案第10條規範委外辦理資通系統之建置、維運或資通服務之提供，應選任適當之受託者，並強化對受託者之資通安全管理要求，爰於第1項增訂「要求受託者建立有效之資通安全管理機制，並

[7] 參「國家關鍵資訊基礎設施」(CII)之定義，其所稱該等資通訊類資產，亦未排除「調度及控制系統」而專指「資訊系統」。

[8] AIoT Cloud 物聯雲，IT 與 OT 的融合如何實現智慧工廠？，就享知 DigiKnow，112 年 4 月 7 日，網址：https://www.digiknow.com.tw/knowledge/642e298a57b33，最後瀏覽日期：113 年 9 月 25 日。

[9] 施柏榮，為什麼我們應該再談數位關鍵基礎設施？，財團法人資訊工業策進會，112 年 4 月 6 日，網址：https://www.iii.org.tw/focus/FocusDtl.aspx?f_type=1&f_sqno=fWF0UuVWfaBVyxfq%2bRrwDA__&fm_sqno=12，最後瀏覽日期：113 年 9 月 25 日。

監督該機制之實施」等文字；另為強化各機關落實委外監督管理，爰增訂第 2 項：「公務機關或特定非公務機關辦理前項委外業務，應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。」由於委外辦理資通系統之建置、維運或資通服務之提供不論在公、私部門均為常見之情形，且委外服務所提供之品質、量能直接關係相關設施營運之穩定度與資通安全議題。為使相關契約內容明確化，主管機關宜訂定契約範本供參，該範本除就契約當事人雙方應有的權利義務內容予以規範，亦應載明契約之格式、內容、其應記載及不得記載事項，期以合理的規定，提供委託者及受託者作為訂定有關契約參考之用，具有教育及示範作用，減少因契約規範不明或不當衍生之資通安全風險，爰參考老人福利法第 38 條第 2 項、補習及進修教育法第 9 條第 2 項規定之體例，建議本條增訂第 3 項：「前項書面契約之格式、內容，中央主管機關應訂定定型化契約範本及其應記載及不得記載事項。」

四、為落實政府資訊公開之原則，危害國家資通安全產品之產品清單，宜由主管機關定期公告之（草案第 11 條第 3 項）

現行對各機關有關危害國家資通安全產品之使用，係以行政規則「各機關對危害國家資通安全產品限制使用原則」(以下簡稱使用原則)規範，惟考量該等產品之使用涉及重大公共利益，行政院爰提升以法律及其明確授權之法規命令為依據；另現今資訊流通速度極快，且資訊內容影響公眾生活及公共安全，考量公務機關自行或委外營運場所之傳播設備及網際網路接取服務，與資訊流通密切相關，亦有納管規範之必要，行政院爰增訂本草案第11條。

行政院僅說明本條所定「危害國家資通安全產品」包含但不限於受反滲透法所稱滲透來源實質控制者所提供之產品，但未於草案明確

定義何謂「危害國家資通安全產品」，學者認為此舉恐違反民主國家政府應盡可能公開政府資訊的治理原則。雖然數發部回應理由是避免廠商「洗產地」，然針對「洗產地」之避免，或可參考美國出口管制清單的做法，針對欲管制項目，描述產品、軟體、服務、功能和參數以及相關利害關係人之國籍。此外，草案未能將「使用原則」第3點[10]規定，主管機關應定期評估與核定有害國安資通訊產品入法，從而使國家的資安業務辦理減少法規政策影響評估（Regulatory Impact Analysis, RIA）的功能[11]。

為落實政府資訊公開之原則，並使各機關利於確實遵行不得下載、安裝或使用危害國家資通安全產品等之規定，「危害國家資通安全產品」宜清楚定義並予公告之以供查詢。爰參酌「使用原則」第3點規定，本草案第11條第3項建議修正為：「前二項有關危害國家資通安全產品之審查程序、風險評估、情資分享、使用限制及其他相關事項之辦法，由主管機關會商有關機關擬訂，報請行政院核定之；危害國家資通安全產品之產品清單，由主管機關定期公告之。」

五、遇有重大資通安全事件，資安署「得調度各級機關資通安全人員支援之」之規定，宜於子法訂定相關機制（草案第18條第2項）

公務機關依「資通安全責任等級分級辦法」(下稱分級辦法）附表一、附表三及附表五[12]之規定，應設置一定人數之專職人員辦理資通安全業務。行政院為強化公務機關之資通安全防護能量

[10] 「各機關對危害國家資通安全產品限制使用原則」第3點：
「本法主管機關應基於國家安全、國際情資分享、潛在風險及衝擊分析等因素，蒐集相關機關意見綜合評估，據以核定生產、研發、製造或提供前點產品之廠商及前點之產品清單。本法主管機關應定期檢視前項核定之廠商及產品清單，並依前項因素重新評估後，視需要調整。」

[11] 余啟民，〈從歐美資安法制發展淺析我國資通安全管理法修法草案〉，《電腦稽核期刊》，第49期，113年2月，頁50。

[12] 附表一 資通安全責任等級A級之公務機關應辦事項、附表三 資通安全責任等級B級之公務機關應辦事項、附表五 資通安全責任等級C級之公務機關應辦事項。

及提升資通安全專職人員之職能，本草案爰增訂第18條第1項及第2項前段規定；另考量透過實戰訓練，得快速累積人員經驗及提升應處能力，增訂第2項後段規定，定明遇有重大資安事件時，資安署得調度資通安全人員支援之，俾利落實資通安全聯防政策。前開資通安全人員，係指資通安全專職人員及專責人員。

我國目前的政府機關中，僅有警察、人事、政風、主計等單位屬於從上到下的「一條鞭」管理制度，從中央部會到地方政府機關的事權統一。中央的主管機關有統一的統籌訓練和主管考核機制，具有跨機關、跨單位進行人事調度的權利。為了使公務機關一旦發生重大資安事件，更有效率、更即時的解決，此次修正草案第18條特別賦予資安署有直接調度各機關資安人員支援的權利(外界稱本草案讓公務機關的資訊(安)人員具有「類一條鞭」之性質)。惟數位部曾於今年3月表示該部非以資訊類一條鞭制度指導其他基關資訊單位，而採用其他任務導向型配套措施與各機關資訊單位協同合作……，引導政府機關落實數位發展政策[13]。

本條所稱「得調度」之資通安全人員，依行政院說明第三點，係指資通安全專職人員及專責人員，所涉人員較廣，啟動調度可能影響各機關之人力缺口；另現行制度上不屬於具有一條鞭管理機制的單位，主管機關並無跨機關逕行調度人事之權，實務上仍需與各機關商議(經機關首長同意)甚或兼顧機關人員之意願[14]。為使遇有重大資通安全事件時，資安署具有較目前更具彈性之人

[13] 引述數位部副司長楊耿瑜發言，詳見：賴怡瑩，《政府機關資訊單位設置及留才攬才相關問題探討(編號A01675)》，臺北市：立法院法制局，113年4月，頁27。

[14] 因調度人員尚涉及考績、升遷，以及原單位業務受影響等議題，詳見：黃彥棻，【盤點《資安法》修法草案重點 3】公務機關遇重大資安事件，資安署有權調度各機關資安人員支援，iThome，112 年 11 月 10 日，網址：https://www.ithome.com.tw/news/159736，最後瀏覽日期：113 年10月1日。

員調度權，本報告肯認本草案增訂調度人員之相關內容，惟啟動調度程序前除評估事件規模、性質外，並於子法訂定相關機制(例如經機關同意)及其他具體事項(例如調度人數或比例是否訂有上限等)。

六、特定關鍵基礎設施提供者以外之特定非公務機關，設置「資通安全專職人員」，建議修正為「資通安全人員」(草案第 21 條第 1 項)

本草案於第7條第3項[15]、第18條第1項及第2項[16]、第19條第1項[17]、第20條第2項[18]及 第21條第1項等諸多條次規範「專職人員」，其中第7條係主管機關對專職人員之整體性規定；第18條及第19條第1項為「公務機關」專職人員之相關規定；第20條第2項係「特定關鍵基礎設施提供者」專職人員之規定，前述該等規範尚稱合理，惟第21條第1項[19]規範對象為「特定關鍵基礎設施提供者以外之特定非公務機關」，其既非公務機關，亦未提供特定關鍵基礎設施，倘依本草案要求該等企業或財團法人須「……設置資通安全專職人員，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。」恐生規定過嚴致難以執行及監督之問題。

雖草案說明「考量資安威脅日漸加劇，資安作業須持續維

[15] 本草案第 7 條第 3 項：「……**專職人員**之配置與專業條件及其他相關事項之辦法，由主管機關定之。」

[16] 本草案第 18 條：「公務機關應符合其資通安全責任等級之要求，設置資通安全**專職人員**，辦理資通安全業務及應變處理；所屬人員辦理資通安全業務績效優良者，應予獎勵。資安署應妥善規劃推動**專職人員**之職能訓練……」

[17] 本草案第 19 條第 1 項：「公務機關於必要時，得對所屬資通安全**專職人員**之適任性進行查核。」

[18] 本草案第 20 條第 2 項：「特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，設置資通安全**專職人員**，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。」

[19] 本草案第 21 條第 1 項：「特定關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，設置資通安全專職人員，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。」

持，為強化特定關鍵基礎設施提供者以外之特定非公務機關資安防護量能並能及時應處，避免其他業務排擠資安業務量能造成事件擴散，需要投入相關成本，人力資源是其中重要一環，故符合特定資通安全責任等級之特定關鍵基礎設施提供者以外之特定非公務機關，應設置專人專職辦理資通安全業務，以落實事前、事中及事後各項資安作業，確保其具有安全可靠的資通環境，爰修正第一項。」之立意雖佳，然實務上國內許多企業僅設少數資訊人員，甚或是2家以上之企業「共用」少數資訊人員(例如外包駐點資訊人員)，該等企業如何再行分流出設置資通安全專職人員之人力。況資訊時代資訊業務繁多，即使是公務機關未必能全面落實真正的資通安全專職人員，該等人員實際上亦可能兼辦部分資通安全以外之資訊業務[20]。因此，若以此要求特定關鍵基礎設施提供者以外之特定非公務機關，恐使法律規定流於形式，爰建議本條項之「資通安全專職人員」(必須全職辦理資安工作)，刪除「專職」二字，調整為「資通安全人員[21]」(可指資通安全專職人員或專責人員)，爰建議修正本草案第21條第1項：「特定關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，設置資通安全人員，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。」

七、中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專

[20] 以行政院所屬「部」層級機關而言，國防部、財政部及文化部未設置資訊相關單位；內政部等11個機關均設置資訊相關單位，業務職掌均包括資訊安全規劃及推動。目前在制度設計及業務推動上，似尚難明確區隔資訊及資安業務。詳見：賴怡瑩，〈資安治理機制之法制研析〉，立法院法制局議題研析(編號R02361)，113年2月15日，頁2。

[21] 草案第18條行政院說明二第3點：「……定明遇有重大資安事件時，資安署得調度資通安全人員支援之，俾利落實資通安全聯防政策。前開資通安全人員，係指資通安全專職人員及專責人員。」

線（草案第 24 條第 2 項）

冷戰結束後，隨著安全威脅情勢的轉變及資訊科技的快速發展，美國於1995年開始以資訊安全的角度，關注關鍵基礎設施保護（Critical Infrastructure Protection,CIP），由於美國關鍵基礎設施高達85%屬私部門擁有，美國政府早已體認其成功要素在於公、私部門能否充分協力、分享資訊。而健全資訊分享環境，建立互信而穩固的夥伴關係，有賴權責分明的組織、一致的流程標準、多元而友善的分享管道。其中由國家保護計畫局基礎設施保護辦公室（Office of Infrastructure Protection，OIP）營運的國家基礎設施協調中心（National Infrastructure Coordinating Center,NICC），是聯邦政府專用的全天候協調與資訊共享運營中心，當發生影響關鍵基礎設施的事故或事件，而需要國土安全部和國家基礎設施的擁有者及經營者之間進行協調時，NICC 即擔任資訊共享的樞紐來支援這些重要資產的安全性和韌性[22]。

