監察院交通及採購委員會
111年度通案性案件調查研究報告

壹、題目:「政府機關推動資通安全防護之探討」通案性案件調查研究。

貳、結論與建議：

觀諸全球化資訊社會中，各國企業及政府機關為減少人力、物力、財力之投資，追求行政效能以實現便民、利民之目標，無不相繼採用電腦資訊化作業，致需面臨網路攻擊，財產或隱私的個人資料，成為網路駭客攻擊之重要目標，相關研究發現網路攻擊儼然已成另一種虛擬戰爭，影響範圍小至個人生活，大至國家安全層級；惟在便利、快速的前提下，如何防止國家機密外洩、網路犯罪以及不良言論散播，已經成為攸關國家安全之重要議題[1]，隨著越來越多服務須仰賴資通系統，資通安全相形重要，蔡英文總統於2020年就職時提出資安即國安2.0戰略[2]，然而，追溯我國資通安全推動歷程，自民國（下同）90年迄今，陸續推動6個階段、各為期4年之重大資通安全計畫或方案，目前依「國家資通安全發展方案（110年至113年）」，作為我國推動資安防護策略與計畫之依循目標，期間面臨法令更迭、制度資源、主管機關均有改善空間之問題，遂有數位發展部(下稱數位部)的成立與資通安全管理法（下稱資安法）的制定，負責推動我國數位政策的創新與變革，整合電信、資訊、資安、網路與傳播五大領域，為國內資通防護上無可忽視之重要創舉，以利我國資安法制政策之健全，完善我國

[1]資料來源：行政院國家資通安全會報，取自網址：https://moda.gov.tw/ACS/nicst/background/658。

[2] 資料來源：總統府（110），國家安全會議於110年9月發布「資安即國安2.0」戰略報告，以充實資安卓越人才（People）、強化人民家園安全防護及鞏固資安外交網路防禦（Protection）、促進產業繁榮發展（Prosperity）為三大推動目標；結合政府、民間與產業的力量，共同打造堅韌、安全、可信賴的智慧國家，取自網址：https://www.president.gov.tw/issue/439。

產業發展環境基礎。此外，一個國家中為維持國家安全、民生、經濟而提供的國家關鍵基礎建設（Critical Infrastructures，CI）[3]，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，下稱八大CI」。另為提升我國整體資訊安全防護，於各關鍵領域設立電腦緊急應變團隊（Computer Emergency Response Team，CERT）、資安資訊分享與分析中心（Information Sharing and Analysis Center，ISAC）及資訊安全監控中心（Security Operation Center，SOC），進行資安事件通報應變處理、資安情資分享以及網路威脅監控等重要資安業務，並建立跨領域之資安防護協防機制，最上層有國家層級National SOC、National CERT、National ISAC（下稱3N），成為國家資安聯防架構。

綜上，究我國資通安全防護現況與未來，政府與經營者面臨推陳出新的課題與挑戰，仍有待進一步觀察與探究，實有調查研究之必要，本院交通及採購委員會決議組成調查研究小組進行研究，期作為政府主管機關及經營者之參考。

本案經向數位部、資通安全署（下稱資安署）、數位產業署（下稱產業者）、國家資通安全研究院（下稱資安院）、國家通訊傳播委員會（下稱通傳會）、國家科學及技術委員會（下稱國科會）調閱相關資料，並於112年4月27日舉辦諮詢會議，邀請專家學者與會，提出相關諮詢意見。又為瞭解中央及地方政府辦理「資通安全防護」等現況情形，本院於112年2月至4月間擇日實地訪查臺南、高雄、臺中、新北、臺北等地區，訪查標的包含具

[3] 資安法第3條所指關鍵基礎設施：「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，經主管機關定期檢視並公告之領域」。

代表性八大CI（通訊傳播、水資源[4]、科學園區）及民間資安公司，並與相關機關（構）進行座談會，就整體實施成效、困境、國際比較及未來策略議題等進行交流，已完成之國內實地訪查之行程如下：

場次	日期	相關機關	訪查標的
1	112.02.02-112.02.03	數位部、國科會、財團法人國家實驗研究院、財團法人電信技術中心	1. 沙崙智慧綠能科學城（臺灣智駕測試實驗室、ACW SOUTH沙崙資安應用多元展區、資安院沙崙院區、資安防護及培訓場域、ACW SOUTH資安共創空間、TTA南部據點）。 2. 財團法人電信技術中心。
2	112.03.09-112.03.10	經濟部水利署、數位部、通傳會、國科會、財團法人國家實驗研究院	1. 中水局石岡壩管理中心。 2. 國科會中科管理局。 3. 大肚山電波監測站。
3	112.04.21	資安新創公司、數位部	1. 資安新創公司。 2. 國家層級資安聯防體系（N-ISAC、N-CERT、N-SOC）。

日期格式：年.月.日

資料來源：本調查研究自行整理。

此外，為參考國外資通安全防護經驗，本案調查研究委員於112年3月24日至4月4日赴以色列考察相關資安防護之經驗與成果，期間關懷駐地概況並聽取業務簡報外，並陸續參訪政府部門、科技園區、資安公司，並參加國際創新資安科技會議，除資安議題外，亦對人權教育、水資源議題進行深入瞭解。繼之，本案經綜整國內外實地訪查及座談所發掘之問題，再於112年5月3日與數位部、資安院、通傳會到院座談說明，就本案調卷內容

[4] 行政院資通安全處「強化國家資安基礎建設計畫」(108)，計畫期程：107年1月至109年12月，該計畫指出略以，該計畫優先完成能源、通訊傳播領域之資安 防護建置，目標如下：強化水資源關鍵資訊基礎設施之資安防護，防範水資源領域免於遭受駭客入侵攻擊。2.建構通傳業者之資通訊安全防護機制，強化我國數位匯流及網路資通訊安全，打造數位國家・創新經濟發展方案之「數位創新基礎環境」。此計畫已執行完畢，爰優先擇定八大CI之通訊與水資源作為訪查標的。

及現行資通安全防護執行成果、國內外實地訪查(考察)發現之問題及未來策進作為等相關議題交換意見，並經前揭機關現場說明及補充資料，茲將本研究所得相關結論與建議臚列如后：

一、資通安全管理法於107年6月6日制定公布，行政院為該法之主管機關，然於111年8月24日以院函公告調整權責事項，自同年月27日起變更資安法及相關法規之管轄機關為數位部，衍生主管機關定位不明、權責不清，實際稽核與檢查亦無明確法律授權，存有模糊地帶，在執行上面臨諸多挑戰，行政院允宜正視目前所遇所遇困難，並督促數位部及相關機關儘速提出法律修正案，使法規具體明確授權，以符實際並據以執行

(一)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，此為資安法第1條所揭櫫之立法目的。同法第3條將「資通系統、資通服務、資通安全、資通安全事件、公務機關、特定非公務機關、關鍵基礎設施、關鍵基礎設施提供者，以及政府捐助之財團法人」等九類名詞予以定義[5]。再依同法第2條規定，「本法之主管機關為行政院」。準此，行政院為該法主管機關，並無疑義。

[5] **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。

(二)經查，對於我國關鍵基礎設施之防護體系，可分為實體和資通安全兩層面的保護，前者由行政院國土安全政策會報、國土安全辦公室統籌，後者由行政院資通安全會報、數位部資通安全署負責。由於關鍵基礎設施之防護牽涉到不同層級、不同單位，甚至橫跨公、私部門，且關鍵基礎設施有其相依性[6]，可能牽一髮動全身。勢必得強調跨部門的合作以及資訊共享，才能及時做出應變處理，故資通安全體系的完善，重要性日益增長[7]。相關演變歷程從行政院102年3月8日設立資通安全辦公室，105年8月1日正式設立資通安全處，於107年6月6日公布資安法，並於108年1月1日施行，統整國家資通安全機制，將國家整體資安工作正式法制化，此法係屬我國重要法律改革，讓政府落實國家資安防護策略的同時，也為我國資安產業帶來嶄新的營運商機，行政院因應數位部於111年8月27日成立，早於前3日（即111年8月24日）以院臺規字第1110184307號公告部分條文列屬「行政院」之權責事項，自111年8月27日起改由「數位部」管轄。顯見從行政院設立資通安全辦公室至數位部起迄期間，面臨法令更迭、制度資源、主管機關均有改善空間之問題，遂有數位部的成立與資安法的出現，負責推動我國數位政策的創新與變革。

(三)然而，資安法主管機關自111年8月27日起已公告變更為「數位部」，除部分事項仍由「行政院」管轄外，其餘資安法主管機關應辦理事項，均改由「數位部」

[6] 行政院，國家關鍵基礎設施安全防護指導綱要，相依性所指：「是關鍵基礎設施之間的一種關係，彼此相互依賴、互相產生作用，如某設施核心功能失效，將產生連鎖反應，造成其他設施無法運作。」

[7] 資料來源：李峙錡（111），關鍵基礎設施的主管機關與權限調整，取自網址：https://ai.iias.sinica.edu.tw/critical-infra-authority/#easy-footnote-bottom-22-6784。

管轄，兩機關資安業務與管轄事項說明如下[8]：

1、第2條、第5條第1項、第6條第1項、第7條、第8條、第12條、第14條第2項、第3項、第4項、第15條第2項、第18條第3項、第4項、第5項、第19條第2項、第20條第3款、第5款、第22條所列屬「行政院」之權責事項，自111年8月27日起改由「數位部」管轄。

2、第3條第7款、第8款、第4條第2項、第16條第1項、第6項、第17條第4項、第23條所列屬「行政院」之權責事項，自111年8月27日起仍由「行政院」管轄。

(四)另依資安法第13條第1項、第16條第4項明文規定：「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」、「中央目的事業主管機關**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」，即表示各部會對其所屬或特定非公務機關，負有稽核、監督之責。是以，數位部成立前，係由原本的行政院資通安全處統禦資通安全事項，行政院轄下所有部會皆為其所屬，可依資安法第13條規定進行稽核，惟數位部成立後，不論該部或所屬資安署，與內政部、交通部、經濟部……等，均為平行機關，互不隸屬，於現行法律規定下，是否仍有稽核權力，顯有疑義。甚且，國內所有不論公、私部門發生駭客攻擊、個資外洩、電子看板入侵等情事，皆找上數位部或資安署負責、解決或詢問如何防護，現行法制架構下，衍生主管機關定位不明，存有模糊地帶。

