　　　　　　　　　　　　　　　　　　　　　　　　　　　　　議案編號：202110047780000

立法院議案關係文書

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 院總第20號 | 委員 | 提案第 | 11004778 | 號 |  |  |

案由：本院委員蔡其昌、陳冠廷、吳秉叡、蘇巧慧等18人，鑒於網路攻擊無遠弗屆，近年無論是公務機關或民間企業，其資通安全受到危脅的情況日益嚴重且逐年增加，為確保國家安全、維護社會公益，以及預防過多資安事件影響經濟發展之穩定性，爰擬具「資通安全管理法部分條文修正草案」，就民間企業方面，要求政府應提供資源，協助民間處理、因應及防範資通安全威脅事件；就公務機關方面，強化各機關委外辦理資通訊系統之監督機制、限制公務機關與特定非公務機關下載、安裝或使用危害國家資通安全產品。是否有當？敬請公決。

說明：鑒於網路攻擊無遠弗屆，不僅是政府機關受駭客攻擊會對社會造成衝擊，民間企業的資安事件對大眾的影響亦不容小覷，為確保國家安全、維護社會公益，以及預防過多資安事件影響經濟發展之穩定性，擬具「資通安全管理法部分條文修正草案」，各修正條文說明如下：

一、修正本法之主管機關為數位發展部。（修正條文第二條）

二、明定政府應提供資源，協助民間處理、因應及防範資通安全威脅事件。（修正條文第四條）

資訊化時代資通安全管理已成為公司營運的重要議題，不僅和大眾權益相關，亦對經濟穩定度造成影響，是以金融監督管理委員會（以下簡稱：金管會）早在三年前（民國110年）修正《公開發行公司年報應行記載事項準則》要求公司公布重大資訊安全事件之影響和公司之因應措施，且根據金管會統計，企業資安事件有增加的趨勢，111年上市公司僅有5家發生重大資安事件，112年卻大增至14家，而今（113）年才到2月底，就有6家。金管會（證期局）雖有資安聯防機制，也就是將上市櫃公司依風險等級分期加入台灣電腦網路危機處理暨協調中心（TWCERT/CC）的共享資安情資聯防機制，而根據金管會調查，符合風險等級的目標群共有1,567家，目前僅722家加入，未加入的有845家。又查，民間資安事件受害的產業相當廣泛，不僅是科技業、電子零組件，即便是藥局、汽車、自行車、觀光、化學、塑膠、生技都難以倖免。並且駭客攻擊的目標也不限於大企業，中、小企業也逐漸傳出災情，這些中小企業的資安水準存在一定的落差，相較於大企業，駭客反而無需使用更複雜的手法，但中、小企業卻將因此疲於奔命，營運受影響。鑒於我國超過九成屬於中小企業，其經營良窳和整體社會經濟能否穩定發展息息相關，爰此，新增規定要求政府應提供資源，協助民間處理、因應及防範資通安全威脅事件。

三、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。（修正條文第九條）

公務機關或特定非公務機關委外辦理資通訊系統者，需簽訂書面契約，要求受託者建立有效的資通安全管理機制，並加以監督。主管機關（數位發展部）則應訂定該書面契約範本供參，以確保國家資通訊安全。

四、增訂公務機關和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。（增訂第十條之一、第十條之二及第十八條之一）

為維護國家安全和公共利益，禁止及限制公務機關和特定非公務機關下載、安裝或使用危害國家資通安全產品；公務人員獲配之公務用資通訊設備，亦不得下載、安裝或使用危害國家資通安全產品；主管機關應會商有關機關擬訂關於危害國家資通安全產品等相關規定。此外，由於國內曾發生公共場域傳播設備遭駭客入侵，意圖以竄改網站內容、散播不實訊息等手段，達到認知作戰目的，調查發現是承包政府採購的廠商使用的軟體有問題，為避免公共看板遭駭客入侵，用假訊息造成社會混亂，修正條文亦要求公務機關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，也不得下載、安裝或使用危害國家資通安全產品。