本草案在107年制定前，即有與會代表表示若無統一對外窗口，非公務機關發生資安事件時，無法立即求援[23]。在數位轉型加速發展下，企業遭受網路攻擊情況有逐年增加之趨勢，尤其自107年後陡升。新冠疫情趨動了遠距工作型態，亦讓企業內網、外網邊界模糊，防衛變得複雜，企業被攻擊介面變多，而我國產業多是彼此相連的上下游供應鏈，駭客只要找到一個破口，就可以循線往上又往下進行攻擊，甚至造成企業營運中斷等重大損失

[22] 黃俊泰，〈美國關鍵基礎設施威脅資訊分享框架簡介〉，《清流雙月刊》，第 14 期，107 年 3 月頁 4-5。

[23] 陳映竹，〈網路治理趨勢下之資通安全法令：談台灣「資通安全管理法（草案）」〉，《臺灣經濟研究月刊》，第 40 卷第 10 期，106 年 10 月，頁 52。

[24]。我國目前雖尚未建立如同美國NICC規模之全天候協調與資訊共享運營中心，惟本草案第24條第2項明定，特定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通報。鑑於公、私部門（含特定非公務機關）間資通安全事件之縱向及橫向聯繫重要性及即時性之要求日增，為強化公、私協力，建立情資分享及合作聯防機制，中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線，俾利及時應變及合作。爰參酌人口販運防治法第10條[25]規定之體例，建議本草案第24條第2項修正為：「特定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通報。中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線。」。

八、資安署知悉重大資通安全事件時，「應」提供相關協助（草案第24條第5項）

本草案第24條第5項：「中央目的事業主管機關或資安署知悉重大資通安全事件時，得提供相關協助……」。綜覽我國於法律中使用「得提供相關協助」文字者，現行法中僅「文化部協助獎勵或補助文化創意事業辦法」第2條的1項：「從事本法第三條第一項第一款至第七款及第十五款之文化創意產業，且符合下列資格條件之一之文化創意事業，文化部（以下簡稱本部）得提供相關協助、獎勵或補助：……」，且其得提供相關「協助」，與其後之「獎勵或補助」屬於同位一體之概念。而行政機關所為之獎勵或補助，其性質係屬給付行政，故於法條文字中使用「得」尚屬

[24] 呂正華，〈資安即國安，提升資安韌性 實踐企業永續〉，《會計研究月刊》，第 456 期，112 年 11 月，頁 76。

[25] 人口販運防治法第 10 條規定：「司法警察機關及勞動主管機關應設置二十四小時檢舉通報窗口、線上檢舉平台或報案專線。」

合宜。然本草案中重大資通安全事件之提供協助與前揭文化協助及獎補助性質迥異，資安主管機關有積極提供協助之必要。而面對無所不在的資安挑戰，政府亦曾允若要協助各行各業提升資安防護韌性[26]，爰建議本草案第24條第5項修正為：「中央目的事業主管機關或資安署知悉重大資通安全事件時，應提供相關協助……」，以利建立公、私協力聯防機制。

九、法案性別與人權影響評估

依行政院所屬各機關主管法案報院審查應注意事項第 3 點規定：「各機關研擬法案，除應遵照『中央行政機關法制作業應注意事項』之規定辦理外，應切實注意下列各款規定：……（四）法案衝擊影響層面及其範圍，包括成本、效益及對人權之影響等，應有完整之評估。（五）除廢止案外，應進行性別影響評估。……」，草案主管機關已填報法案及性別影響評估檢視表（詳如附錄）。

經初步檢視，在性別影響評估部分，本草案內容之執行方式無因性別、性傾向或性別認同不同而有差異，對於性別對象及執行方式並無區別，故就不同性別、性傾向或性別認同者亦不會產生不同結果。在人權影響評估部分，本草案亦無違反公民與政治權利國際公約、經濟社會文化權利國際公約等內容，爰草案符合憲法、國際規範、性別平等政策綱領等要求，並符合憲法有關人民權利之規定、公民與政治權利國際公約及經濟社會文化權利國際公約。

肆、結論

本草案內容主要涉及資通安全管理法之適用對象，為強化資通安

[26] 面對無所不在的資安挑戰，時任總統蔡英文表示，我們需要不斷強化應變能力和管理機制。政府會持續推動國產自主研發資安產品和服務，也會鼓勵投資資安新創。我們要協助各行各業提升資安防護韌性，目標是「資安好，臺灣產業才會更好」，詳見：崔慈悌，臺灣資安國家隊成立！蔡英文：確保數位國土安全，中時電子報，112 年 5 月 9 日，網址：https://www.chinatimes.com/realtimenews/20230509002860-260407?chdtv，最後瀏覽日期：113 年 9 月 25 日。

全所為之通報義務、監管機制、限制規定以及人員查核及調度等，以有效保護關鍵（資訊）基礎設施及確保國家安全。茲就行政院提案相關內容進行研析，並就其性別及人權影響評估報告結果加以檢視，提出相關建議如下，俾供委員於問政及審查法案參考：

一、關鍵基礎設施應宜於本法明定主要領域，以符法律保留原則。

二、有關特定關鍵基礎設施提供者定義之「資通系統」宜修正為「資通系統或調度、控制系統」。

三、建議由中央主管機關訂定契約範本供參，減少因契約規範不明衍生之資通安全風險。

四、為落實政府資訊公開之原則，危害國家資通安全產品之產品清單，宜由主管機關定期公告之。

五、遇有重大資通安全事件，資安署「得調度各級機關資通安全人員支援之」之規定，宜於子法訂定相關機制。

六、特定關鍵基礎設施提供者以外之特定非公務機關，設置「資通安全專職人員」，建議修正為「資通安全人員」。

七、中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線。

八、資安署知悉重大資通安全事件時，「應」提供相關協助。

伍、條文對照表

行政院函送本院審議之「資通安全管理法修正草案」，共計修正25條，新增9條。本報告經研析後，建議修正5條（第3條、第10條、第11條、第21條、第24條）。茲就相關條文建議修正情形，臚列條文對照表如下：

資通安全管理法修正草案條文對照表

行政院提案條文	本報告建議條文	現行條文	說明
第一章　總則	第一章　總則	第一章　總則	章名未修正。
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，以保障國家安全，維護社會公共利益，特制定本法。	（無修正意見）	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，以保障國家安全，維護社會公共利益，特制定本法。	本條未修正。
第二條　本法之主管機關為數位發展部。 國家資通安全業務，由數位發展部資通安全署（以下簡稱資安署）辦理。	（無修正意見）	第二條　本法之主管機關為行政院。	一、依行政院一百十一年八月二十四日院臺規字第一一一〇一八四三〇七號公告，本法之主管機關，自一百十一年八月二十七日起變更為數位發展部，爰配合上開公告修正現行條文，並列為第一項。 二、因應數位發展部資通安全署成立，掌理國家資通

			安全業務，為符權責，爰增訂第二項。
第三條　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，或其他情形影響其機密性、完整性或可用性。 四、資通安全事件：指系統、服務或	第三條　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，或其他情形影響其機密性、完整性或可用性。 四、資通安全事件：指系統、服務或	第三條　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、資通安全事件：指系統、服務或	**行政院說明：** 一、第一款、第二款及第五款未修正。 二、第三款及第四款酌作文字修正，以符實際。 三、第六款配合第八款、第九款用詞修正為特定關鍵基礎設施提供者、特定財團法人。 四、依行政院一百十一年八月二十四日院臺規字第一一一〇一八四三〇七號公告，第七款及第八款所列主管機關權責事項，自一百十一年八月二十七日起仍由行政院管轄，並配合現行實務作法，爰予修正。另第八款用詞，考量本法係以維運或提供關鍵基礎設施全部或一部所依賴之「資通系統」

網路狀態經鑑別而顯示可能有違反資通安全或保護措施失效之狀態發生，影響資通系統機能運作。 五、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。 六、特定非公務機關：指特定關鍵基礎設施提供者、公營事業或特定財團法人。 七、關鍵基礎設施：指行政院定期檢視並公告之領域中，該領域服務所依賴之實體或虛擬資產、系統或網路，其功能一旦停止運作或	網路狀態經鑑別而顯示可能有違反資通安全或保護措施失效之狀態發生，影響資通系統機能運作。 五、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。 六、特定非公務機關：指特定關鍵基礎設施提供者、公營事業或特定財團法人。 七、關鍵基礎設施：指能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等行政院定期檢視並公告之	網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。 五、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。 六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。 七、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	者為規範對象，為避免混淆，爰由現行「關鍵基礎設施提供者」修正為「特定關鍵基礎設施提供者」，惟實質內涵並未變更，兩者具有同一性，不影響原經指定為關鍵基礎設施提供者之效力，不生重行指定之問題，並配合修正本法相關條文用詞。 五、現行第九款制定公布時，財團法人法尚未完成立法，考量該法已制定公布施行，爰修正第九款，定明符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定，且屬該法第二條第八項所定全國性財團法人者，為本法所稱特定財團法人。 **本報告說明：**

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者。 八、特定關鍵基礎設施提供者：指維運或提供關鍵基礎設施全部或一部所依賴之資通系統，經中央目的事業主管機關指定，送由主管機關報請行政院核定者。 九、特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。	領域中，該領域服務所依賴之實體或虛擬資產、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者。 八、特定關鍵基礎設施提供者：指維運或提供關鍵基礎設施全部或一部所依賴之資通系統或調度、控制系統，經中央目的事業主管機關指定，送由主管機關報請行政院核定者。 九、特定財團法人：指符合財團法人法第二條第二項、第三項或第六十三	公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。 八、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，經中央目的事業主管機關指定，並報主管機關核定者。 九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。	一、本草案納管部分非公務機關，加諸其通報等義務並定有罰則，因此包含哪些產業別及相關構成要件或領域，宜直接於資安法中明列。建議將關鍵基礎設施分類之第一層主領域在定義中敘明，明確規定關鍵基礎設施安全防護範圍，爰建議修正第七款。 二、工業自動化(Industrial Automation)時代，維運或提供關鍵基礎設施似難單僅依賴「資通系統」，尚應包含支持關鍵基礎設施得以順利營運操作(Operation)之「調度及控制系統」，該等系統同屬國家關鍵基礎設施之重要元件(資通訊類資產)，爰建議修正

	條第一項、第四項規定之財團法人，並屬該法第二條第八項所定全國性財團法人者。		第八款。
第四條　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。 三、資通安全產業之發展。 四、資通安全軟硬體技術規範、相關服務及審驗機制之發展。 前項相關事項之推動，由主管機關擬訂國家資通安全發展方案，報請行政院核定後	（無修正意見）	第四條　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。 三、資通安全產業之發展。 四、資通安全軟硬體技術規範、相關服務與審驗機制之發展。 前項相關事項之推動，由主管機關以國家資通安全發展方案定之。	一、第一項第四款酌作文字修正，其餘各款未修正。 二、第二項配合實務作法，修正為由數位發展部擬訂國家資通安全發展方案，報請行政院核定後實施。

實施。			
第五條　為落實國家資通安全政策，各政府機關、中央及地方間，應致力配合推動執行國家資通安全措施，共同建構國家資通安全環境。 為辦理國家資通安全政策、應變機制與重大計畫之諮詢審議，協調各政府機關、中央及地方間之資通安全相關事務，行政院應召開國家資通安全會報，其幕僚作業由主管機關辦理。 前項國家資通安全會報決議事項，相關政府部門應予執行，由主管機關定期追蹤管考，並得辦理績效評核。 第二項國家資通安全會報之組成、任務、議事程序及其他相關事項之辦法，由行政院定之。	（無修正意見）		一、本條新增。 二、因應越趨增強之全球資通安全威脅及突發資通安全事件，各政府機關應建立中央地方聯防體系，以完備國家資通安全，爰規定第一項及第二項，強化跨機關資通安全事件應處及協調能力。 三、為確保落實國家資通安全會報決議事項，爰規定第三項。 四、第二項國家資通安全會報之組成、任務、議事程序及其他相關事項之辦法，於第四項授權由行政院定之。
第六條　主管機關應規劃並推動國家資通安	（無修正意見）	第五條　主管機關應規劃並推動國家資通安	一、條次變更。 二、第一項酌作文字修正。