(五)其次，關鍵基礎設施的保護，已逐漸成為各國所重

[8] 行政院於111年8月24日以院臺規字第1110184307號公告。

視議題，攸關國家安全、政府運作、人民生活、經濟發展與永續生活，依據行政院103年12月23日頒布之「國家關鍵基礎設施防護指導綱要」，我國關鍵基礎設施（Critical Infrastructure，CI）依功能屬性區分為八大領域：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及高科技園區（詳下圖）。關鍵基礎設施之資安防護，則納為關鍵基礎設施提供者資安法法遵事項，前揭八大關鍵基礎設施，係為行政院於103年12月29日函頒之「國家關鍵基礎設施安全防護指導綱要」內所明定，未見於資安法之授權，就此議題，本院諮詢學者亦表示：「八大CI無法源依據，且其無具體定義，需與時俱進滾動式檢討」等語。況該法主管機關為行政院，故八大關鍵基礎設施以外，行政院與數位部之權責未盡明確，亦應釐清管轄範圍，實有討論的空間。

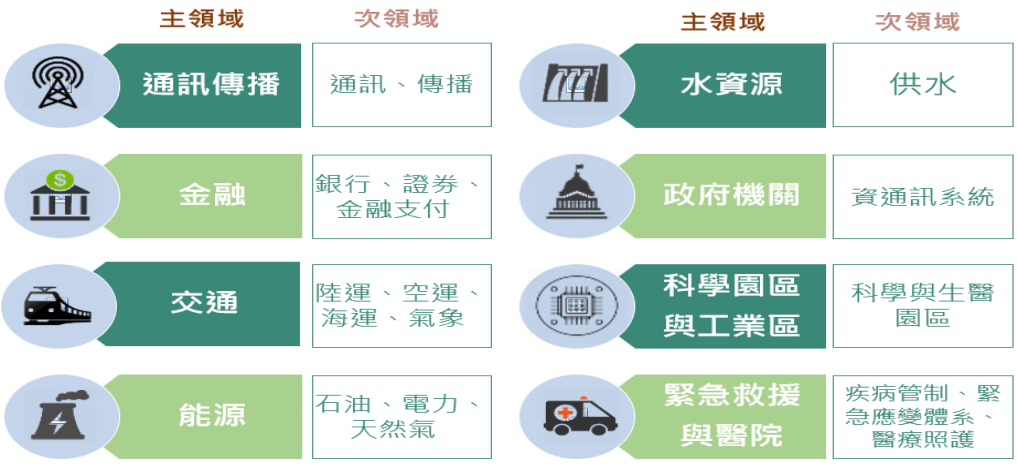

圖1　資安法所納管之關鍵基礎設施提供者

資料來源：112.3.9資安署簡報資料。

(六)綜上，資通安全管理法於107年6月6日制定公布，行政院為該法之主管機關，然於111年8月24日以院函公告調整權責事項，自同年月27日起變更資安法及相關法規之管轄機關為數位部，衍生主管機關定位

不明、權責不清，實際稽核與檢查亦無明確法律授權，存有模糊地帶，在執行上面臨諸多挑戰，行政院允宜正視目前所遇所遇困難，並督促數位部及相關機關儘速提出法律修正案，使法規具體明確授權，以符實際並據以執行。

二、八大關鍵基礎設施於107年至109年間，藉由強化國家資安基礎建設計畫，陸續完成各領域之ISAC、CERT、SOC，進行資安事件通報應變處理、資安情資分享及網路威脅監控等重要資安業務，建立跨領域之前、中、後資安防護協防機制，相關主管機關宜持續強化資安防護，定期辦理資安稽核與演練，驗證資安防護能力與應變韌性，以有效因應資通安全事件，期達成國家關鍵基礎設施安全防護目標，確保八大關鍵基礎設施正常運作

(一)關鍵基礎設設保護之法源與分類，依資安法第3條第7款、第8款，關鍵基礎設施乃指係指「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，經主管機關定期檢視並公告之領域」；關鍵基礎設施提供者則為「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」。另依同法第16條第1項規定：「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」，再依關鍵基礎設施盤點作業須知規定，具體關鍵基礎設施之篩選準則為：「基礎設施遭攻擊或災損時，有造成如下影響者，應列為關鍵基礎設施」：

（1）足以直接或間接造成大規模人口傷亡或避難遷徙者。

（2）足以直接或間接造成重大經濟損失者。

（3）足以直接或間接影響其他關鍵基礎設施營運之能力者。

（4）足以影響政府功能持續運作、民心士氣、社會安定者。

2、依據八大關鍵基礎設施領域分類詳下表，包含主領域與次領域：

主領域（8）		次領域（20）		
名稱	協調機關	名稱	重要業務功能	主管機關
能源	經濟部	電力	穩定提供發電、輸電、配電、調度、監控等供電服務之重要設施或系統。	**經濟部**
		石油	穩定供應油品，及帶動石化相關工業發展之重要設施或系統。	**經濟部**
		天然氣	提供輸儲、接收、遮斷等設備，穩定供應天然氣之重要設施及控制系統。	**經濟部**
水資源	經濟部	供水	提供質佳、量足、穩定供水之水源、水庫、淨水、供水、水質保護等重要設施或系統。	**經濟部**
通訊傳播	數位部	通訊	支持通訊服務之重要設施或系統，例如：市內/長途/國際通信、行動通信、衛星通信、國際海纜及數據通信等。	數位部
		傳播	支持傳播服務之重要設施或系統，例如：無線廣播電視及有線廣播電視。	數位部
交通	交通部	陸運	提供大眾陸上運輸服務之重要設施或系統，例如：公路運輸系統、鐵路運輸系統(含一般鐵路、高速鐵路、大眾捷運)。	交通部
		海運	提供航運服務之重要設施或系統，例如：商港、工業港及漁港。	交通部 **經濟部** 農委會
		空運	提供航空營運管理及航空運輸關聯服務之重要設施或系統。	交通部
		氣象	提供氣象觀測、氣象預報、地震測報	交通部

主領域（8）		次領域（20）		
名稱	協調機關	名稱	重要業務功能	主管機關
			、海象測報及相關資訊發布等相關服務之重要設施或系統。	
金融	金融監督管理委員會	銀行	提供新臺幣跨行通匯資金調撥服務、ATM存提款、轉帳及餘額查詢等跨行交易服務之重要設施或系統。	金管會 交通部
		證券	執行全國證券、期貨市場交易及結算、交割之重要設施或系統。	金管會
		金融支付	支持我國貨幣及支付之重要設施或系統。	中央銀行
緊急救援與醫院	衛生福利部	醫療照護	提供醫療照護之重要系統及醫療院所。	衛福部
		疾病管制	提供傳染病疫情監測與預警、傳染病防治與應變、傳染病邊境檢疫，以及生物病原檢驗與技術研發等重要設施或系統。	
		緊急應變體系	災害或緊急應變中心、消防救災救護及政府指管等重要設施或系統。	內政部 海委會
政府機關	國土安全辦公室	機關場所與設施	支持政府核心業務運作及重要領導權與人員辦公之重要設施與場所。	中央政府機關
	數位部	資通訊系統	支持政府核心業務運作之重要資通訊系統。	
科學園區與工業區	國家科學及技術委員會	科學與生醫園區	科學園區、生物醫學園區等。	國科會
		軟體園區與工業區	軟體園區、工業區、科技工業區等。	**經濟部**

資料來源：本研究自行整理。

(二)所謂「資安即國安」是我國未來在達成數位國家發展目標的一項重要工作。為提升我國整體資訊安全防護，行政院國家資通安全會報因應我國資安威脅加劇，建構關鍵資訊基礎設施防護（Critical Information Infrastructure Protection，CIIP），於各關鍵領域設立電腦緊急應變團隊（Computer Emergency Response Team，CERT）、資安資訊分享

與分析中心（Information Sharing and Analysis Center，ISAC）及資訊安全監控中心（Security Operation Center，SOC），進行資安事件[9]通報應變處理、資安情資分享以及網路威脅監控等重要資安業務，並建立跨領域之資安防護協防機制。查上開八大關鍵基礎設施於107年至109年間，藉由強化國家資安基礎建設計畫，陸續完成各領域之ISAC、CERT、SOC相關建置工作，進而掌握網際網路接取服務之資安事件及垃圾郵件情資，並建立與國內及國際相關組織之資安情資分享機制，強化八大領域之資安防護能力，提升通報、應變及處置能力，建構資安聯防機制與推動國家級跨域資安聯防體系。

(三)然而，八大關鍵基礎設施的存在性，乃係一個國家為維持國家安全、民生、經濟而提供的基本產品或服務，包含維持國家最起碼的經濟、民生、政府運作與國家安全息息相關的實體和以資訊電子為基礎的運作系統[10]。是以，八大關鍵基礎設施應屬高度監理，給予所屬資安指引，數位部或資安署發布相關法遵事項，八大CI應轉換自身相對應、適合方式之規範，令頒轉下遵循，並持續完善關鍵基礎設施防禦體系，降低遭遇網路攻擊之風險，例如：經濟部同時肩負政府機關水利署提供的水資源關鍵基礎設施之管理，亦包括油、水、電等民間能源業者之管理，以及掌管陸運、海運、空運、氣象之交通部皆為不可或缺的角色，其他另有數位部、農委會、

[9] 資安法所稱資安事件：「通安全事件：指系統、服務或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」。

[10] 資安法第3條所指關鍵基礎設施：「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，經主管機關定期檢視並公告之領域」。