提案人：蔡其昌　　陳冠廷　　吳秉叡　　蘇巧慧

連署人：陳秀寳　　陳俊宇　　李坤城　　王美惠　　邱議瑩　　羅美玲　　李柏毅　　沈發惠　　陳素月　　徐富癸　　黃　捷　　王正旭　　林月琴　　蔡易餘

|  |  |  |
| --- | --- | --- |
| 資通安全管理法部分條文修正草案對照表 | | |
| 修正條文 | 現行條文 | 說明 |
| 第二條　本法之主管機關為數位發展部。 | 第二條　本法之主管機關為行政院。 | 數位發展部業於民國111年8月27日成立，確保國家資通訊安全乃數位發展部之法定任務之一，配合行政院數位發展部成立，修正本條文文字，本法主管機關為數位發展部。 |
| 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。  五、協助民間處理、因應及防範資通安全事件。  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。 | 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、增訂第一項第五款，要求政府應提供資源，協助民間處理、因應及防範資通安全事件，蓋根據最新報導，臺灣企業資安事故有增加的趨勢，單以今（2024）年上市櫃公司的狀況來看，一至二月的資安事件重大訊息就有9件，平均每月4.5件；去（2023）年則有23件（遭網路攻擊資安事故17件、其他與資安相關的事件6件），平均每月近1.9件。受害的產業相當廣泛，不僅是科技業、電子零組件，即便是藥局、汽車、自行車、觀光、化學、塑膠、生技都難以倖免。並且駭客攻擊的目標也不限於大企業，中、小企業也逐漸傳出災情，這些中小企業的資安水準存在一定的落差，相較於大企業，駭客反而無需使用更複雜的手法，但中、小企業卻將因此疲於奔命，營運受影響。鑒於我國超過九成屬於中小企業，其經營良窳和整體社會經濟能否穩定發展息息相關，爰此，新增規定要求政府應提供資源，協助民間處理、因應及防範資通安全威脅事件。  二、第二項未修正。 |
| 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，及要求受託者建立有效之資通安全管理機制；公務機關或特定非公務機關並應監督該機制之實施。  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。  為確保國家資通訊安全，主管機關應訂定前項書面契約範本供參。 | 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。 | 一、修正第一項文字：為強化對受託者之資通安全管理要求，修正第一項文字，委託機關應要求受託者建立有效的資通安全管理機制，並加以監督該機制實施之效能。  二、新增第二項：為促使受託廠商加強資安風險管理，新增第二項規定，機關辦理資訊系統委外業務應訂立書面契約，明定權利義務和違約責任，藉由契約控管機關委外服務的資安風險。  三、新增第三項：鑒於數位發展部下設資通安全署，主責全國資安政策之統合管理，執行資安防護和演練作業，具有相當資安防護風險專業，爰此為確保國家資通訊安全，新增本項要求主管機關主管機關應就機關之資訊系統委外契約訂定範本，提供全國公務機關或本法所稱特定非公務機關參考之。 |
| 第十條之一　公務機關、軍事機關及情報機關不得下載、安裝或使用危害國家資通安全產品；但公務機關因業務需求且無其他替代方案，經該機關資通安全長及第十二條上級或監督機關資通安全長核可，且經主管機關核定，得以專案方式使用。主管機關亦應列冊管理之。  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。  前二項所稱危害國家資通安全產品，其審查程序、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。 |  | 一、本條新增。  二、鑒於本法第二條第五款就公務機關定義，係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，據此，第一項明定公務機關、軍事機關及情報機關均不得下載、安裝或使用危害國家資通安全產品。另外，考量危害國家資通安全，有直接及間接造成危害風險；而資安攻擊亦有對核心系統與非核心系統的危害，風險高低不一，不宜硬性全面至禁止之，故有但書規定，公務機關有業務需求且無其他替代方案的情況下，應取得該機關的資安長和資安上級（監督）機關的資安長核可，以及主管機關核定，則可採專案的方式使用。  三、第二項明定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。  四、第三項明定危害國家資通安全產品的其審查程序、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。又「反滲透法」第二條滲透來源的實質控制者所提供或產生的產品亦屬危害國家資通安全產品，併此敘明。 |
| 第十條之二　前條第一項公務機關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適用之。 |  | 一、本條新增。  二、由於國內曾發生公共場域傳播設備遭駭客入侵，意圖以竄改網站內容、散播不實訊息等手段，達到認知作戰目的，調查發現是承包政府採購的廠商使用的軟體有問題，為避免公共看板遭駭客入侵，用假訊息造成社會混亂，新增本條規定，明定公務機關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，不得下載、安裝或使用危害國家資通安全產品。 |
| 第十八條之一　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。 |  | 一、本條新增。  二、配合新增第十條之一和第十條之二的規定，關於特定非公務機關，本條明定中央目的事業主管機關可基於維護國家資通安全考量，得限制或禁止其下載、安裝或使用危害國家資通安全的產品。 |