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、對公務機關資通安全維護計畫實施情形稽核概況報告及國家資通安全發展方案。 前項情勢報告、實施情形稽核概況報告及國家資通安全發展方案，應由主管機關送立法院備查。		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、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。 前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。	三、第二項修正定明辦理之主體，並酌作文字修正。
第七條　公務機關及特定非公務機關，應按其業務重要性與機敏性、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，報由資安署核定或備查其資通安全責任等級。 公務機關及特定非公務機關應符合資通安全責任等級之要求，並自管理、技術、認知及訓練等面向，辦理資通安	（無修正意見）	第七條　主管機關應衡酌公務機關及特定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，由主管機關定之。 主管機關	一、現行第一項前段規定酌作文字修正，以符實際，並列為修正條文第一項。 二、公務機關及特定非公務機關辦理資通安全防護措施應符合資通安全責任等級之要求，爰增訂第二項。 三、現行第一項後段規定移列為修正條文第三項，並就其授權範圍及內容酌

全防護措施。 前二項資通安全責任等級之區分基準、核定或備查程序、變更申請、資通安全防護措施辦理項目、內容、專職人員之配置與專業條件及其他相關事項之辦法，由主管機關定之。		得稽核特定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，由主管機關定之。 特定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，應向主管機關提出改善報告，並送中央目的事業主管機關。	作修正，以資明確。 四、現行第二項及第三項移列修正條文第八條規定，爰予刪除。
第八條　資安署得定期或不定期稽核公務機關及特定非公務機關之資通安全維護計畫實施情形。 前項稽核後，發現受稽核機關資通安全維護計畫實施情形有缺失或待改善者，受稽核機關應提出改善報告，公務機關送交依第十四條規定收受其實施情形之機關、特定非公務機關送交中央目的事業主管機關審查	（無修正意見）	第七條第二項及第三項 主管機關得稽核特定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，由主管機關定之。 特定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，應向主管機關提出改善報告，並送中央目的事業主管機	一、第一項由現行第七條第二項前段規定移列，酌作文字修正，並為協助公務機關檢視自身資通安全維護計畫實施情形，增訂資安署得稽核公務機關。 二、第二項由現行第七條第三項規定移列，並配合實務執行需求酌作修正。 三、為使收受改善報告之機關得對受稽核機關進行

後，由該審查機關送交資安署。 前項收受改善報告之機關認有必要時，得要求受稽核機關進行說明或調整。 前三項資通安全維護計畫實施情形之稽核頻率、內容與方法、改善報告之提出及其他相關事項之辦法，由主管機關定之。 第一項稽核由資安署擬訂年度計畫，送由主管機關報請行政院核定後辦理，年度計畫及年度成果報告應送交國家資通安全會報備查。		關。	監督及指導，爰增訂第三項，俾使其得就缺失或待改善事項妥為處理。 四、第四項由現行第七條第二項後段規定移列，並酌作修正。 五、為使第一項稽核辦理有據，並考量事涉公務機關及特定非公務機關，有賴各政府機關間配合推動執行，爰增訂第五項。
第九條　資安署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、方法及其他相關事項之辦法，由主管機關定之。	（無修正意見）	第八條　主管機關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、方法及其他相關事項之辦法，由主管機關定之。	一、條次變更。 二、資通安全情資分享之執行，主要係國內外之資通安全資訊交流、資通安全警訊發布等技術性事務，目前實務現況係由資安署辦理，爰修正第一項。 三、第二項未修正。

第十條　公務機關或特定非公務機關，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，應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。 公務機關或特定非公務機關辦理前項委外業務，應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。	第十條　公務機關或特定非公務機關，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，應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。 公務機關或特定非公務機關辦理前項委外業務，應與受託者簽訂書面契約，載明雙方之權利義務及違約責任。 前項書面契約之格式、內容，中央主管機關應訂定定型化契約範本及其應記載及不得記載事項。	第九條　公務機關或特定非公務機關，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。	**行政院說明：** 一、條次變更。 二、考量現行條文規定公務機關或特定非公務機關選任受託者時，所應考量之「專業能力與經驗、委外項目之性質及資通安全需求」等事項，本即屬其「適當性」之考量範疇，又為強化對受託者之資通安全管理要求，爰修正現行條文，並列為第一項。 三、為強化各機關落實委外監督管理，各機關應與受託者簽訂書面契約，並載明雙方之權利義務及違約責任，爰增訂第二項。 **本報告說明：** 資通系統委外服務所提供之品質、量能直接關係相關設施營運之穩定度與資通安全議題。為使相關契約內容明確化，爰參考老人福利法第三十八條第二

			項、補習及進修教育法第九條第二項規定之體例，建議增訂第三項。
第二章　公務機關資通安全管理	第二章　公務機關資通安全管理	第二章　公務機關資通安全管理	章名未修正。
第十一條　公務機關不得下載、安裝或使用危害國家資通安全產品；其自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，亦同。但因業務需求且無其他替代方案者，經該機關資通安全長及依第十四條規定收受其實施情形之機關資通安全長核可，函報主管機關核定後，得以專案方式使用，並列冊管理。 公務人員獲配之公務用資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。 前二項有關危害國家資通安全產品之審查程序、風險	第十一條　公務機關不得下載、安裝或使用危害國家資通安全產品；其自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務，亦同。但因業務需求且無其他替代方案者，經該機關資通安全長及依第十四條規定收受其實施情形之機關資通安全長核可，函報主管機關核定後，得以專案方式使用，並列冊管理。 公務人員獲配之公務用資通訊設備，不得下載、安裝或使用危害國家資通安全產品，並應遵守相關法令規範。 前二項有關危害國家資通安全產品之審查程序、風險		**行政院說明：** 一、本條新增。 二、現行對各機關有關危害國家資通安全產品之使用，係以行政規則「各機關對危害國家資通安全產品限制使用原則」規範，惟考量該等產品之使用涉及重大公共利益，爰提升以法律及其明確授權之法規命令為依據；另現今資訊流通速度極快，且資訊內容影響公眾生活及公共安全，考量公務機關自行或委外營運場所之傳播設備及網際網路接取服務，與資訊流通密切相關，亦有納管規範之必

評估、情資分享、使用限制及其他相關事項之辦法，由主管機關會商有關機關擬訂，報請行政院核定之。	評估、情資分享、使用限制及其他相關事項之辦法，由主管機關會商有關機關擬訂，報請行政院核定之；危害國家資通安全產品之產品清單，由主管機關定期公告之。		要，爰訂定本條。 三、本條所定「危害國家資通安全產品」，包含但不限於受反滲透法所稱滲透來源實質控制者所提供之產品；其中第三項規定危害國家資通安全產品之審查程序、風險評估、情資分享、使用限制及其他相關事項，授權由主管機關訂定辦法，以符合授權明確性原則。又為妥適評估產品資安風險，前開審查程序規劃由相關主管機關，例如該產品產業之中央目的事業主管機關、國安、經貿等相關主管機關，共同審查產品情資，並據以分享。 **本報告說明：** 為落實政府資訊公開之原則，並使各機關利於確實

			遵行不得下載、安裝或使用危害國家資通安全產品等之規定，「危害國家資通安全產品」宜清楚定義並予公告之以供查詢，爰建議修正第三項。
第十二條　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。	（無修正意見）	第十一條　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。	條次變更，內容未修正。
第十三條　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。	（無修正意見）	第十條　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。	條次變更，內容未修正。
第十四條　公務機關應每年向上級機關或監督機關提出資通安全維護計畫實施情形；無上級機關或監督機關者，其資通安全維護計畫實施情形應依下列各款規	（無修正意見）	第十二條　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主管機關。	一、條次變更。 二、為明確規範公務機關資通安全維護計畫實施情形提出之管道，按現行條文規定之運作模式，修正本條，並定明第一款及第

定辦理： 一、總統府、國家安全會議及五院，向資安署提出。 二、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會，向資安署提出。 三、直轄市山地原住民區公所、直轄市山地原住民區民代表會，向直轄市政府提出；鄉（鎮、市）公所、鄉（鎮、市）民代表會，向縣政府提出。			二款公務機關資通安全維護計畫實施情形提出之對象。 三、為強化地區聯防，將直轄市山地原住民區公所、直轄市山地原住民區民代表會、鄉（鎮、市）公所以及鄉（鎮、市）民代表會之提出對象，定明為直轄市政府及縣政府，爰規定第三款。
第十五條　公務機關應稽核其所屬、所監督之公務機關、所轄鄉（鎮、市）公所、直轄市山地原住民區公所及鄉（鎮、市）民代表會、直轄市山地原住民區民代表會之資通安全維護計畫實施情形。	（無修正意見）	第十三條　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、條次變更。 二、為落實資通安全聯防政策，公務機關資通安全維護計畫實施情形之稽核，採分層監督管理模式，依現行第一項規定，由上級機關或監督機關稽核之。惟無上級機

			關或監督機關者，現行僅有內部稽核規定，爰增訂直轄市政府應稽核所轄直轄市山地原住民區公所、直轄市山地原住民區民代表會，以及縣政府應稽核所轄鄉（鎮、市）公所、鄉（鎮、市）民代表會。 三、現行第二項移列修正條文第十六條第一項規定，爰予刪除。
第十六條　受稽核機關之資通安全維護計畫實施情形有缺失或待改善者，應向稽核機關提出改善報告，並由稽核機關連同稽核結果依資安署指定之方式送交資安署。 稽核機關或資安署認有必要時，得要求受稽核機關進行說明或調整。 前三條及第一項資通安全維護計畫必	（無修正意見）	第十三條第二項　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、第一項由現行第十三條第二項規定移列，除修正定明改善報告之提出對象外，並為利資安署掌握全國資通安全現況，修正定明稽核結果及改善報告由稽核機關送交該署。 二、為使稽核機關、資安署就受稽核機關之改善報告得進行監督及指導，爰增

要事項、實施情形之提出、稽核之頻率、內容與方法、結果之交付、改善報告之提出及其他相關事項之辦法，由主管機關定之。			訂第二項，俾使其得就缺失或待改善事項妥為處理。 三、修正條文第十三條至第十五條與第一項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、結果之交付、改善報告之提出及其他相關事項，增訂第三項授權由主管機關以辦法定之。
第十七條　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，應向第十四條規定收受其實施情形	（無修正意見）	第十四條　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	一、條次變更。 二、第一項未修正。 三、配合修正條文第十四條已定明公務機關資通安全維護計畫實施情形之提出對象，及

之機關及資安署通報。 公務機關應向前項受通報機關提出資通安全事件調查、處理及改善報告。 前三項通報與應變機制之必要事項、通報內容、報告之提出、演練作業及其他相關事項之辦法，由主管機關定之。 第二項受通報機關知悉重大資通安全事件時，得提供公務機關相關協助；於適當時機並得公告與事件相關之必要內容及因應措施。		報主管機關；無上級機關者，應通報主管機關。 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，並送交主管機關；無上級機關者，應送交主管機關。 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，由主管機關定之。	實務運作現況，爰修正第二項及第三項。 四、為增進公務機關因應資通安全事件之處理能力，爰於第四項授權項目增訂演練作業，俾利透過實施模擬演練以熟悉應變作為、提升應變技能，並酌作文字修正。 五、考量重大資通安全事件可能影響人民之生命、身體或財產安全，爰比照特定非公務機關之規定，增訂第五項，由受通報機關於知悉後，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，以避免損害之擴大。
第十八條　公務機關應符合其資通安全責任等級之要求，設	（無修正意見）	第十五條　公務機關所屬人員對於機關之資通安全維護績	一、條次變更。 二、公務機關依資通安全責任等級分級

置資通安全專職人員，辦理資通安全業務及應變處理；所屬人員辦理資通安全業務績效優良者，應予獎勵。 資安署應妥善規劃推動專職人員之職能訓練，增進其資通安全專業知能；遇有重大資通安全事件，資安署得調度各級機關資通安全人員支援之。 前二項人員獎勵、職能訓練、調度支援及其他相關事項之辦法，由主管機關定之。		效優良者，應予獎勵。 前項獎勵事項之辦法，由主管機關定之。	辦法附表一、附表三、附表五之規定，應設置一定人數之專職人員辦理資通安全業務，為強化公務機關之資通安全防護能量，爰將其意旨修正為第一項前段規定，現行第一項則酌作文字修正後列為後段規定。 三、因資通安全人員之專業知能，與公務機關資通安全防護能量有密切關係，為強化並提升公務機關專職人員之職能，爰增訂第二項前段規定；另考量透過實戰訓練，得快速累積人員經驗及提升應處能力，爰增訂第二項後段規定，定明遇有重大資安事件時，資安署得調度資通安全人員支援之，俾