金管會、中央銀行、衛福部、內政部、海委會、國科會等各司其職。另參據本院諮詢學者、出國考察報告[11]對於八大CI資安演練與防護指出：「目前八大CI的資安防護，除有實質國安考量外，輔以主管機關法規要求，需加強稽核及演練作為」、「各種兵棋演練都要有場域，讓攻擊者與防衛者都能有操練的空間，資安攻防演練自不例外，以往我們大多只能在營運中的系統演練，惟又顧及系統事後能否順利恢復營運，演練情境的設定總有保留，也造成演練效果被打折」，以及數位部亦表示略以：「資安署後續在稽核八大CI時，會詢問該機關是否採用複合情形進行演練」、「為求演練真實性，資安署會尋找各類型攻擊手進行實兵演練」。是以，相關主管機關宜持續強化資安防護，定期辦理各領域資安稽核與資安事件攻防演練，立求實兵演練，以提升CI領域進行攻防演練之真實性及有效性。

(四)綜上，八大關鍵基礎設施於107年至109年間，藉由強化國家資安基礎建設計畫，陸續完成各領域之ISAC、CERT、SOC，進行資安事件通報應變處理、資安情資分享及網路威脅監控等重要資安業務，建立跨領域之前、中、後資安防護協防機制，相關主管機關宜持續強化資安防護，定期辦理資安稽核與演練，驗證資安防護能力與應變韌性，以有效因應資通安全事件，期達成國家關鍵基礎設施安全防護目標，確保八大關鍵基礎設施正常運作。

三、因應資通訊科技發展及資安威脅趨勢，先進國家已將

[11] 資料來源：2018年以色列國土安全暨資安大會，服務機關：財政部財政資料中心，出國期間：107年11月10日至11月17日，報告日期：108年2月15日。

「資安管理」提升至「資安治理」層次，除內部資通安全稽核與資安演練，資安成熟度自評亦屬重要的概念，數位部允宜參照行政院核定之第六期國家資通安全發展方案(110年至113年)，持續辦理政府機關與關鍵基礎設施提供者資安治理成熟度之評估作業，俾使所有A級政府機關確實達到成熟度3級以上，並逐步推行至B級政府機關，以健全政府部門資通安全之機制

(一)資通安全責任等級分級辦法第4條、第5條規定：「各機關有下列情形之一者，其**資通安全責任等級為A級**：一、業務涉及國家機密。二、業務涉及外交、國防或國土安全事項。三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。四、業務涉及全國性民眾或公務員個人資料檔案之持有。五、屬公務機關，且業務涉及全國性之關鍵基礎設施事項。六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。七、屬公立醫學中心。」、「各機關有下列情形之一者，其**資通安全責任等級為B級**：一、業務涉及公務機關捐助、資助或研發之國家核心科技資訊之安全維護及管理。二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。三、業務涉及區域性或地區性民眾個人資料檔案之持有。四、業務涉及中央二級機關及所屬各級機關（構）共用性資通系統之維運。五、屬公務機關，且業務涉及區域性或地區性之關鍵基礎設施事項。六、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵

基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。七、屬公立區域醫院或地區醫院」。因應資通訊科技發展及資安威脅趨勢，先進國家已將「資安管理」提升至「資安治理」層次，資安風險為組織重要風險之一，資安目標亦為組織重要目標之一，管理高層加強對於資安防護工作之重視，同時亦反映在組織資安相關人力與經費等資源之投入，以降低資安風險[12]，過去推動落實資安，導入資訊安全管理制度已是常見的作法，除內部資通安全稽核、相關資安演練，資安成熟度自評也是重要的概念。是以，為衡量我國政府機關之防禦能力及治理成效，於第五期國家資通發展方案（106年至109年）[13]積極推動政府機關資安治理成熟度，並於資安法子法「資通安全責任等級分級辦法」之應辦事項，**明定資通安全責任等級A級與B級[14]之公務機關，每年應辦理1次資安治理成熟度評估作業**。

(二)另參行政院[15]核定之第六期國家資通發展方案（110年至113年）[16]，**現有資安治理成熟度評估方式**係於資安治理之「**策略面**」、「**管理面**」及「**技術面**」三大面向設計對應之檢核項目，包含政策與組織管理

[12] 吳啟文、林晶瑩，政府機關資安治理成熟度評估機制，國土及公共治理學刊，第7卷第4期，108年12月。

[13] 資料來源：數位部資通安全署，國家資通安全發展方案（106年至109年），取自網址：chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www-api.moda.gov.tw/File/Get/acs/zh-tw/cYa9VkznxWRvmqR。

[14] 依據「資通安全責任等級分級辦法」第2條規定，公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。有關5級的要件可參照同法第4條至第8條的規定。

[15] 行政院111年2月23日院臺護字第1110165094號函。

[16] 數位部資通安全署，國家資通安全發展方案（110年至113年），取自網址：https://moda.gov.tw/ACS/operations/policies-and-regulations/648。

有效性、績效與成果監督落實性、資安事件管理與緊急應變有效性等指標問項，將評估後之能力度等級由低至高分為6級，分別為「Level 0 未執行流程（Incomplete Process）」、「Level 1 已執行流程（Performed Process）」、「Level 2 已管理流程（Managed Process）」、「Level 3 標準化流程（Established Process）」、「Level 4 可預測流程（ Predictable Process ）」及「Level 5 最佳化流程（Optimizing Process）」，成熟度等級與對應流程構面詳下圖。

圖2　建構OT資安治理機制

資料來源：112.3.9資安署簡報資料。

(三)復依前揭第六期國家資通發展方案指出，推動政府機關資安治理成熟度之分年里程碑KPI為：1.110年：建立政府機關資安治理成熟度客觀指標。2.111年：推動3個A級政府機關落實資安治理成熟度達第2級以上。3.112年：推動30個A級政府機關落實資安

治理成熟度達第2級以上。4.**113年：推動所有A級政府機關落實資安治理成熟度達第3級以上**。此外，為精進既有資訊科技領域(Information Technology)之資安治理成熟度，後續將加入客觀指標，例如蒐集監控數據、攻防演練成效等資訊，分析其防護等級真實性；另同步訂定OT資安治理成熟度評估機制相關標準文件，並試行導入至CI提供者。藉由上述資安治理成熟度衡量機制，於113年時，所有A級政府機關達資安治理成熟度(含客觀指標)第3級以上，期望我國資安防禦作為能達超前部署、制敵機先及溯源追蹤。基此，未來需持續精進及擴大推動資安治理成熟度評估，以加速建構我國資通安全環境。

(四)綜上，因應資通訊科技發展及資安威脅趨勢，先進國家已將「資安管理」提升至「資安治理」層次，除內部資通安全稽核與資安演練，資安成熟度自評亦屬重要的概念，數位部允宜參照行政院核定之第六期國家資通安全發展方案(110年至113年)，持續辦理政府機關與關鍵基礎設施提供者資安治理成熟度之評估作業，俾使所有A級政府機關確實達到成熟度3級以上，並逐步推行至B級政府機關，以健全政府部門資通安全之機制。

四、我國建立國家層級資安聯防體系，包含N-ISAC、N-CERT、N-SOC，以因應資安挑戰與威脅；從111年八大關鍵基礎設施等各領域與N-ISAC情資分享情形可知，向下情資交流達77萬餘筆，惟向上分享情資僅有612筆，形成情資「不公開化、不透明化」，存在諸多黑數，宜鼓勵勇於發布訊息並揭露策進作為，避免「盡量不通報、家醜不外揚」之情事發生，持續蒐整國際資安情資分享並與國際資安組織交流合作，發揮各領域間

去識別化後的情資功能，降低資安事件之風險

(一)因應資安挑戰與威脅，我國資安聯防體系的建立，必須建立在高效率的自動化資安情資分享機制之上，而情資蒐集與分享則必須要仰賴各單位分工合作並互信分享才能夠讓重大情資即時進行傳遞，有關國家層級資安聯防體系，包含N-ISAC、N-CERT、N-SOC（下稱3N），即各領域之ISAC、CERT、SOC（詳結論與建議二所述）再加上N，N代表National（即國家），分別說明如下：

1、N-SOC：國家資安聯防監控中心，提供事前資安威脅監控，跨領域資安聯防分析與回饋，與掌握國家整體資安現況及趨勢，目前N-SOC分析領域回傳情資，整體威脅主要以掃描刺探為主，其次為入侵攻擊，資安院分析政府網路資安威脅趨勢呈現上升，112年網路攻擊數量約每日498萬次，需發展主動掃描與早期預警機制，提升政府網路資安韌性。

2、N-CERT：國家資安通報應變中心，為促進各領域CERT聯防作業，針對重要資安事件適時提供協助，與掌握國家資安事件通報概況，N-CERT資安事件應變中心109年至111年共接獲2,650件資安事件通報，以中央及地方政府為主，而事件通報類型主要係非法入侵，通報等級以1級[17]資安事件為主。

3、N-ISAC：國家資安資訊分享與分析中心，為建構跨領域資安情資分析機制、蒐整國際資安情資，並促進各領域ISAC間的合作交流，包括八大關鍵

[17] 依據「國家資通安全通報應變作業綱要」規定，資安事件影響等級分為4個級別，由重至輕分別為「4級」、「3級」、「2級」與「1級」，1級事件為非核心業務資料遭洩漏、非核心業務系統或資料遭竄改、非核心業務運作遭影響或短暫停頓。