			利落實資通安全聯防政策。前開資通安全人員，係指資通安全專職人員及專責人員。 四、現行第二項配合修正條文第一項及第二項酌作文字修正，增訂授權項目，並移列為第三項。
第十九條　公務機關於必要時，得對所屬資通安全專職人員之適任性進行查核。 主管機關得於資通安全人員任用考試榜示後，對錄取人員之適任性進行查核。 拒絕查核或前二項查核結果經用人機關認定未通過者，不得辦理涉及國家機密、軍事機密及國防秘密之資通安全業務。 前項人員職務得由用人機關基於內部管理及業務運作需要，依法進行調整。	（無修正意見）		一、本條新增。 二、考量公務機關之資通安全專職人員辦理資通安全業務時，可能觸及國家機密、軍事機密及國防秘密，有予以查核其適任性之必要，是以將現職人員及考試錄取人員定為得查核之對象範圍，並定明拒絕查核或查核未通過之法律效果。至所定必要時，係指經公務機關綜合業務屬性、人員實際情形予以審認，爰規定第一項

第一項及第二項查核紀錄，由用人機關依相關規定保密處理，並妥為保管，不得移作他用；違反者，視情節予以議處。 有關查核權責機關、應受查核人員、查核程序、內容及其他相關事項之辦法，由主管機關會商有關機關定之。			至第四項。另第二項「資通安全人員任用考試」，係指考試類科為「資通安全」者。 三、查核紀錄涉及受查核者之個人資料，用人機關應注意相關保密及保管措施，爰規定第五項。 四、有關查核權責機關、應受查核人員、查核程序、內容及其他相關事項，授權主管機關訂定辦法，以符合授權明確性原則，爰規定第六項。另受查核人員就查核結果經用人機關認定未通過者，現職資通安全專職人員對於用人機關之決定，認有違法或顯然不當致損害其權利或利益，得依公務人員保障法規定，提起救濟；非現職者得依訴願

			法規定，提起救濟，併予敘明。
第三章　特定非公務機關資通安全管理	第三章　特定非公務機關資通安全管理	第三章　特定非公務機關資通安全管理	
第二十條　中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定特定關鍵基礎設施提供者，送由主管機關報請行政院核定，並以書面通知受核定者。 特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，設置資通安全專職人員，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。 特定關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。 中央目的	（無修正意見）	第十六條　中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。 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提出資通安全維護計畫實施情形。 中央目的事業主管機關應稽核所管關鍵基礎設施提	一、條次變更。 二、依行政院一百十一年八月二十四日院臺規字第一一一〇一八四三〇七號公告，第一項所列主管機關權責事項，自一百十一年八月二十七日起仍由行政院管轄，並配合現行實務作法，爰修正第一項。 三、考量資安威脅日漸加劇，資安作業須持續維持，為強化特定關鍵基礎設施提供者資安防護量能並能及時應處，避免其他業務排擠資安業務量能造成事件擴散，需要投入相關成本，人力資源是其中重要一環，故符合特定資

事業主管機關應綜合考量所管特定關鍵基礎設施提供者業務之重要性與機敏性、資通系統之規模、性質、資通安全事件發生之頻率、程度及其他與資通安全相關之因素，定期稽核其資通安全維護計畫之實施情形。 特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，應向中央目的事業主管機關提出改善報告。 中央目的事業主管機關應依資安署指定之方式將稽核結果及改善報告送交資安署。		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。 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，報請主管機關核定之。	通安全責任等級之特定關鍵基礎設施提供者，應設置專人專職辦理資通安全業務，以落實事前、事中及事後各項資安作業，確保其具有安全可靠之資通環境，爰修正第二項。 四、第三項配合修正條文第三條第八款用詞，酌作文字修正。 五、考量行政資源有效利用，擇定適當之特定關鍵基礎設施提供者，稽核其資通安全維護計畫實施情形，爰於第四項增訂中央目的事業主管機關定期辦理稽核時應審酌之因素。 六、第五項酌作文字修正。 七、為利資安署掌握全國資通安全現況，爰增訂第六項。 八、現行第六項

			移列修正條文第二十二條規定，爰予刪除。
第二十一條　特定關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，設置資通安全專職人員，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得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關得稽核所管第一項特定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特定非公務機關提出改善報告。 中央目的事業主管機關	第二十一條　特定關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，設置資通安全人員，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得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關得稽核所管第一項特定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特定非公務機關提出改善報告。 中央目的事業主管機關	第十七條　關鍵基礎設施提供者以外之特定非公務機關，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得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。 中央目的事業主管機關得稽核所管第一項特定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特定非公務機關提出改善報告。 前三項之資通安全維護計畫必要事項、實施情形之提	**行政院說明：** 一、條次變更。 二、考量資安威脅日漸加劇，資安作業須持續維持，為強化特定關鍵基礎設施提供者以外之特定非公務機關資安防護量能並能及時應處，避免其他業務排擠資安業務量能造成事件擴散，需要投入相關成本，人力資源是其中重要一環，故符合特定資通安全責任等級之特定關鍵基礎設施提供者以外之特定非公務機關，應設置專人專職辦理資通安全業務，以落實事前、事中及事後各項資安作業，確保其具有安全可靠的資通環境，爰修正第一項。

應依資安署指定之方式將稽核結果及改善報告送交資安署。	應依資安署指定之方式將稽核結果及改善報告送交資安署。	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，報請主管機關核定之。	三、第二項及第三項未修正。 四、為利資安署掌握全國資通安全現況，爰增訂第四項。 五、現行第四項移列修正條文第二十二條規定，爰予刪除。 **本報告說明：** 資訊時代資訊業務繁多，即使是公務機關未必能全面落實真正的資通安全專職人員。因此，若以此要求特定關鍵基礎設施提供者以外之特定非公務機關，恐使法律規定流於形式，爰建議第一項之「資通安全專職人員」，刪除「專職」二字。
第二十二條　前二條資通安全維護計畫之必要事項、實施情形之提出、稽核之頻率、內容與方法、結果之交付、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，報由主管機關核定。	（無修正意見）	第十六條第六項　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，報請主管機關核定之。	本條由現行第十六條第六項及第十七條第四項合併修正移列，並配合修正條文第二十條及第二十一條，增訂授權項目及酌作文字修正。

		第十七條第四項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，報請主管機關核定之。	
第二十三條　特定非公務機關應置資通安全長，由特定非公務機關之代表人、管理人、其他有代表權人或其指派之適當人員擔任，負責推動及監督機關內資通安全相關事務。	（無修正意見）		一、本條新增。 二、為確保有效推動資通安全維護事項，比照公務機關規定，特定非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，爰為本條規定。
第二十四條　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。 特定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通報。 特定非公務機關應向中	第二十四條　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。 特定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通報。中央目的事業主管機關應設置通報	第十八條　特定非公務機關為因應資通安全事件，應訂定通報及應變機制。 特定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通報。 特定非公務機關應向中央目的事業主	**行政院說明：** 一、條次變更。 二、第一項及第二項未修正。 三、配合修正條文第二條第二項規定，將第三項及第五項所定主管機關修正為資安署，並酌作文字修正。 四、為增進特定

央目的事業主管機關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，並應送交資安署。 前三項通報與應變機制之必要事項、通報內容、報告之提出、送交、演練作業及其他應遵行事項之辦法，由主管機關定之。 中央目的事業主管機關或資安署知悉重大資通安全事件時，得提供相關協助；於適當時機並得公告與事件相關之必要內容及因應措施。	窗口、線上通報平臺或通報專線。 特定非公務機關應向中央目的事業主管機關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，並應送交資安署。 前三項通報與應變機制之必要事項、通報內容、報告之提出、送交、演練作業及其他應遵行事項之辦法，由主管機關定之。 中央目的事業主管機關或資安署知悉重大資通安全事件時，應提供相關協助；於適當時機並得公告與事件相關之必要內容及因應措施。	管機關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，並應送交主管機關。 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，由主管機關定之。 知悉重大資通安全事件時，主管機關或中央目的事業主管機關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。	非公務機關因應資通安全事件之處理能力，於第四項之授權項目增訂演練作業，並酌作文字修正。 **本報告說明：** 一、鑑於公、私部門（含特定非公務機關）間資通安全事件聯繫之重要性及即時性要求日增，為強化公、私協力聯防，中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線，俾利及時應變及合作，爰建議修正第二項。 二、中央目的事業主管機關知悉該管業務相關之重大安全事件時，有積極提供協助之必要，爰建議第五項「得」提供相關協助修正為「應」提供相關協助，以利建立公、私協力機制。

第二十五條　中央目的事業主管機關為調查特定非公務機關發生重大資通安全事件，得依下列程序辦理： 一、通知當事人或關係人到場陳述意見。 二、通知當事人及關係人提出獨立第三方機構出具之鑑識或調查報告。 三、派員、委任或委託其他機關（構）前往當事人及關係人之處所實施必要之檢查。 前項所定關係人，以該項特定非公務機關委託辦理資通系統之建置、維運或資通服務提供之受託者，且與重大資通安全事件相關者為限。 受調查者對於中央目的事業主管機關依第一項所為	（無修正意見）		一、本條新增。 二、為落實特定非公務機關資通安全之維護，強化中央目的事業主管機關之監督權責，爰規定第一項，賦予中央目的事業主管機關對於重大資通安全事件之調查權。 三、為符合法律明確性原則，定明應受調查之關係人範圍，爰規定第二項。 四、配合第一項規定中央目的事業主管機關對特定非公務機關重大資通安全事件之調查權責，於第三項增訂受調查者對中央目的事業主管機關所為調查措施，不得規避、妨礙或拒絕，並於第四項規定中央目的事業主管機關執行調查時應出示證明文件之

之調查，不得規避、妨礙或拒絕。 執行調查之人員應出示有關執行職務之證明文件；其未出示者，受調查者得拒絕之。 第一項第三款受委任或委託之機關（構）對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。			程序。 五、為避免特定非公務機關之秘密，因重大資通安全事件之調查而洩漏，爰規定第五項受委任或委託機關（構）之保密義務。
第二十六條　特定非公務機關對於所屬人員辦理資通安全業務績效優良者，應予獎勵。	（無修正意見）		一、本條新增。 二、為促進特定非公務機關所屬人員對於資通安全工作之重視與投入，該等人員於踐行本法要求事項績效優良時，應予獎勵，爰為本條規定。
第二十七條　中央目的事業主管機關對特定非公務機關下載、安裝或使用危害國家資通安全產品，得予以限制或禁止；特定非公務機關自行或委外營運場所提	（無修正意見）		一、本條新增。 二、配合修正條文第十一條規定將危害國家資通安全產品限制使用之事項提升以法律位階規範，增訂中央目的事業主管機

供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時，亦同。但因業務需求且無其他替代方案者，經該特定非公務機關資通安全長核可，函報中央目的事業主管機關核定後，得以專案方式使用，並列冊管理。 前項對特定非公務機關限制或禁止使用危害國家資通安全產品之管控措施，由中央目的事業主管機關訂定，報主管機關備查。			關為維護國家資通安全，對特定非公務機關下載、安裝或使用危害國家資通安全產品，得予以限制或禁止之規定。
第四章　罰則	第四章　罰則	第四章　罰則	章名未修正。
第二十八條　公務機關所屬人員未依本法規定辦理者，應按其情節輕重，依相關規定予以懲戒或懲處。 前項懲處事項之辦法，由主管機關定之。 特定非公務機關所屬人員未依本法規定辦理，情節重大者，由特定非	（無修正意見）	第十九條　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。 前項懲處事項之辦法，由主管機關定之。	一、條次變更。 二、第一項酌作文字修正。 三、第二項未修正。 四、為促進特定非公務機關所屬人員對於資通安全工作之重視與投入，比照公務機關所屬人員規定，對未依本法規定辦理，情

公務機關依規定予以懲處。			節重大者，定明由特定非公務機關予以懲處，爰增訂第三項。
第二十九條　特定非公務機關未依第二十四條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	（無修正意見）	第二十一條　特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。	一、條次變更。 二、配合現行第十八條之條次變更，修正所引條次。
第三十條　特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；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、未依第二十條第二項或第二十一條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第二十二條所定辦法中有關	（無修正意見）	第二十條　特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；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、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項	一、條次變更。 二、配合相關現行條文條次變更或內容修正，修正所引條次及內容。