基礎設施、六都區域聯防中心、犯罪偵防單位，以及民間技術支援、監控服務等，即時分享資安情資，另亦有蒐整國際資安情資來源、與國際CERT、ISAC組織交流合作。

4、有關國家層級的ISAC、CERT、SOC與八大關鍵基礎設施之聯防體系，以及3N之功能角色與運作模式，詳下圖。

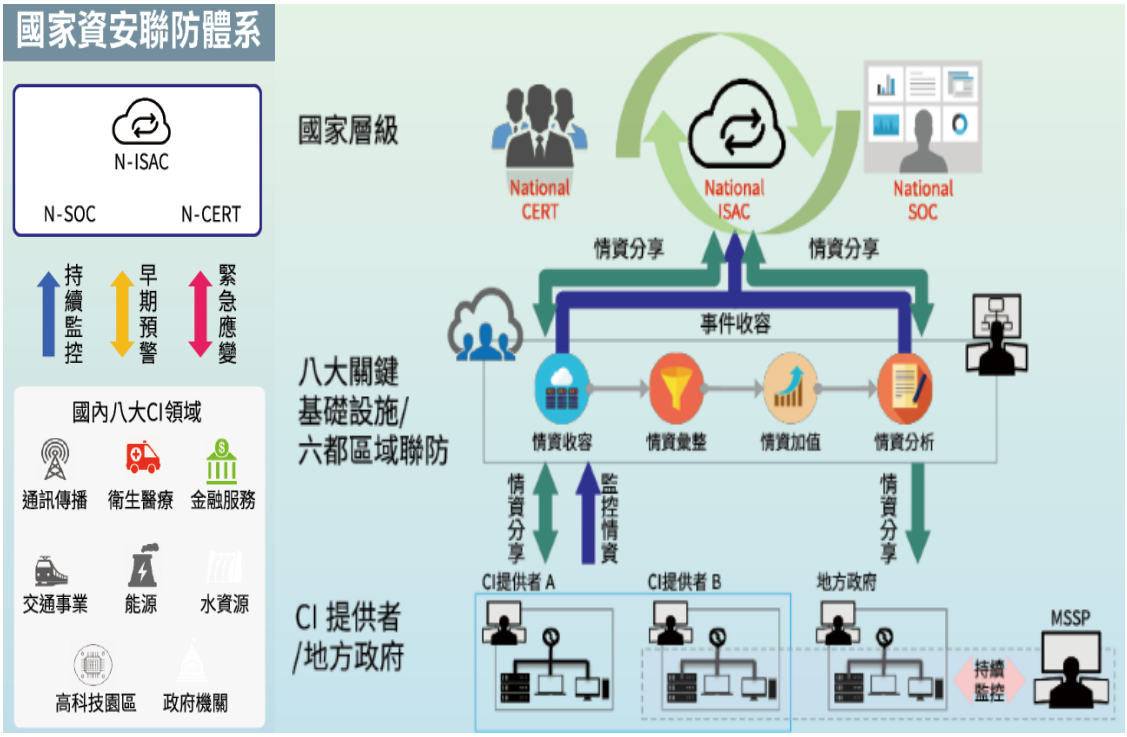

圖3　國家級資安聯防體系

資料來源：iThome，取自網址：https://www.ithome.com.tw/news/132220

圖4　3N事前威脅監控、事中通報應變、事後情資分享之功能角色
資料來源：112.4.21資安院簡報資料。

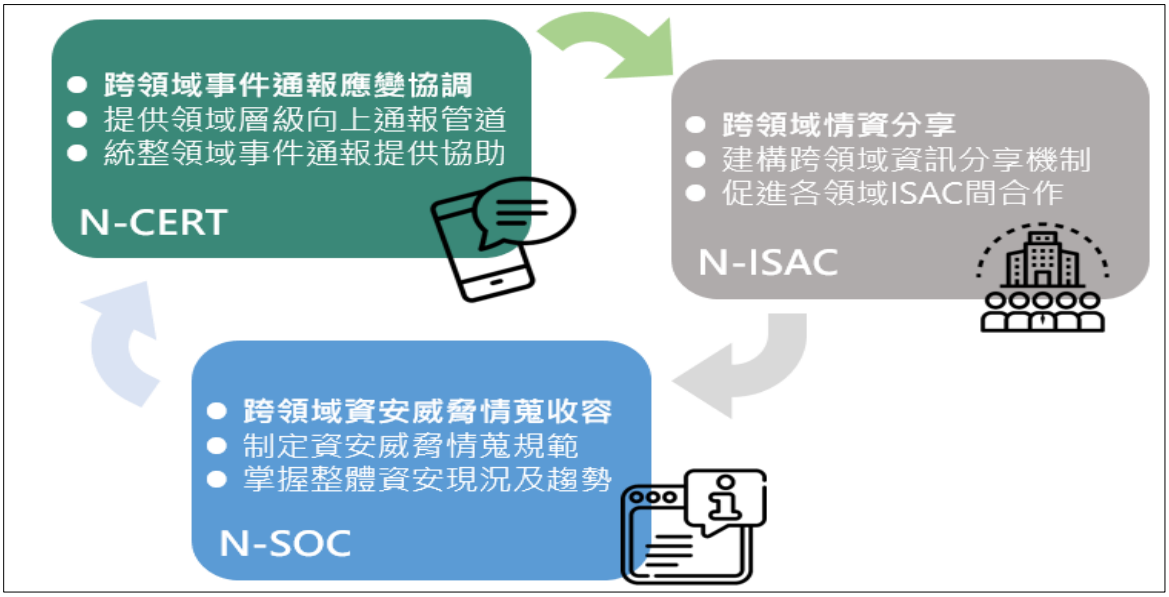

圖5　國家層級3N運作模式
資料來源：112.3.9資安署簡報資料。

(二)經查，第五期國家資通安全發展方案（106年至109年）[18]，已建置國家層級的ISAC、CERT、SOC，達到

[18] 數位部資通安全署，國家資通安全發展方案（106年至109年），取自網址：chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www-api.moda.gov.tw/File/Get/acs/

跨領域之情資分享、緊急應變及資安監控，強化縱向通報及橫向通知機制，以掌握國家整體資安風險，並即時分析資安事件樣態及駭侵手法，並部署主動式防禦機制，以建立跨域資安聯防機制，定期實施關鍵基礎設施跨領域相關演練。

(三)本院於112年4月21日赴國家資通安全研究院（基信院區）實地訪查，瞭解111年八大關鍵基礎設施等各領域與N-ISAC情資分享情形，發現向上分享情資與向下分享情資數量相差甚遠，茲就分別說明如下：

1、**向下**分享情資之數量：已達772,715筆，以資安預警情資為主，其次為資安訊息情資，統計109年至111年分享資安情資合計達2,298萬561筆[19]。

2、**向上**分享情資之數量：111年各領域合計僅有612筆訊息，包括資安防護報告、威脅阻擋清單及漏洞訊息等。

圖6　111年八大CI與N-ISAC情資分享情形一覽表

單位：筆；%

N-ISAC **↑向上** 八大CI				N-ISAC **↓向下** 八大CI
CI領域	**代碼**	**情資分享數**	**占比(%)**	**情資分享數**
金融	F-ISAC	241	39	【計772,715筆】 備註：資安預警情資為主（94.58%），其次為資安訊息情資(2.28%)。
高科技園區	SP-ISAC	102	17	
交通	T-ISAC	93	15	
教育	A-ISAC	71	12	
能源與水資源	E-ISAC	48	8	
緊急救援與醫院	H-ISAC	44	7	
通訊傳播	C-ISAC	13	2	
合計		**612**	100	

資料來源：據112.4.21資安院簡報資料自行繪製。

zh-tw/cYa9VkznxWRvmqR。

[19] 109年至111年情資總數分別為440,386、1,085,460、772,715。

(四)綜上，我國建立國家層級資安聯防體系，包含N-ISAC、N-CERT、N-SOC，以因應資安挑戰與威脅；從111年八大關鍵基礎設施等各領域與N-ISAC情資分享情形可知，向下情資交流達77萬餘筆，惟向上分享情資僅有612筆，形成情資「不公開化、不透明化」，存在諸多黑數，宜鼓勵勇於發布訊息並揭露策進作為，避免「盡量不通報、家醜不外揚」之情事發生，且持續與國際資安組織交流合作、蒐整國際資安情資分享，發揮各領域間去識別化後的情資交流，降低資安事件之風險。

五、政府零信任網路架構係參考美國國家標準暨技術研究院零信任架構，同時結合向上集中之防護需求；然政府機關推動資安零信任牽涉諸多面向與磨合，尚有努力的空間，數位部宜透過「身分鑑別、設備鑑別及信任推斷」3大核心機制，落實政府機關試行零信任網路，並藉由檢核清單，逐步擴大導入機關，透過可操作性之導入步驟，降低機關實施零信任網路之疑慮與負擔，逐步建立零信任網路資安防護環境

(一)零信任架構（Zero Trust Architecture，ZTA）備受資安圈與全球政府重視，縱觀全球，美國政府推動零信任網路安全戰略腳步最快，已經公告明確政策與時程表，他們要求聯邦機關要在西元2024年前完成初步遷移，也透過該國的國家資安卓越中心（NCCoE），推動商用產品符合NIST零信任架構[20]。我國同步跟進，參考第六期國家資通安全發展方案（110年至113年）[21]，於「善用智慧前瞻科技、主動

[20] 美國國家標準暨技術研究院（National Institute of Standards and Technology ，NIST），所發布的NIST零信任架構文件SP 800-207。

[21] 數位部資通安全署，國家資通安全發展方案（110年至113年），取自網址：https://moda.