資通安全維護計畫必要事項之規定。 二、未依第二十條第三項或第二十一條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第二十二條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、未依第八條第二項、第二十條第五項或第二十一條第三項規定，提出改善報告送交中央目的事業主管機關，或違反第二十二條所定辦法中有關改善報告提出之規定。		法所定辦法中有關資通安全維護計畫必要事項之規定。 二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七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、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條	

四、未依第二十四條第一項規定，訂定資通安全事件之通報及應變機制，或違反第二十四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、未依第二十四條第三項規定，向中央目的事業主管機關提出或向資安署送交資通安全事件之調查、處理及改善報告，或違反第二十四條第四項所定辦法中有關報告提出、送交之規定。 六、違反第二十四條第四項所定辦法中有關通報內容、演練作業之規定。		或第六項或第十七條第四項所定辦法中有關改善報告提出之規定。 四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八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、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。 六、違反第十八條第四	

		項所定辦法中有關通報內容之規定。	
第三十一條　違反第二十五條第三項規定，規避、妨礙或拒絕調查者，由中央目的事業主管機關處新臺幣十萬元以上一百萬元以下罰鍰。	（無修正意見）		一、本條新增。 二、配合修正條文第二十五條第三項，增訂違反者之處罰規定。
第五章　附則	第五章　附則	第五章　附則	章名未修正。
第三十二條　主管機關得委託其他公務機關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。 資安署得委託其他公務機關辦理國家資通安全防護、演練、稽核及其他資通安全相關事務。 前二項受委託之公務機關，不得洩露辦理相關事務過程中所知悉之秘密。 特定非公務機關之業務涉及數個中央目的事業主管機關之權責，主管機關得協調	（無修正意見）	第六條　主管機關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。 前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。	一、條次變更。 二、考量現行實務運作，未將權限移轉委任所屬機關或委託法人或團體，爰修正第一項。 三、配合修正條文第二條第二項規定，增訂第二項，定明資安署得委託辦理國家資通安全防護、演練、稽核及其他資通安全相關事務之依據。 四、考量公權力之委託並無複委託情事，及受委託者就執行或辦理相關事務過程中所知

指定其中一個或數個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。			悉之秘密，除有正當理由外，應有保密之義務，不以關鍵基礎設施提供者之秘密為限，爰將現行第二項移列為第三項，並酌作文字修正。 五、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，為避免該等機關就本法所定事項權責不清，須有解決之機制，爰增訂第四項，將本法施行細則第十二條規定提升至本法規定，並酌作修正。
第三十三條　本法所定資通安全事件，涉及個人資料外洩時，公務機關及特定非公務機關應另依個人資料保護法及其相關法令規定辦理。	（無修正意見）		一、本條新增。 二、本法要求納管之公務機關及特定非公務機關訂定「資通安全維護」計畫並依計畫實施相關資通安全管理事項、訂定資通安全事件之通報及應變機

			制、通報資通安全事件等，均係屬資通安全維護義務，與個人資料保護法要求保有個人資料者應採行適當之安全措施、訂定「個人資料檔案安全維護」計畫或業務終止後個人資料處理方法等，兩者規範目的及事項不同，並無普通法及特別法之關係，有予以明辨之必要，爰增訂本條。
第三十四條　本法施行細則，由主管機關定之。	（無修正意見）	第二十二條　本法施行細則，由主管機關定之。	條次變更，內容未修正。
第三十五條　本法施行日期，由行政院定之。	（無修正意見）	第二十三條　本法施行日期，由主管機關定之。	條次變更，並修正定明本次修正條文施行日期由行政院定之。

參考文獻

一、政府出版品

1、立法院第 11 屆第 1 會期第 22 次會議議案關係文書(院總第 20 號政府提案第11006152號)，113 年 7 月 10 日印發。

2、行政院國土安全政策會報，《關鍵基礎設施盤點作業須知》，111 年 3 月 30 日。

3、行政院，《國家關鍵基礎設施安全防護指導綱要》，107 年 5 月 18 日訂正。

二、期刊論文

1、余啟民，〈從歐美資安法制發展淺析我國資通安全管理法修法草案〉，《電腦稽核期刊》，第 49 期，113 年 2 月，頁 39-55。

2、賴怡瑩，《政府機關資訊單位設置及留才攬才相關問題探討(編號A01675)》，臺北市：立法院法制局，113 年 4 月。

3、賴怡瑩，〈資安治理機制之法制研析〉，立法院法制局議題研析(編號 R02361)，113 年 2 月 15 日，頁 1-3。

4、黃俊泰，〈美國關鍵基礎設施威脅資訊分享框架簡介〉，《清流雙月刊》，第 14 期，107 年 3 月，頁 4-10。

5、陳映竹，〈網路治理趨勢下之資通安全法令：談臺灣「資通安全管理法（草案）」〉，《臺灣經濟研究月刊》，第 40 卷第 10 期，106 年 10 月，頁 46-53。

6、呂正華，〈資安即國安，提升資安韌性 實踐企業永續〉，《會計研究月刊》，第 456 期，112 年 11 月，頁 76-81。

三、網路資源

1、資安署網站/關鍵基礎設施資安防護，112 年 2 月 21 日，網址：https://moda.gov.tw/ACS/operations/ciip/650，最後瀏覽日期：113 年 10 月 2 日。

2、AIoT Cloud 物聯雲，IT 與 OT 的融合如何實現智慧工廠？，就享知 DigiKnow，112 年 4 月 7 日，網址：https://www.digiknow.com.tw/knowledge/642e298a57b33，最後瀏覽日期：113 年 9 月 25 日。

3、施柏榮，為什麼我們應該再談數位關鍵基礎設施？，財團法人資訊工業策進會，112 年 4 月 6 日，網址：https://www.iii.org.tw/focus/FocusDtl.aspx?f_type=1&f_sqno=fWF0UuVWfaBVyxfq%2bRrwDA__&fm_sqno=12，最後瀏覽日期：113 年 9 月 25 日。

4、黃彥棻，【盤點《資安法》修法草案重點 3】公務機關遇重大資安事件，資安署有權調度各機關資安人員支援，iThome，112 年 11 月 10 日，網址：https://www.ithome.com.tw/news/159736，最後瀏覽日期：113 年 10 月 1 日。

5、崔慈悌，臺灣資安國家隊成立！蔡英文：確保數位國土安全，中時電子報，112 年 5 月 9 日，網址：https://www.chinatimes.com/realtimenews/20230509002860-260407?chdtv，最後瀏覽日期：113 年 9 月 25 日。

附錄一：「資通安全管理法修正草案」評估報告（初稿）座談會紀錄及參採情形

時間：民國 113 年 10 月 9 日（星期三）上午 10 時

地點：立法院法制局 305 會議室

主席：盧組長焜鑫　　紀錄：楊蕙如

參加人員：

一、 學者專家

東吳大學法律學系 余副教授啟民

二、 數位發展部資通安全署

副組長　黃哲上

科　長　林郁智

視　察　李媛婷

視　察　楊維銘

三、 本局出席人員

賴研究員怡瑩

楊副研究員盛旺

曾副研究員耀民

發言要點：

東吳大學法律學系余副教授啟民：

原則上對於以下分析建議均採支持，惟建議以下供參：

一、關鍵基礎設施應宜於本法明定主要領域，以符法律保留原則（草案第 3 條第 7 款）：關鍵基礎設施的指定目前在國土安全辦公室，明定與否恐非資安署所能為。

二、有關特定關鍵基礎設施提供者定義之「資通系統」宜修正為「資通系統或調度、控制系統」，以資明確並符實際（草案第 3 條第 8 款）：在歷次公聽會中獲得的迴響是不希望將「特定關鍵基礎設施提供者」予以擴張，否則將可能涵及電商業者（目前為產發署轄管）。至於增設「或調度、控制系統」立意甚佳，但立法過程可能產生「**或**調度、控制系統」及「**及**調度、控制系統」等不同提案版本之不確定法律概念之嫌。

三、建議由中央主管機關訂定契約範本供參，減少因契約規範不明衍生之資通安全風險（增訂草案第 10 條第 3 項）：支持。

四、為落實政府資訊公開之原則，危害國家資通安全產品之產品清單，宜由主管機關定期公告之（草案第 11 條第 3 項）：支持，建議資安署應將此點與第七點整合評析建立平臺，利用 API(Application Programming Interface)介接，定期反映，以落實資訊公開並符合民眾及廠商之企盼。

五、遇有重大資通安全事件，資安署「得調度各級機關資通安全人員支援之」之規定，宜於子法訂定相關機制（草案第 18 條第 2 項）：資通安全管理法母法本身比較扼要，相關配套子法非常多，宜全盤檢討調整因應。建議未來法案討論時資安署能針對此詳細說明相關配套子法調修之方向與進程。

六、特定關鍵基礎設施提供者以外之特定非公務機關，設置「資通安全專職人員」，建議修正為「資通安全人員」（草案第 21 條第 1 項）：資通安全管理法與個人資料保護法兩法之設計類似，均在規範中分成公務機關與非公務機關。但資安法並未像個人資料保護法施行細則第 12 條有「比例原則」之適用。未來母法或子

法修訂時宜針對非公務機關部分參酌「比例原則」設計，以符實際所需。

七、中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線（草案第 24 條第 2 項）：支持，請與第四點一併考量整合評析建立平臺，利用 API 介接，定期反映，以落實資訊公開並符合民眾及廠商之企盼。

八、資安署知悉重大資通安全事件時，「應」提供相關協助（草案第 24 條第 5 項）：通報應變機制為此次資通安全管理法修法重點方向，建議於適當處將 CERT 機制導入或列於立法說明中，以利落實時要求通報聯防之需。

參採情形：

一、第一點意見，說明關鍵基礎設施的指定非資安署之權。惟關鍵基礎設施「主領域」係關鍵基礎設施分類之第一層，非經年變動，非謂不得於法律中明定，錄供參考。

二、第二點意見，說明增設「或調度、控制系統」立意佳，可能產生「**或**調度、控制系統」及「**及**調度、控制系統」等諸多提案版本之議論，涉及納管業者之認定。因第 3 條第 8 款尚有「經中央目的事業主管機關指定，送由主管機關報請行政院核定者。」程序之規定；若仍有疑義，亦可透過子法詳訂本條款之適用規則，明確相關權責，錄供參考。

三、第三點意見，贊同本報告所提建議。

四、第四點及第七點意見，贊同本報告所提建議，具體作法為建議資安署應將第四點(國家資通安全產品之公告)與第七點(通報窗口、線上通報平臺)整合評析建立平臺，利用 API 應用程式介面之

介接(即定義不同軟體系統之間如何互動的規則和協定)，定期反映並落實資訊公開。

五、第五點意見，建議未來法案討論時資安署能針對人員調度詳細說明人員調度相關「配套子法」調修之方向與進程。

六、第六點意見，說明個人資料保護法施行細則第 12 條有關配置管理之人員及相當資源，與所欲達成之個人資料保護目的間，具有適當比例為原則，可供本法針對非公務機關人員設置時參酌，錄供參考。

七、第八點意見，建議將 CERT 機制(Taiwan Computer Emergency Response Team Coordination Center，臺灣電腦網路危機處理暨協調中心)導入或列於立法說明中，以利落實時要求通報聯防之需，錄供參考。

數位發展部

資通安全署黃副組長哲上：

一、關鍵基礎設施應宜於本法明定主要領域，以符法律保留原則：建議維持原院版條文內容，理由：行政院設國土安全政策會報已依我國各領域現況視情形定期盤點及評估，滾動調整 CI 領域。建議無須於資安法之重複定義或另規範 CI 領域;另考量 CI 領域判斷非僅資安問題，又衡酌技術更新速度，為免遇 CI 新增或領域異動時，需重新修正資安法案搭配，致影響業務效率等問題，故建議不另於資安法中另定 CI 領域之規範。

二、為落實政府資訊公開之原則，危害國家資通安全產品之產品清單，宜由主管機關定期公告之：建議維持原院版條文內容，理由：未來規劃資安法改以產品風險情資方式分享，訂定危害國家資通

安全產品之審查程序、產品情資分享等作法，並同時考量國安、經貿等領域衝擊因素，綜合妥適評估產品資安風險，並透過分享產品風險情資方式，強化公務機關資通安全防護，降低國家資通安全風險。