抵禦潛在威脅」推動策略，亦明定發展零信任網路資安防護環境，評估並導入零信任網路(Zero Trust Network)，逐步試行以驗證其可行性，完善政府網際網路防禦深廣度。

(二)經查，美國國家標準技術研究所（National Institute of Standard and Technology，NIST）制定國家測量標準，乃於2014年2月發布資通安全架構（Cybersecurity Framework，CSF）1.0版，並於2018年4月發布修正後之1.1版，以利聯邦政府各機關或相關單位遵守。美國NIST之CSF架構係以識別（Identify）、保護（Protect）、偵測（Detect）、應變（Respond）、復原（Recover）五大功能進行區分。聯邦政府各機關及關鍵基礎設施等，搭配NIST之CSF架構與資通安全相關文件，據以規劃與建立資通安全管理制度。且因該架構亦能適用於一般企業，爰已逐漸成為其他國家或地區之企業或組織，就資通安全之風險管理的主要參考工具之一。

(三)我國政府零信任網路架構係參考美國NIST零信任架構，同時結合向上集中之防護需求，採取資源門戶之部署方式（Resource Portal-Based Deployment），包含身分鑑別、設備鑑別及信任推斷3大核心機制，詳下圖，其中身分鑑別為多因子身分鑑別與身分鑑別聲明、設備鑑別為設備鑑別與設備健康管理、信任推斷為使用者情境信任推斷機制。另，政府零信任網路架構採資源門戶之部署方式，「存取閘道」為機關資通系統之存取門戶，其依據決策引擎之存取決定，負責建立、監控及終止使用者與機關資通系統間之網路連線，不論來自內部或

gov.tw/ACS/operations/policies-and-regulations/648。

外部網路，均經由存取閘道進行存取，且透過反向代理技術，隱藏內部伺服器與機關資通系統之網路路徑，並實施負載平衡與防止阻斷服務攻擊之機制。

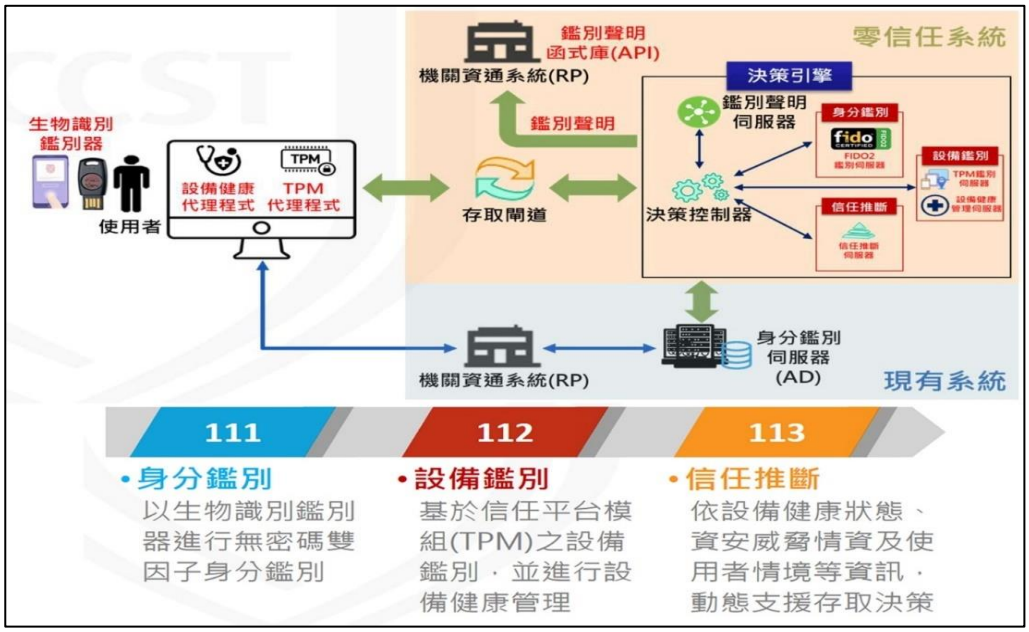

圖7　政府零信任網路架構

資料來源：NCCST，政府零信任網路說明簡報。

(四)然而，有關政府機關推動資安零信任架構之可行性與困難度，數位部、資安院、業者及諮詢學者分別表示意見臚列如下：

1、數位部與資安院表示:「為強化我國資安防護，建議推動重點包含主動防禦機制、推動零信任機制、資安人才培育、全民資安意識推廣及加強國際合作」、「導入零信任網路為逐步成熟之過程，非一次性大規模替換基礎架構與存取流程，欲推動零信任網路，身分鑑別為優先導入機制，藉由提供導入建議，協助政府機關實施零信任網路，強化資安防護能力」等語。

2、本院於112年4月21日與資安公司業者座談時，業者建議略以,「加速擁抱零信任，以利動態評估政

策與風險」、「加速A級機關導入零信任，且三階段（身分驗證/設備驗證/信任推斷）要一起搭配」。

3、本院諮詢學者提出看法如下：

（1）零信任架構政府可以做，不是光買產品就可以做到，其實是架構的改變，是需要有人去設計政府的架構。

（2）零信任架構最重要的是「觀念的改變」，以前進辦公室就覺得安全，現在不同以往，要提醒你進辦公室也不是安全的，要縮到核心的系統，而系統的管理人是自己人，而非把管理權再委外，如果可以重新設計內部的架構，要使用資料需身分與設備之鑑別。

（3）零信任架構是一個口號，應該要實際做一些事情，在必要的設備外還有人，內容合不合理，評估哪些設備較重要需加驗證機制，全部零信任不可行，人的觀念在零信任上辨別訊息的真假相同重要。

（4）零信任問題研析：

〈1〉系統整合問題：政府組織可能已有許多不同的系統和應用程序，而所依賴不同的身分驗證和授權機制，要將這些系統整合到一個統一的零信任架構下，需耗費大量之時間和資源。

〈2〉使用者體驗問題：零信任架構要求使用者在每一次訪問時都要進行身分驗證和授權，這可能會導致使用者體驗變得複雜和繁瑣，對使用者的工作效率和滿意度造成負面影響。

〈3〉費用問題：實施零信任架構需要投入大量的資源，包括硬體、軟體和人力等方面的成本，可能會對組織的成本造成壓力。

〈4〉文化變革問題：零信任架構需要組織內部文化的轉變，包括讓使用者接受這種新的安全模式和實踐，以及組織需要重新定義對於安全的觀念和目標等方面。

〈5〉舊有系統和設備的問題：部分組織可能有老舊的系統和設備，造成系統和設備可能無法適應零信任架構的需求,需重新升級或替換,會增加實施零信任架構的難度和成本。

(五)承前所述,政府機關推動資安零信任牽涉諸多面向,存有困難度，尚有努力的空間。為了讓政府機關導入零信任網路有依循方針，資安院針對身分鑑別機制導入檢核清單建議文件，包含規劃、建置、驗證等三階段，提供政府機關參考，當中包含具體參考步驟與檢核表，協助機關逐步建立零信任網路資安防護環境。另發現數位部第六期國家資通安全方案（110年至113年）[22]，在工作項目之3-1「建立零信任架構資安防護驗證環境，完善網路防禦縱深」,設定110年至113年重要進程之量化目標，分別為：110年完成零信任網路與概念性驗證機制研究與部署機制，111年推動2個機關導入零信任網路之身分鑑別機制，112年推動2個機關導入零信任網路之設備鑑別機制，113年推動2個機關導入零信任網路之信任推斷機制。是以，數位部現已循序漸進式評估並導入零信任網路，未來可依資安院提供的導入建議,協助政府機關零信任網路,強化資安防護能力,並驗證其可行性。

[22] 數位部資通安全署，國家資通安全發展方案（110年至113年)，取自網址：https://moda.gov.tw/ACS/operations/policies-and-regulations/648。

項次	導入作為	依據	完成
規劃階段			
1	選擇導入之資通系統	表1-1	□
2	評估身分鑑別方式是否新舊併行	表2-1、表2-2	□
3	評估使用者帳號是否維持一致	表3-1	□
4	尋求零信任網路身分鑑別系統	通過功能符合性驗證廠商清單	□
5	評估鑑別器採用方案	表5-1	□
6	評估資通系統介接之工作量	表6-1	□
7	規劃導入所需軟體	表7-1	□
8	規劃導入所需硬體	表8-1	□
9	規劃導入所需經費	表9-1	□
建置階段			
10	採購導入所需之軟硬體	機關採購作業程序	□
11	部署零信任網路身分鑑別系統	表11-1	□
12	介接現有身分鑑別伺服器	表12-1	□
13	介接導入之資通系統	零信任網路資通系統連線測試	□
14	設定網路環境	表14-1、表14-2	□
15	訂定鑑別器管理作業辦法	機關鑑別器管理作業辦法	□
驗證階段			
16	驗收採購項目	機關採購驗收作業程序	□
17	驗證部署符合性	政府零信任網路身分鑑別部署驗證檢核表	□
18	確保具備維運與使用能力	說明文件與教育訓練課程	□

圖8　零信任檢核清單建議文件（含規劃、建置、驗證各階段）
資料來源：NCCST，政府零信任網路身分鑑別機制導入建議(V1.0)。

(六)綜上，政府零信任網路架構係參考美國國家標準暨技術研究院零信任架構，同時結合向上集中之防護需求；然政府機關推動資安零信任牽涉諸多面向與磨合，尚有努力的空間，數位部宜透過「身分鑑別、設備鑑別及信任推斷」3大核心機制，落實政府機關試行零信任網路，並藉由檢核清單，逐步擴大導入機關，透過可操作性之導入步驟，降低機關實施零信任網路之疑慮與負擔，逐步建立零信任網路資安防護環境。

六、資通產品或服務琳瑯滿目，即使有完善管理制度，若不慎採用危害資通安全的產品，仍不免有機敏資料遭竄改、竊取之風險。基此，數位部允宜儘速要求各政府機關暨所屬單位依據「各機關對危害國家資通安全產品限制使用原則」規定，查核盤點現有產品及關鍵零件，是否仍有中製產品存在，並追蹤機關截至111年底已盤查之危害國家資通安全產品約2千多件之汰換

進度，並向所屬人員宣導使用危害國家資通安全產品之風險。此外，產品可追溯已是國際趨勢，數位部與經濟部等相關機關積極合作建構「資安生產履歷制度」，期整合產銷供應鏈，以降低國家資通安全風險

(一)資通產品或服務琳瑯滿目，即使有完善管理制度，若不慎採用了危害資通安全的產品，仍不免有機敏資料遭竄改、竊取之風險。行政院因而訂定「限制使用危害國家資通安全產品」，針對公務體系(包括公務機關及公營事業等)要求禁用中國大陸廠牌產品之規定，分別說明如下[23]：