三、中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線：建議維持原院版條文內容，理由：有關草案第 24 條第 1 項業敘明特定非公務機關為因應資通安全事件，應訂定通報及應變機制，又依資通安全事件及通報應變辦法第 11 條特定非公務機關知悉資通安全事件後，應依中央目的事業主管機關指定方式，進行資通安全事件通報，各關鍵基礎設施領域業建立通報平臺如金融領域 F-CERT 並有對應之通報窗口，相關機制已完備。

四、資安署知悉重大資通安全事件時，「應」提供相關協助：建議維持原院版條文內容，理由：機關於發生資通安全事件時，應依「資通安全事件通報及應變辦法」相關規定即時通報及應變，迅速完成損害控制或復原作業，降低資通安全事件對各機關業務之衝擊影響，並確保資通安全事件發生時之跡證保存；又機關發生重大資安事件原因不盡相同，機關於事件通報時皆會先行評估是否請求支援，倘有需求者主管機關將於確認後提供進一步之協助，故有關是否提供相關協助應視該資安事件情境及機關本身需求而定，尚非能一體適用。

資通安全署林科長郁智：

五、特定關鍵基礎設施提供者定義之「資通系統」宜修正為「資通系統或調度、控制系統」：建議維持原院版條文內容，理由：資安法第 3 條第 1 款「資通系統」係「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」，已涵括調度、控制系統之功能。故第 3 條第 8 款特定關鍵基礎設施者之「資通系統」定義建議無須修正。

六、由中央主管機關訂定契約範本供參，減少因契約規範不明衍生之資通安全風險：建議維持原院版條文內容，理由：各機關辦理資通訊採購案，以採用行政院公共工程委員會(下稱工程會)訂定之採購契約範本為原則。為協助各機關強化資通安全防護及妥適辦理資訊服務採購，工程會亦持續與本部合作研訂採購文件範本，考量政府採購之主管機關為行政院公共工程委員會，且相關規定於政府採購法已有明文，故建議不另於資安法中規範。

七、遇有重大資通安全事件，資安署「得調度各級機關資通安全人員支援之」之規定，宜於子法訂定相關機制：法制局建議有關調度支援部分，目前本署已規劃於子法訂定相關機制，包括調度前需徵得機關同意，並以短期支援處理重大資安事件為原則，如情形特殊必要時再評估是否延長調度時間，以減少對機關業務運作之影響。

八、特定關鍵基礎設施提供者以外之特定非公務機關，設置「資通安全專職人員」建議修正為「資通安全人員」：建議維持原院版條文內容，理由：資安工作需具備獨立性，各機關於進行數位化的同時，應輔以資安管控措施，而資安法為最基礎要求。資安人員因身兼稽核角色，且資安工作屬組織安控機制之一環，應確保其角色所必須之獨立性，如資安人員同時兼任其他工作，則易造成實務工作上之矛盾，或因角色衝突易選擇降低資安防護所需之資源配置；「專職」之角色設計賦予人員具備使命感，可深化資安

人員之角色認知，對於應承擔責任之具備足夠之認識，有助於資安應變所需之時效性及專業性，以促進機關整體資安政策及相關機制之推動。

參採情形：

一、第一點意見，說明行政院既已定期盤點，無在法條中規範之必要。惟鑑於本草案納管對象加諸其通報等義務並定有罰則，基於法律保留原則，維持本報告所提建議。

二、第二點意見，說明以情資分享方式來強化機關之安全防護。惟定期公告產品清單之方式更為明確，爰維持本報告所提建議。

三、第三點意見，說明關鍵基礎設施之 8 大領域領中之金融領域已有機制完備之通報窗口。惟本報告建議不分領域均得通報之整合評析平臺、窗口，非僅某領域有其個別之通報平臺，爰維持本報告所提建議。

四、第四點意見，說明機關於遭遇資安事件通報時會先評估是否請求支援，依情境及需求而定。惟本報告建議資安署「應」提供相關協助之情形，僅限於「重大資安事件」，例如 2022 年 8 月美國聯邦眾議院議長裴洛西（Nancy Pelosi）訪臺，部分公共場域電子看板遭駭出現謾罵議長之不雅內容，為近年發生之重大資安事件。由於全臺各地多處運輸系統及超商電子看板遭駭已非單一事件，中央目的事業主管機關或資安署知悉此等重大資安事件發生時「應」提供相關協助、強化資通安全事件之處理能力，尚無疑義，爰維持本報告所提建議。

五、第五點意見，說明資安法第 3 條第 1 款有關資通系統之定義「指用以蒐集、控制……刪除資訊……」，故建議無須修正第 3 條第 8 款

。惟維運或提供關鍵基礎設施全部或一部所依賴之系統，非僅只資訊內部的控制，尚係包含其它操作技術（調度、控制系統），例如106年之815大停電，起因於更換電源供應器作業疏失，導致暫停供應天然氣2分鐘，造成台電大潭電廠機組跳電，瞬間減少420萬瓩供電量，幾乎癱瘓所有交通、郵政、科技及民生等設施。關鍵基礎設施防護的失效，造成國家經濟重大損失，甚至有可能影響國家安全。資通系統須與關注實際的工業操作和過程控制之操作技術（調度、控制系統）接軌合作，方能使關鍵基礎設施順利維運。另特定業者是否納管，因其尚經主管機關指定程序，亦可透過子法詳訂本條款之適用規則，明確相關權責，爰維持本報告所提建議。

六、第六點意見，說明以工程會現有之採購契約範本為主，不建議於本法中再規範。由於資通(安全)服務領域重要性提升，且相關採購金額及數量龐大，有必要建立更明確之規範(包含「應記載及不得記載事項」之契約範本)，以減少因契約規範不明或不當衍生之風險。然目前工程會現行公告之採購契約範本並非均包含「應記載及不得記載事項」，爰維持本報告所提建議。

七、第七點意見，說明資安署已規劃於子法定相關機制，包括調度前徵得機關同意，與本報告所提建議方向一致。

八、第八點意見，敘明設置資通安全專職人員可強化其獨立性及使命感，有助資安政策推動。惟實務上資訊安全無法單獨存在，因資安業務實為資訊業務之一環，不但應並重且應該高度整合於資訊軟硬體設施與相關業務系統生命週期的所有階段，並讓資訊與資安人力得以相互支援合作，方對資訊資安業務有根本助益。尤其在目前人力有限之情況下，若要求資安人力只能全職從事資安業

務，縱使可強化其獨立性及使命感，卻未必利於特定關鍵基礎設施提供者以外之特定非公務機關之整體資訊業務運作，爰維持本報告所提建議。

賴研究員怡瑩：

一、本草案第 7 條第 3 項規定，公務機關及非特定公務機關「專職人員之配置與專業條件」另定辦法；第 18 條第 1 項及第 2 項及第 19 條第 1 項規定，公務機關「資通安全專職人員」相關規定；第 20 條第 2 項規定，特定關鍵基礎設施提供者設置「資通安全專職人員」；及第 21 條第 1 項規定，特定關鍵基礎設施提供者以外之特定非公務機關設置「資通安全專職人員」等，係以法律明文匡定「**公務機關**」「**非特定公務機關**」及「**特定關鍵基礎設施提供者**」均需設置「**資通安全**」「**專職人員**」。上開規定實有下述疑義：

（一）實務界認為，資訊安全沒辦法單獨存在，沒有資訊直接談資安其實是不切實際的，所以在討論資訊安全時必須同時重視資訊，資訊和資安應該要並重[27]；另學者亦認為，以學理定義與實務運作來看，資安業務其實為資訊業務的一環，不但應該並重，而且應該高度整合於資訊軟硬體設施與相關業務系統生命週期的所有階段[28]。爰此，目前在制度設計及業務推動上，似尚難明確區隔資訊及資安業務，

（二）再者，學者認為，兼具效率與品質的人力運用機制，應該是善用資安法規與機關業務需求，讓資訊與資安人力得以相互支援及輪調，同時善用相關專業誘因（如專業加給）

[27]立法院第 10 屆第 2 會期「因應數位發展部成立，公、私部門資安人力建制及產業資源探討」公聽會報告-行政院資通安全處書面報告資料，109 年 12 月 7 日，頁 10。

[28] 引國立政治大學公共行政系蕭副教授兼系主任乃沂發言，詳見：賴怡瑩，同註 13，頁 24。

與人力培訓發展制度，才能對於人力素質提升與資訊資安業務推動有根本助益[29]，因之，資安人力如全職從事資安業務，恐不利公、私部門整體資訊業務運作。

二、依上，本研究建議本草案第 21 條第 1 項「特定關鍵基礎設施提供者以外之特定非公務機關，設置『資通安全專職人員』，建議修正為『資通安全人員』」值得肯定；惟似得進一步研議「公務機關」及「特定關鍵基礎設施提供者」資訊及資安業務區別情形，以及設置「資通安全」「專職人員」是否會造成整體資訊業務推動之困擾。

三、其餘敬表尊重與贊同。

參採情形：

一、第一點及第三點意見，贊同本報告所提建議。

二、第二點意見，「公務機關」及「特定關鍵基礎設施提供者」資訊及資安業務區別之妥適性亦得進一步研議，錄供參考。

楊副研究員盛旺：

一、本報告建議宜將關鍵基礎設施分類之第一層「主領域」在草案第 3 條第 7 款關鍵基礎設施之定義中明確敘明，將關鍵基礎設施安全防護之範圍予以明確規定，爰本報告建議第 3 條第 7 款修正條文「關鍵基礎設施：指能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等行政院定期檢視並公告之領域中，該領域服務所依賴之實體或虛擬資產、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者。」惟查行政院「國家關鍵基礎設施安全防護指導綱要」附件一「國

[29] 同前註。

家關鍵基礎設施領域分類」已定明能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等 8 項主領域及其所對應之 20 項次領域。行政院提案建議第 3 條第 7 款修正條文：「關鍵基礎設施：指行政院定期檢視並公告之領域中，該領域服務所依賴之實體或虛擬資產、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者。」按其文義，行政院似將透過定期檢視並公告關鍵基礎設施分類領域，以定期滾動檢討之機制，保持彈性調整關鍵基礎設施分類領域，且行政院已於前開指導綱要明定關鍵基礎設施領域分類，未來也將定期檢視公告調整，爰此，是否維持行政院提案條文，有否再洽行政院意見以釐清之必要，以上意見，僅供參酌。

二、本報告所提其他研析建議，均敬表贊同。

參採情形：

一、第一點意見，說明行政院既定期檢視並公告，是否有在法條中再行釐清之必要。鑑於本草案納管對象加諸其通報等義務並定有罰則，基於法律保留原則，維持本報告所提建議。

二、第二點意見，贊同本報告所提其他建議。

曾副研究員耀民：

一、本報告問題研析與建議第 1 項（第 2 頁）關鍵基礎設施應宜於本法明定主要領域，以符法律保留原則。經查本法於民國 107 年 5 月通過制定時有附帶決議表示：「這個草案還有一些不足的地方，譬如對於關鍵基礎設施的定義。目前關鍵基礎設施是透過 20 年前國土安全辦公室的功能性分類，但是依照科技的進步，這個部分將來或許會有所不足。所以，依然必須堅持以精確的定義來

重新定義關鍵基礎設施，希望在此法上路後，可以滾動式檢討、確保公開透明，並且邀請相關學者專家加入討論。」因此，對於本報告（第 3 頁）指出，基於法律之位階與明確性，爰建議修正本草案第 3 條第 7 款：「關鍵基礎設施：指能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等行政院定期檢視並公告之領域中，該領域服務所依賴之實體或虛擬資產、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者。」，可資贊同。

二、有關本報告問題研析與建議第 4 項（草案第 11 條第 3 項），2022 年 8 月美國聯邦眾議院議長裴洛西（Nancy Pelosi）訪臺，隨後部分機關傳出網站癱瘓，部分公共場域電子看板內容亦遭竄改，監察院通過調查報告，指出在公私協力、橫向協調、改善公私部門資安從業人員困境及軟體供應鏈安全等面向確有不足。調查報告還指出，資安法規範對象為公務機關及特定非公務機關；然而對於私部門之資安風險事前控制措施建立尚無有效政策推動工具，允宜加強。綜上所述，為落實政府資訊公開之原則，並使各機關利於確實遵行不得下載、安裝或使用危害國家資通安全產品等之規定，「危害國家資通安全產品」宜清楚定義並予公告之以供查詢。所以，問題研析與建議第 4 項，為落實政府資訊公開之原則，危害國家資通安全產品之產品清單，宜由主管機關定期公告之（草案第 11 條第 3 項），可資贊同。

三、問題研析與建議第 7 項，中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線（草案第 24 條第 2 項）。本報告指出，鑑於公、私部門（含特定非公務機關）間資通安全事件之縱向及橫向聯繫重要性及即時性之要求日增，為強化公、私協力，

建立情資分享及合作聯防機制，中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線，俾利及時應變及合作。爰參酌人口販運防治法規定之體例，建議本草案第 24 條第 2 項修正為：「特定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通報。中央目的事業主管機關應設置通報窗口、線上通報平臺或通報專線。」，基於國家重大資安事件之緊急性及嚴重性甚至超過人口販運事件，主管機關設置通報窗口等，當屬可資贊同。

參採情形：

第一點、第二點及第三點意見，贊同本報告所提建議。

散會：上午 11 時 15 分

附錄二：數位發展部法案及性別影響評估檢視表

【第一部分】：本部分由機關人員填寫　　108.10.01 生效

填表日期：　113 年　2 月　15　日
‧填表人姓名：楊維銘 職稱：視察　電話：02-2380-8807　e-mail：crisot52@acs.gov.tw 身分：□業務單位人員　　■法制單位人員　□其他，請說明：＿＿＿＿＿＿ ‧法案已於研擬初期■徵詢性別諮詢員之意見，或□提報各部會性別平等專案小組（會議日期：＿＿＿年＿＿＿月＿＿＿日） 性別諮詢員姓名：莊喬汝 服務單位及職稱：德臻法律事務所身分：符合本表填表說明第三點第（一）款（如係提報各部會性別平等專案小組者，免填）
填　表　說　明 1、行政院所屬各機關主管法律案報院審查，應依「行政院所屬各機關主管法案報院審查應注意事項」及「中央行政機關法制作業應注意事項」規定辦理。 2、除廢止案（及配合行政院組織改造整批處理、單純訂修之法律案）外，皆應依據本表進行「法案及性別影響評估」。 三、建議各單位於法案研擬初期，即應徵詢性別諮詢員（至少 1 人），或提報各部會性別平等專案小組，收集性別平等觀點之意見。性別諮詢員應符合下列資格之一（請提醒性別諮詢員恪遵保密義務，未經部會同意不得逕自對外公開法案草案）： （一）現任臺灣國家婦女館「性別主流化人才資料庫」專家學者（公、私部門均可）。(人才資料庫網址: http://gm.taiwanwomencenter.org.tw/zh-tw/Home/Index/) （二）現任或曾任行政院性別平等會民間委員。 （三）現任或曾任各部會性別平等專案小組民間委員。 （四）曾任各機關性別平等專責人員（性平業務至少占所辦業務 7 成以上）累積滿 2 年者，或曾任性別平等兼辦人員（性平業務至少占所辦業務 3 成以上）累積滿 3 年者。 （五）曾辦理或協助各機關「法案及性別影響評估檢視表」填寫作業，且經行政院性別平等處「性別影響評估案例分享專區」收錄至少 1 案者。 四、法案研擬完成後，應併同本表送請性別平等專家學者進行程序參與（至少預留 1 週之填寫時間），參酌其意見修正法案內容，並填寫「玖、性別影響評估結果」後通知程序參與者。

壹、法案名稱	資通安全管理法修正草案		
貳、主管機關	數位發展部	主辦機關	數位發展部資通安全署

參、法案內容涉及領域：	勾選（可複選）
3-1 權力、決策、影響力領域	
3-2 就業、經濟、福利領域	
3-3 人口、婚姻、家庭領域	
3-4 教育、文化、媒體領域	
3-5 人身安全、司法領域	
3-6 健康、醫療、照顧領域	
3-7 環境、能源、科技領域	V
3-8 其他（勾選「其他」欄位者，請簡述法案涉及領域）	

肆、問題界定與訂修需求			
項　目		**說　明**	**備　註**
4-1 問題界定	**4-1-1 問題描述**	1.資通安全管理法（以下簡稱資安法)於 107 年 6 月 6 日制定公布，並於 108 年 1 月 1 日施行，迄今未曾修正。 2.配合數位發展部（以下簡稱數位部）於 111 年 8 月 27 日成立，掌理國家資通安全業務，並下設數位發展部資通安全署（以下簡稱資安署)，掌理國家資通安全之規劃、推動與執行。 3.因應資訊安全威脅之數量及複雜性加劇、納管對象範圍及相關法遵事項有不足或待修正之處、國際情勢及地緣政治特性等，資通安全重要性等同國家安全，應有更高資通安全防護之需求，爰有修正資安法之必要性。	簡要說明所面臨問題之梗概。
	4-1-2 執行現況及問題之分析	1.111 年 8 月 27 日數位部及資安署成立後，外界就國家資通安全業務分工常有疑義，爰明定權責機關；部分納管機關缺乏第二方稽核制度，難以確認法遵落實情形，易生資安風險，爰增訂資安署之稽核權限。 2.為落實橫向聯繫機制與健全資通安全管理法制，宜將現行國家資通安全會報入法，以強化中央地方聯防機制。 3.現行危害國家資通安全產品之管制係規定於行政規則，其效力範圍有其侷限性，爰將公務機關不得下載、安裝或使用危害國家資通安全產品及產品情資分享入法明文化。 4.公務機關之資安人員流動頻繁，不利於國家整體資安防禦工作，爰增訂強化資通安全人員專業知能及重大資通安全事件之調度支援，以利全面性提升政府資安	1.業務推動執行時，遭遇問題之原因分析。 2.說明現行法規是否不足、須否配合現況或政策調整。

		防護效能。 5.考量公務機關之資通安全專職人員辦理資通安全業務時，可能觸及國家、軍事及國防秘密，爰增訂適任性查核機制。 6.為確保有效推動資通安全維護事項，強化特定非公務機關資安管理，爰明定應置資安長及專職人員，提升其法遵義務，並增訂應配合接受行政調查。 7.有關中央目的事業主管機關辦理特定非公務機關發生重大資通安全事件之調查，為確保隱私權及營業秘密之維護，明定受委任或委託機關（構）之保密義務，避免因重大資通安全事件之調查而洩密。 8.資通安全管理法規範屬資通安全維護義務；個人資料保護法要求保有個人資料者應採行適當之安全措拖，兩者之立法目的及構成要件皆不相同，有予以明辨之必要，爰增訂資通安全事件如涉個人資料外洩，應另依個人資料保護法及其相關法令規定辦理。	
4-2 訂修需求	**4-2-1 解決問題可能方案**	1.因應行政院公告數位部為資安法之主管機關，及下設資安署執掌職國家資通安全業務，配合上開公告修正現行條文。 2.透過修正現行資安法規定，再配合增訂及修正相關子法，全面性提升國家資通安全防護效能。 3.綜上，僅能修正母法增加相關權責，以達資通安全管理法立法目的。	請詳列解決問題之可能方案及其評估（涉及性別平等議題者，併列之）。
	4-2-2 訂修必要性	如不修訂，可能難以因應目前資通安全威脅之數量及其加劇之複雜性。	請說明最終必須訂修法案以解決問題之理由；如有立委提案，並請納入研析。
4-3 配套措施及相關機關協力事項		1.配合資安法修正，增訂及修正相關子法規定。 2.因應修法議題及可能衍生爭議之組職人力需求。	配套措施諸如人力、經費需求或法制整備等；相關機關協力事項請予詳列。

	3.透過辦理相關子法修法說明會，加強與納管機關、民眾溝通。 4.特定非公務機關應置資安長及專職人員，並配合重大資安事件行政調查，相關特定非公務機關可能提高相關人力成本。 5.建立中央地方聯防體系，強化跨機關資通安全事件應處及協調能力。 6.因應資安法修法擴大稽核範圍，衍生人力及經費需求。 7.跨部會研商危害國家資通安全產品之情資分享。 8.跨部會研商適任性查核權責機關、應受查核人員、查核程序、內容及其他相關事項之辦理。	
伍、政策目標	完善資安法制，明確劃分權責機關、擴大稽核範圍、強化特定非公務機關風險管理、增訂公務機關及特定非公務機關對於危害國家資通安全產品有關下載、安裝或使用之相關規定及強化資通安全人員專業知能及重大資通安全事件之調度支援，以期國家整體資通安全防護更有韌性。	簡要說明政策取向。

陸、徵詢及協商程序

項　目	說　明	備　註
6-1 法案主要影響對象	本草案適用對象為公務機關及特定非公務機關等，不因不同對象性別而有差別對待情事。	請說明法案內容主要影響之機關（構）、團體或人員。
6-2 對外意見徵詢	1.針對修正草案重點內容，於 112 年 舉辦 6 次修法工作坊及 16 次修法說明會，與納管機關及相關利害關係人進行意見交換。出席人員共計 1778 名，男性 1152 名占 65%，女性 626 名占 35%。 2.修正草案於 112 年 9 月 22 日公告於行政院國發會眾開講平臺及數位部官網法規預告 60 日，並函知各政府機關、各相關團	1.請說明對社會各界徵詢意見及與相關機關（構）、地方自治團體協商之人事時地。 2.徵詢或協商時，應敘明其重要事項、有無爭議、相關條文、主要意見、參採與否及其理由（含國際參考案例），並請填列於**附表**；如有其他相關資料，亦請一併檢附。 3.對社會各界徵詢意見，應落實性

	體，以蒐集各前開機關、團體意見。	別參與，如有相關參與者性別統計資料，請一併檢附。
6-3 與相關機關（構）及地方自治團體協商	於 113 年 1 月 24 日召開跨院、部、會之溝通會議，並函請六都派員與會，參酌各機關建議，調修草案。	

柒、成本效益分析及對人權之影響：

項　目		**說　明**	**備　註**
7-1 成本		配合資安法新增相關人力成本、行政成本。	1.關於成本及效益，指政府及社會為推動及落實法案必須付出之代價及可能得到之效益。 2.得量化者應有明確數字，難以量化者亦應有詳細說明。
7-2 效益		完善資通安全管理法制，提升納管對象之法遵義務，強化監督機關之職責，以期國家整體資通安全防護更為堅實。	
7-3 對人權之影響	**7-3-1 憲法有關人民權利之規定**	經檢視無違憲之虞。且經檢視憲法工作權及平等原則，本法規定並無差別對待及性別歧視。	請檢視法案是否符合憲法有關人民權利之規定及司法院解釋。
	7-3-2 公民與政治權利國際公約	經檢視無違反公民與政治權利國際公約之虞。	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國人權事務委員會之一般性意見，以積極促進各項人權之實現。
	7-3-3 經濟社會文化權利國際公約	經檢視無違反經濟社會文化權利國際公約之虞。	依公民與政治權利國際公約及經濟社會文化權利國際公約施行法，請檢視法案是否符合公約規定及聯合國經濟社會文化權利委員會之一般性意見，以積極促進各項人權之實現。

捌、性別影響評估：以下各欄位除評估法案對於不同性別之影響外，亦請關照對不同性傾向、性別特質或性別認同者之影響。

評估項目	評估結果	**備註**

8-1 從性別統計及性別分析，確認與法案相關之性別議題	本修正草案重點為主管機關調適、擴大稽核範圍、強化特定非公務機關管理、增訂公務機關及特定非公務機關對於危害國家資通安全產品有關下載、安裝或使用之相關規定及強化資通安全人員專業知能及重大資通安全事件之調度支援，修正內容並無直接涉及性別，其執法之結果，亦不致對不同性別、性傾向或性別認同者產生差別待遇。	1.請蒐集與法案相關之性別統計既有資料，並進行性別分析。 請參閱行政院性別平等會「性別平等研究文獻資源網（https://www.gender.ey.gov.tw/research/）、「重要性別統計資料庫」（https://www.gender.ey.gov.tw/gecdb/）、各部會性別統計專區、我國婦女人權指標及「行政院性別平等會—性別分析」（https://gec.ey.gov.tw）。 2.前開性別統計與性別分析應盡量顧及不同性別、性傾向、性別特質及性別認同者，探究其處境或需求是否存在差異，及造成差異之原因；並宜與年齡、族群、地區、障礙情形等面向進行交叉分析（例如：高齡身障女性、偏遠地區新住民女性），探究在各因素交織影響下，是否加劇其處境之不利，並分析處境不利群體之需求。 3.請根據前開性別統計及性別分析，確認並說明法案相關之性別議題。 4.如既有性別統計及分析資料不足，請提出需強化之處及其建置方法。
8-2 落實性別平等相關法規與政策之內涵	無關。	1.法案若涉及下列情形，本欄位不得填列無關： (1)內容係以特定性別、性傾向或性別認同者為規範對象。 (2)內容涉及一般社會認知既存之性別偏見。 (3)「8-1」欄所填列之性別統計資料顯示性別比例差距過大。 2.請依「8-1」欄所確認之性別議題，說明其與下列第 3 點所列性別平等相關法規與政策之相關性。 3.本欄位所指性別平等相關法規與政策，包含消除對婦女一切形式歧視公約（CEDAW）及其一般性建議、性別平等政策綱領及各機關有關促進性別平等相關之法規、政策、白皮書或計畫等。 4.落實前開相關法規與政策之常見態