1、原則禁用危安產品：依「各機關對危害國家資通安全產品限制使用原則」[24]規定，有關危害國家資通安全產品係指，對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務。且該原則明示，各機關應向所屬人員宣導使用危害國家資通安全產品之風險。

2、原則禁用中國大陸廠牌產品：行政院於109年12月18日曾行文各公務機關於110年底前，完成汰換所使用或採購中國大陸廠牌資通訊產品作業，先前已採購而未能立即汰換者，則須列冊管理並原則禁止與公務環境介接。至於所謂「中國大陸廠牌」，指廠牌係屬依大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體所擁有者而言；此分類係依據工程會107年12月20日工程企字第1070050131號函中針對「大陸

[23] 資料來源：李婉萍、陳宏志，從《資通安全管理法》看企業資安維護，取自網址：chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.sef.org.tw/files/13055/AB55AFE5-DC99-4E6C-9592-64A523D80CC8.pdf。

[24] 行政院於108年4月18日以院臺護字第1080171497號函頒。

地區廠商」的定義而來[25]。另依「盤點及汰換大廠牌資通訊產品相關注意事項」規定，不限於硬體，亦包含軟體及服務。惟盤點之產品係指機關本身可以辨識之終端產品為主，暫未考量產品內部之構成元件。

(二)是以，參照上開原則意涵，國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務之危害國家資通安全產品，除因業務需求且無其他替代方案外，不得採購。且依原則第1點指出，對象包含中央與地方機關（構）、公立學校、公營事業及行政法人採購資通產品時皆須遵守，其中八大關鍵基礎設施提供者、政府捐助之財團法人，將由中央主管機關督導參考該原則規定辦理。管制之資通產品包含：網路攝影機、無人機、伺服器主機、雲端的服務、電信業核心骨幹網路設備、電腦軟體、防毒軟體、機關委外開發的系統等。

(三)數位部成立後，於111年11月28日以數授資綜字第1111000056號函，修正上開使用原則第4點，對於各公家機關自行或委外營運、提供公眾活動或使用的場地新增規定，也不得使用有資安疑慮產品；如果有特殊原因必須使用，須經**機關資安長及上級機關資安長逐級核可**，另據112年5月3日座談會數位部關政務次長河鳴表示略以，目前危害國家資通安全產品改善情形列管數量，於111年底盤點後約2千多件，宜持續追蹤機關汰換進度。再者，行政院公共工程委員會已將禁止使用及採購有資安疑慮資通

[25] 資料來源：工程會函，主旨：機關辦理資訊、電訊或通訊設備有關採購，相關注意事項如說明，請查照並轉知所屬機關，取自網址：https://planpe.pcc.gov.tw/prms/explainLetter/readPrmsExplainLetterContentDetail?pkPrmsRuleContent=60046771。

訊產品的規定，納入契約範本中，提供各機關採購運用，甚且，行政院將「資訊服務採購案之資安檢核事項」列為各機關採購履約的要求項目。對此，資安署表示，會持續要求各公務機關每年定期盤點危害國家資通訊產品使用情形，以掌握相關風險。

(四)再者，現今我國電子資訊製造業者可透過建構製造執行系統(Manufacturing Execution System，MES)[26]，掌握各類電子產品的「生產履歷」，亦即在製造過程中，詳實地記錄生產資訊，當企業遇到問題必須回收產品時，只需就有問題之該批產品序號進行回收，不必大範圍召回，MES已將生產過程中的人、事、時、地、物完整的記錄管理，提供一個嚴謹的生產履歷管理追蹤機制，經濟部表示，產業署主責產業數位轉型之規劃、輔導及推動，工業局將配合數位部之規劃，協助導入至相關製造產業，亦指出：「由於MES之運作需建立在其他廠務資訊系統的基礎之上，且需有足夠的資訊人員來進行管理，企業亦需要挹注較多營運資金進行數位轉型，目前以中大型製造業較有能力建置完整系統。由於受限於企業營運資金規模之條件，全面導入施行之困難度較高，尚有努力的空間[27]」等。另依中研院資訊及資創中心客座講座李德財亦指出：「建議資安比照食安，建構數位消費產品履歷與安全標章，為管理食品衛生安全及品質，維護國民健康，而制定食安法，可要求主管單位，對民眾消費入肚的食品安全把關，隨時進行抽驗，惟對於網路世界裡的民生消費電子產品，是否一併重視，未來可規劃比照食安法，建

[26] 經濟部112年6月2日經授工字第11251024910號函。

[27] 據資策會MIC於106年製造業智慧科技需求調查，以IC封測產業為例，導入MES系統者占比為91%，資訊硬體產業導入MES系統占比為64%。

構數位產品的透明資安履歷制度，對電子消費產品應標示製造廠地等生產履歷，成立資安檢測機構，建立安全標章制度，上架產品必須通過安全檢驗[28]」。是以，不論硬體製造或軟體研發，面臨資安威脅情況下，建立「產品履歷」有其必要性，推行時恐面臨導入困難需克服，有待數位部與經濟部等相關機關積極研酌並予以推廣。

(五)綜上，資通產品或服務琳瑯滿目，即使有完善管理制度，若不慎採用危害資通安全的產品，仍不免有機敏資料遭竄改、竊取之風險。基此，數位部允宜儘速要求各政府機關暨所屬單位依據「各機關對危害國家資通安全產品限制使用原則」規定，查核盤點現有產品及關鍵零件，是否仍有中製產品存在，並追蹤機關截至111年底已盤查之危害國家資通安全產品約2千多件之汰換進度，並向所屬人員宣導使用危害國家資通安全產品之風險。此外，產品可追溯已是國際趨勢，數位部與經濟部等相關機關積極合作建構「資安生產履歷制度」，期整合產銷供應鏈，以降低國家資通安全風險。

七、資通安全所涉包含人、科技、流程三者之結合，其中「人」方屬確保國家資通安全重要關鍵，觀諸我國政府機關與各產業資安人力之質與量嚴重不足，此議題已成為全世界所面臨之窘境，爰採暫時性措施，以委外或約聘來補充人力，惟其核心業務、技術傳承、機敏性方面恐存有資安風險，數位部允宜確實盤點，並建立專家資料庫所需職能基準，以利各界進用所需資

[28] 資料來源：李德財（2023），建構數位消費產品履歷與安全標章，取自網址：https://www.wealth.com.tw/articles/a762946c-f301-49ca-b08e-1e33f634dcd3。

安人才，並積極設法協助、補充資安人力，填彌補資安人力缺口

(一)大型資安事件頻傳，讓企業高層越來越重視資安，對於資安投資，也比過去更積極，願意設置更多資安人力的編制，再加上近年多項法遵要求，不論是資安法對於八大關鍵基礎設施產業的資安要求，或是金管會要求金融產業、上市櫃公司，都必須設置資安專責人力，惟臺灣政府機關與各產業資安人員能量均嚴重不足，企業資安人力亮警訊，此議題已成為全世界所面臨的問題，以下就我國各產業資安人力現況進行說明：

1、<u>於2022年政府與學校對於資安人才的缺口最大，因此招募人數也最多，資安職缺數平均達到4.3人，金融業居次，平均為3.5人</u>，特別的是，這兩個產業的平均現有資安人力，已經來到5.8人與9.5人，反映他們對資安方面人力的渴求程度依舊高，可參照下圖。

單位：人

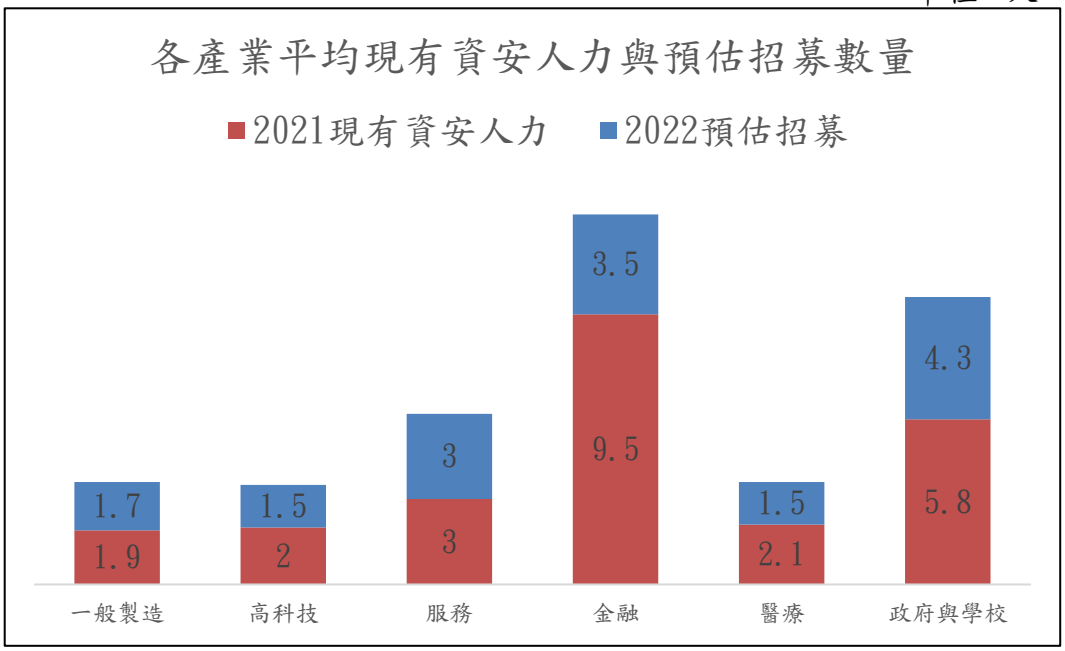

圖9　各產業平均現有資安人力與預估招募數量

資料來源：據2022 iThome資安大調查重新彙製

2、各產業招募資安人力的比例詳下圖，整體為3成，也就是每10家公司有3家要招資安人才，其中金融業的比例達7成2，醫療與高科技業比例在3成以上，一般製造業與服務業也有2成多，另參下圖。