		樣及案例： (1)採行一定方式去除現行法規及其執行所造成之差別待遇，提供較為弱勢之一方必要之協助，以促進其實質地位之平等。 例如：為落實 CEDAW 第 11 條消除在就業方面對婦女之歧視，刪除禁止女性於夜間工作等限制女性工作權之規定，並增訂雇用人應提供必要之夜間安全防護措施。 (2)消除或打破性別刻板印象與性別隔離，以消弭因社會文化面向所形成之差異。 例如：為促進媒體製播內容符合性別平等精神，規範節目或廣告內容不得有性別歧視之情形。 (3)提供不同性別、性傾向或性別認同者平等機會獲取社會資源，提升其參與社會及公共事務之機會。 例如 1：為協助因家庭因素離開職場之婦女，能重返職場，提升婦女勞動參與，規範二度就業婦女為政府致力促進就業之對象。 例如 2：為提升女性參與公共事務之機會，擴大參與管道，對涉及諮詢及審議性質之機制，規範其成員任一性別比例不得少於三分之一。 5.請優先將有助落實上開內容之部分納入法案相關條文規定、授權命令或未來業務執行事項，並於本欄位提出說明。
玖、性別影響評估結果 請機關填表人依據「填表說明四」辦理【第二部分、性別影響評估程序參與】，再續填下列「玖、性別影響評估結果」。		
9-1 評估結果之綜合說明	1.本案在「正當程序中性別參與」、「從性別統計及性別分析與法案相關之性別議題」，及「落實性別平等相關法規與政策之內涵」三項評估項目中，皆經性別平等專家學者表示為「合宜」。 2.性別平等專家學者對本案綜合性評估結果，認為本修正草案修正目的、內容等，未來施行及受益對象為全體國民，尚無涉性別。	
9-2 參採情形	**9-2-1 說明採納意見後之調整情形（含法案、授權命令或業務執行之修正等）**	本案無涉性別，爰未予調整。

	9-2-2 說明未參採之理由或替代規劃	本案無涉性別，爰無未參採理由及替代規劃之情形。

9-3 通知程序參與之專家學者法案評估結果（請填寫日期及勾選通知方式，請勿空白）：

已於 113 年 3 月 1 日將「評估結果」以下列方式通知程序參與者審閱

□傳真　■e-mail　□郵寄　□其他

拾、法制單位復核（此欄空白未填寫者，將以不符形式審查逕予退件。）

10-1 法案內容：　■提經法規會討論通過　■已會法制單位表示意見

10-2 徵詢及協商程序：　■已徵詢及協商法案主要影響對象

■已適當說明與回應徵詢及協商對象所提之主要意見

10-3 對人權之影響：　■已由法規會具人權專長委員、曾受人權教育訓練之參事、其他高階人員或委請之人權學者專家檢視

10-4 訂修程序：　■本檢視表已完整填列

復核人姓名及職稱：林郁智科長

【第二部分－性別影響評估程序參與】：本部分由性別平等專家學者填寫

<table>
<tr><td colspan="2">拾壹、程序參與之性別平等專家學者應符合下列資格之一：
■1.現任臺灣國家婦女館網站「性別主流化人才資料庫」專家學者；其中公部門專家應非本機關及所屬機關之人員（人才資料庫網址:http://www.taiwanwomencenter.org.tw/）。
□2.現任或曾任行政院性別平等會民間委員。
□3.現任或曾任各部會性別平等專案小組民間委員。</td></tr>
<tr><td colspan="2">（一）基本資料</td></tr>
<tr><td>11-1 程序參與期程或時間</td><td>113 年 2 月 15 日 至 113 年 2 月 19 日</td></tr>
<tr><td>11-2 參與者姓名、職稱、服務單位及其專長領域</td><td>莊喬汝律師、德臻法律事務所合夥律師、
性別與法律、性別與勞動</td></tr>
<tr><td>11-3 參與方式</td><td>□法案研商會議 □性別平等專案小組 ■書面意見</td></tr>
<tr><td colspan="2">（二）主要意見（若參與方式為提報各部會性別平等專案小組，可附上會議發言要旨，免填 11-4 至 11-7 欄位，並請通知程序參與者恪遵保密義務）</td></tr>
<tr><td>11-4 正當程序中性別參與之合宜性</td><td>合宜</td></tr>
<tr><td>11-5 從性別統計及性別分析，確認與法案相關之性別議題之合宜性</td><td>合宜</td></tr>
<tr><td>11-6 落實性別平等相關法規與政策之內涵之合宜性</td><td>合宜</td></tr>
<tr><td>11-7 綜合性檢視意見</td><td>本修正草案修正目的及內容係明定主管機關，以明確劃分權責機關、增訂公務機關及特定非公務機關對於危害國家資通安全產品有關下載、安裝及使用之相關規定，同時擴大稽核範圍，強化資通安全人員專業知能及重大資通安全事件之調度支援，健全我國整體資工安全管理，以期完善資安法制，使國家整體資通安全防護更有韌性，本部草案內容未來施行及受益對象為全體國民，尚無涉性別。</td></tr>
<tr><td>（三）參與時機及方式之合宜性</td><td>合宜</td></tr>
<tr><td colspan="2">本人同意恪遵保密義務，未經部會同意不得逕自對外公開所評估之法案。
（簽章，簽名或打字皆可）<u>　　莊喬汝　　</u></td></tr>
</table>

陸、徵詢及協商程序之附表

重要事項	有無爭議	相關條文	相關機關（構）、團體或人員之主要意見	參採與否及其理由（含國際參考案例）
1.明定本法主管機關及各機關權責	■有 □無	§2、§5、§8、§15 §16	1.新設本部為主管機關，是否仍需維持「中央目的事業主管機關」雙軌管理？ 2.資安署(三級機關)可對一、二級公務機關辦理資通安全稽核相關作業，是否符合相關業務之上下權責劃分、組職職掌及地方自治等事宜？ 3.地方公務機關之資通安全管理事項，須地方投注資源、人力，可能涉及中央或地方權限爭議。	1.本法係以分層監督管理概念，由上級機關透過對所屬機關之資通安全稽核及後續改善情形之追蹤，掌握所屬機關之資通安全防護落實程度。復由資安署依機關層級、資通安全責任等級及業務屬性，擇重要機關辦理稽核。 2.修正草案將本法所管相關事項區分為主管機關及執行機關權責，由主管機關負責政策、制度或法規之擬訂；執行機關則係辦理技術性、專業性等業務事項；稽核相關業務涉及本法執行機關對該法納管對象之監督與協助，維持由資安署辦理。 3.有關地方公務機關之資通安全管理可能涉及中央或地方權限之憲法爭議，為避免爭議，爰強化相關規範，於修正條文第十五條第二項明定就資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之，以釐明中央與地方之權限。
2.增訂公務機關及特	■有	§11	1.提出查詢方式、採購疑義	1.將「各機關對危害國家

定非公務機關對於危害國家資通安全產品有關下載、安裝或使用之相關規範	□無	§27	等問題。 2.特定非公務機關亦應適用危害國家資通安全產品之相關規定。	資通安全產品限制使用原則」規範意旨，提升至本法定明相關辦理依據，以利公務機關實務執行。立法目的並非公告禁止生產，僅係禁止使用，且將可提供公務機關查詢，並採取情資分享方式處理。 2.因本條並非就採購面加以管制，如遇採購時尚非危害國家資通安全產品，採購後使用過程中風險升高，甚至已成為危害國家資通安全產品時，建議機關應盡量避免使用，如無法避免使用，則應透過控制措施進行妥善之風險管理。 3.有關外界建議特定非公務機關亦應適用危害國家資通安全產品之規定，已參採增訂於修正條文第二十七條，中央目的事業主管機關對特定非公務機關下載、安裝或使用危害國家資通安全產品，得予以限制或禁止；對於特定非公務機關自行或委外營運，提供公眾活動或使用之場地，基於維護資通安全有必要者，亦同。
3.增訂資通安全專職人員、強化資通安全人員之專業知能及重大資通安全事	■有 □無	§3 §18 §19 §20	1.設置專職人員的必要性，以及為何不能用專責人員處理資通安全業務？	1.資通安全風險升溫，為落實資通安全防護作業並能及時應處，避免其他業務排擠資通

件之調度支援等規定		§21	2.多數意見認資安署得逕予調度支援，與人員及其所屬機關無協商機制，擴權並排擠機關業務。	安全業務量能造成事件擴散，且資通安全專職人員制度執行已逾 5 年，各機關多可配合，為利部分機關資訊單位可依法設置所需人力，故修法明定配置資通安全專職人員確有其必要性。 2.另資通安全責任等級 C 級者，須設置專職人員 1 人。惟倘上級機關適當將系統向上集中，除利資通安全統籌強化外，已完成系統向上集中之 C 級機關更可調降資通安全責任等級，而可免設置專職人員。 3.資通安全為聯防概念，期望透過以戰代訓累積資通安全人員應處之能力。條文所示「調度支援」僅限重大資通安全事件，經彙整各界意見，已刪除「逕予」一詞，以杜外界疑慮，屆時按條文規定為調度時，仍會審酌受調度人員及機關之意願。 4.條文立法目的非為長期借調人力，雖無法預知重大資通安全事件之規模及處理時程，但旨在僅供暫時性調度支援之依據。
4.增訂中央目的事業主管機關對特定非公務機關重大資通安全事件之調查權限	■有 □無	§25 §31	為強化重大資通安全事件應處，中央目的事業主管機關必要時得調查相當事項，受調查者不得規避、妨害或拒絕：與會者認為	有關中央目的事業主管機關辦理特定非公務機關發生重大資通安全事件之調查，為確保隱私權及營業秘密之維護，

			應加強執行調查人員之適任性查核，以確保隱私權及營業秘密之保護。	已於修正條文第二十五條第五項明定受委任或委託機關（構）之保密義務，避免特定非公務機關之秘密，因重大資通安全事件之調查而洩漏。
5.涉及個人資料保護事件，應另依個人資料保護法及其相關法令辦理	□有 ■無	§33	資通安全管理法跟個人資料保護之相關要如何競合，各機關如何配合，如何符合規定，為何不整合？	1.考量二法規保護法益、規制對象、規制方式等皆不相同，國際趨勢亦區分不同法規及主管機關，例如歐盟個人隱私保護以GDPR，資通安全以NIST分別規範。本法的管理架構係以公務機關及特定非公務機關為分類；在特定非公務機關，是否納管之考量因素在於特定非公務機關因維運或提供之服務，對國家安全、民眾生活、經濟活動等有重大影響，因此透過本法管理機制，協助強化這些特定非公務機關資通安全管理措施。 2.個人資料保護法於112年5月31日修正，對民間企業個資外洩事件裁罰方式及額度提高至新臺幣1,500萬，另該法的主管機關個人資料保護委員會已經設立籌備處，將專責個資隱私保護管理，資通安全事件一旦涉及個資外洩將另依個人資料保護法辦理。

註：為茲簡明，「相關條文」欄位中，各條、項、款、目等，分以下列方式表達：條→§（條號以

阿拉伯數字表達）、項→Ⅰ（羅馬符號）、款→(1)（括弧內置阿拉伯數字）、目→（圓圈內置阿拉伯數字），目以下則以「之○（阿拉伯數字）」表達。