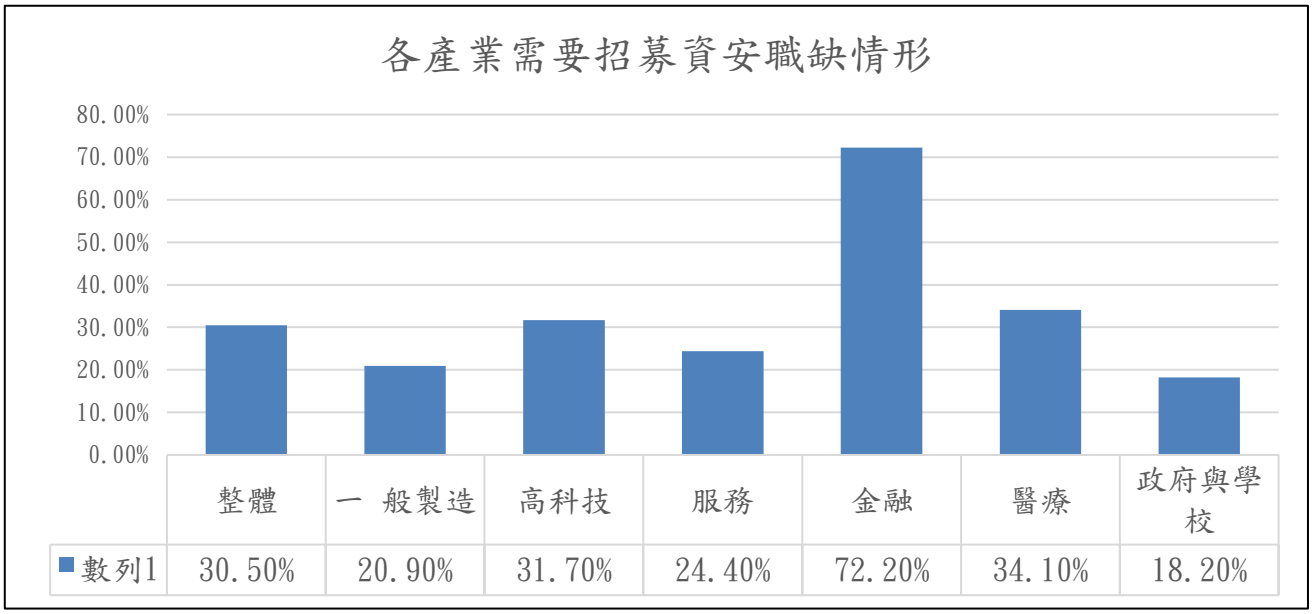

圖10　各產業招募資安職缺概況

資料來源：據2022 iThome資安大調查重新彙製

3、對於資安人力不足，本院蒐整相關報導摘錄如后：

（1）報導1-「找不到資安人才？安碁學苑培育企業資安即戰力首重兩大關鍵[29]」：金管會力推「上市櫃公司資通安全管理措施」，將上市櫃公司分為三級[30]，要求第一級115家在111年底、第二級

[29] 資料來源：ESG遠見，找不到資安人才？安碁學苑培育企業資安即戰力 首重兩大關鍵，取自網址：https://esg.gvm.com.tw/article/27646。

[30] 分級標準：**第1級**（符合條件之一者）：1.資本額100億元以上（**資安單位暨人力編制：應設資安長及設置資安專責單位『包含資安專責主管及至少2名資安專責人員』**）。2.前一年底屬臺灣50指數成分公司。3.藉電子方式媒介商品所有權移轉或提供服務（如電子銷售平台、人力銀行等）收入占最近年度營業收入達80%以上，或占最近二年度營業收入達50%以上者；**第2級**：第一級以外之上市（櫃）公司，最近三年度之稅前純益未有連續虧損，且最近年度財務報告每股淨值未低於面額者（**資安單位暨人力編制：資安專責主管及至少1名資安專責**

1387家在112年底設置資安長及資安人員，市場預估相關人力需求高達五千人，但反觀大學端並沒有相對應的資安科系來產出人才，供需嚴重失衡。

（2）報導2-「今年要求1千4百多家公司設置專責資安單位，目前僅2成達標[31]」：國內已有270多家公司提早完成目標，比例將近2成，仍有8成公司還未行動，目前資安長、資安專責單位及資安人員設置狀況詳下表。

圖11　資安長、資安專責單位及資安人員設置情形

單位：人

		第1級公司		第2級公司	
		上市	上櫃	上市	上櫃
	合計	102	13	772	671
資安主管	已設置	102	13	170	125
	未設置	0	0	602	546
資安人員	已設置	102	13	170	138
	未設置	0	0	602	533
整體設置	皆已設置	102	13	154	118
	尚未完整	0	0	618	553

註：統計時間截至112年4月30日

資料來源：據2022 iThome資安大調查重新彙製

（3）報導3-「祭高薪酬 明年增募資安人才[32]」：官股

人員）；**第3級**：第一級以外上市（櫃）公司，最近3年度稅前純益有連續虧損，或最近年度每股淨值低於面額（**資安單位暨人力編制：至少1名資安專責人員**）；資安專責人員：按負責資通安全事務之人即為資安專責人員，並無強制公司投入專職人力之要求，公司應視實際面臨之資訊安全風險及需求，評估是否藉額外投入或職務劃分方式配置專職負責資訊安全之人力資源，以強化資訊安全控制作業之有效性。資料來源：金管會新聞稿、公開發行公司建立內部控制制度處理準則問答集（111年12月20日版），取自：https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=202112230009&dtable=News；chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.fsc.gov.tw/uploaddowndoc?file=chdownload/202212291737400.pdf&filedisplay=1111220%E5%85%A7%E6%8E%A7QA%28%E5%85%A7%E6%8E%A7%E5%B0%88%E5%AF%A9-%E4%BF%AE%E6%AD%A3%E4%B9%BE%E6%B7%A8.pdf&flag=doc。

[31] 資料來源：iThome，今年要求1千4百多家公司設置專責資安單位，目前僅2成達標，取自網址：https://www.ithome.com.tw/news/157014。

[32] 資料來源：工商時報，祭高薪酬 明年增募資安人才，取自網址：https://ctee.com.tw/n

銀行持續強化增加資訊、資安人才，除了推出有吸引力的薪酬，也加速升遷速度。112年起土地銀行擴增至26名（目前資安專責單位員額20名）、合庫銀行增加3人（資安單位目前37人）、華南銀行規劃年底前招募10位資安工程師、臺灣企銀較111年，預計增加約38%資安人力。

（4）報導4-「數位部加速徵才 先補資安人力[33]」:期盼可先把資通安全人力補足，以彈性用人機制吸引具有數位專長的人才。

（5）報導5-「公務機關資安人力不足 行政院：可約聘僱或委外[34]」：重視資安的蔡政府儘管推動訂定資安法，上路施行已逾3年半，但全國各公務機關仍普遍有資安專職人員不足的問題，據悉，行政院要求各機關應優先在機關總員額內配置資安專職人力，不過，為解決現行專責人力的缺口，各機關可彈性先聘請具資安專業的約聘僱或委外人員擔任，未來再補正式編制人員。

（6）報導6-「人才是確保國家網路安全關鍵[35]」：資安的重要性已是不言而喻的狀態，而關於資安人才不足的議題也存在許多年，而遲遲缺乏有效解方。

（7）報導7-「Fortinet 調查：資安人才缺口持續，遭駭客入侵五次以上企業增逾五成[36]」：全球及

---

ews/finance/767161.html，

[33] 資料來源：聯合新聞網，數位部加速徵才 先補資安人力，取自網址：https://udn.com/news/story/7238/6569541。

[34] 資料來源：自由時報，公務機關資安人力不足 政院：可約聘僱或委外，取自網址：https://news.ltn.com.tw/news/politics/breakingnews/4005119。

[35] iThome，人才是確保國家網路安全關鍵，取自網址：https://www.ithome.com.tw/news/156619。

[36] 資料來源：iThome，Fortinet 調查：資安人才缺口持續，遭駭客入侵五次以上企業增逾五成，取自網址：https://www.ithome.com.tw/pr/156269。

臺灣超過1,800位IT及資安決策者進行調查，結果顯示，資安技能落差導致多數企業必須面對更加嚴峻的資安風險和安全威脅，包括遭到駭客入侵及蒙受財務損失等。而隨著強化資安韌性成為企業組織的優先關注事項，網路安全培訓與認證也在縮短資安技能落差方面，受到眾多企業管理層的高度重視。

（8）報導8-「臺灣資安人才缺口達9萬人，數位部如何縮小缺才困境[37]？」：單就政府需求方面，據資安管理法所訂定出的分級與相對應的人才需求數量，光是政府本身所需要的資安人才就有1,552人。那麼企業的需求量就更大了，臺灣整體中小企業加總起來超過100萬家，而企業的資安人才需大約有8、9萬人。

（9）報導9-「一紙法令，曝資安2萬人才缺口[38]！」：資安人才需求5年成長2倍，法令要求下，造成了資安人才需求的擴大。

(二)再參，國家「資通安全戰略報告，資安即國安2.0」亦指出，現今政府與產業各界均面臨資安人力不足的窘境，前者受限於公務人員選才制度（可參結論與建議九所述），致資安人才招募不易，而專責資安職缺與任務日增，專職資安人員的空缺仍多，其中又以關鍵基礎設施之相關事業單位缺少資安人才為最迫切。從供給面來看，許多在校修讀資訊/資安相關科系領域的優秀人才，在強大的就業磁吸效應與跨國企業提供優渥的待遇條件影響下，並未選擇進

[37] 資料來源：科技新報，台灣資安人才缺口達 9 萬人，數位部如何縮小缺才困境？取自網址：https://technews.tw/2022/12/22/cyber-security-in-taiwan/。

[38] 資料來源：數位時代，一紙法令，曝資安2萬人才缺口！取自網址：https://www.bnext.com.tw/article/67764/cybersecurity-talents-?。

入資安領域的職場工作；至於針對在職者進行跨領域別的資安能力培育則更加不易。在此種種狀況下，國內整體優質資安人才無論質與量提升的努力空間仍大，且整體的聯合防禦能量仍有待進一步提升[39]。對此議題本院請數位部統計政府機關資安專職人員數據如下表，然該部提供資料發現目前資安專職人員應置人數不足，在行政院缺額僅0.52%，地方政府缺額高達52.53%，且統計時間還是之前的資料，此數據與實際恐有落差。對此，歷次履勘與座談會闕次長河鳴表示略以:「資安署開始盤點資安的人員的缺口，同步訂定資安人員基準，未來持續培育政府及資安產業資安人才」、「資安人力不足是全世界的問題，美國、臺灣都面臨此窘境，巨大的缺口是存在的」等語益徵，足見政府與產業各界均面臨資安人才不足的窘境，宜確實全盤性的盤點資安人力缺口，並設法補足。

圖12　政府機關資安專職人員一覽表

單位：人；%

		資安專職人員					
		應置人數A	現任職員B	在職約聘僱C	委外派駐D	不足人數 E=A-B-C-D	不足比率 E/A*100%
行政院		776	497	186	89	4	**0.52**
地方	直轄市	390	299	67	2	22	**5.64**
	縣市	386	165	38	2	181	**46.89**
合計		1,552	961	291	93	207	13.34

統計時間：111年6月。

資料來源：數位部座談會資料

[39] 資料來源：國家資通安全戰略報告，資安即國安2.0，摘錄總統蔡英文2021年7月12日序，取自網址：file:///C:/Users/hjgao/Downloads/6cd56ef5-29fd-42d8-90cc-6228e7ed3ab4.pdf。

(三)綜上，資通安全所涉包含人、科技、流程三者之結合，其中「人」方屬確保國家資通安全重要關鍵，觀諸我國政府機關與各產業資安人力之質與量嚴重不足，此議題已成為全世界所面臨之窘境，爰採暫時性措施，以委外或約聘來補充人力，惟其核心業務、技術傳承、機敏性方面恐存有資安風險，數位部允宜確實盤點，並建立專家資料庫所需職能基準，以利各界進用所需資安人才，並積極設法協助、補充資安人力，填彌補資安人力缺口。

八、數位部與國家資通安全研究院被賦予培育與訓練資安人才之重要責任，面臨產業資安需求擴大，對於產業資安人才之養成、訓練及實戰演練等，允宜與時俱進持續規劃相關培訓課程，並善用全國首座資安攻防演訓實證場域，培育產業所需之資安專才，協助國內資安產業研發能量，藉以提升企業資安意識，充實與厚植我國資安實戰人才與防護能量

(一)除政府機關資安人力出現缺口外，產業資安人才亦隨著資安需求擴大，人才供給面臨挑戰（詳結論與建議七所述），依資安產業發展行動計畫（107年至114年）[40]指出，我國資安產業發展劣勢之一，欠缺關鍵技術與專業人才，提出「建立需求導向之資安人才培訓體系」之策略與目標，並依資安產業發展策略會議(SRB)，提出人才培育相關策略與目標[41]，

[40] 行政院，資安產業發展行動計畫（107年至114年），取自網址：https://www.ey.gov.tw/Page/5A8A0CB5B41DA11E/4415fe14-477e-45cb-9a09-cb6962054fa6。

[41] 1.建立人才與產學研鏈結體系，掌握產業資安人才需求，結合學校、公協會建立自主培訓體系，培育產業資安新血。2、推動資安菁英培育機制，如每年提供大量研究生名額參與 先進國家的資安培訓計畫，或參與國際資安團隊實作。3、推動資安人才在職培訓，彌補產業人才缺口，並鼓勵產學 研界資安人才流動，從研究機構釋出研發人員到業界，提 升產業資安產品研發能量。4、強化人才投入之誘因，提共多發展的舞臺，並可以透過競賽的方式找到優異人才。

說明如下：

1、策略：掌握企業專屬資安人才、建置校園人才培育系統、設置資安研訓機構、媒合人才就業及延攬國際人才等5項具體措施，初期連結既有培育能量成立資安學院，並建立特色資安系所，終極目標是打造世界級資安研訓機構。短期成立資安研訓院，媒合人才就業，中期發展特色資安系所，長期打造世界級資安研訓機構為目標。

2、具體目標：114年目標為達1萬人；一般(非資安)產業(包括關鍵基礎設施、政府單位)資安從業人口達11,000人，詳下圖。

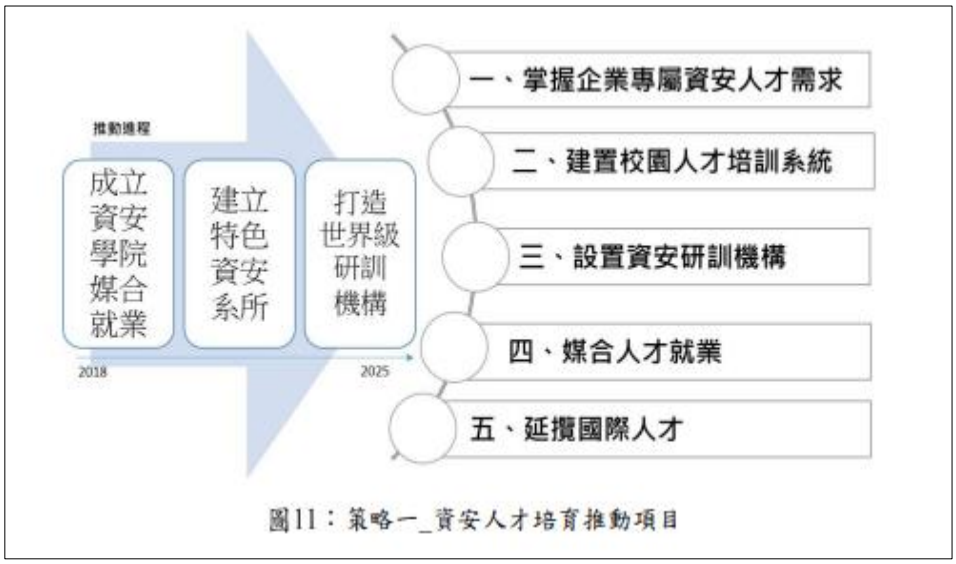

圖13　資安人才培育推動項目
資料來源：資安產業發展行動計畫

3、另參第六期國家資通安全發展方案（110年至113年）[42]之重要績效指標中，亦有培育資安實戰人才之規劃，其中110年至113年間，分別培育50名、50名、125名、125名等，計至少培育350名資安實戰人才。

[42] 數位部資通安全署，國家資通安全發展方案（110年至113年），取自網址：https://moda.gov.tw/ACS/operations/policies-and-regulations/648。

(二)承前所述，我國資安人才需求急迫，已不足以快速因應補足政府與企業對於專職資安人力，總統亦表示，政府會全力推動資安政策，強化組織、完善法制，並培養更多人才。基此，究如何延攬、招募及培育相關資安人才？數位部與資安院說明如下：

（1）依112年2月3日總統府新聞稿與相關報導[43]，總統表示略以，「政府會全力推動資安即國安2.0政策，持續強化組織、完善法制，並培養更多人才，提供產業更多支持」、「一起帶動整體資安產業的發展，共同建立堅韌、安全、可信賴的智慧國家」」、「全力推動資安即國安2.0，強化法制及人才培育」、「臺灣在資安領域有很好的競爭力，期待未來能有更多本土廠商、更多優質產品邁向國際市場」、「資安就是政府的重要施政目標，政府持續推動數位轉型、加強社會各領域的資安韌性」。

（2）數位部產業署：資安人才培育不僅著重實務，還需考慮各種不同類型的資安人才養成，該署表示藉由實務課程，就不同對象與層級的資安知識、技能和能力，強化產業的資安防護力，同時透過與資安院合作提升全民資安意識，提高國內資安素養水平；另據該署說明，依據不同對象之需求，規劃相關實務訓練課程，包括資安主管、特定資安專家、資安工程師和一般人員等4類。針對資安主管，提供法規遵循、資

[43] 資料來源：總統府，接見2022資安獎得獎廠商　總統盼與業界共同建立「堅韌、安全、可信賴的智慧國家」，取自網址：https://www.president.gov.tw/NEWS/27282?DeteailNo=%E8%B3%87%E5%AE%89；中央廣播電臺，總統：全力推動資安即國安2.0 強化法制及人才培育，取自網址：https://www.rti.org.tw/news/view/id/2157932；自由時報，力推「資安即國安2.0」 蔡英文：培養人才、提供產業更多支持，取自網址：https://news.ltn.com.tw/news/politics/breakingnews/4200021；中央通訊社，總統接見資安得獎廠商 全力推動資安即國安2.0政策，取自網址：https://www.cna.com.tw/news/aipl/202302030069.aspx。

安技術、縱深防護和整合性營運思維的工作坊；對於資安專家，提供新興議題、跨域資安應用技術課程；針對資安工程師，則提供資安專業技能培訓，結合實務實戰訓練，規劃訓練養成技能課程；對於一般人員，則安排多元形式的資安認知與實務型課程。

（3）資安院：對於人才培育與養成方面，依照資安職能地圖持續擴充資安課程，課程規劃參考歐盟ENISA之 European Cybersecurity Skills Framework (ECSF)與美國NIST網路安全人力框架(Cybersecurity Workforce Framework，NICE Framework)研訂資安職能基準，持續擴充完備資安課程，提升資安人才培育成效，擴大資安人力供給。另，針對資安高階人才養成，除現有政府機關資安職能課程外，設置資安人培實習場域，強化工控領域訓練，並持續開發紅藍攻防實戰平臺腳本，提供線上學習與演練管道，加強紅藍隊頂尖人才訓練及養成，因應新興資安議題，掌握關鍵資安技術之高階資安菁英人才，強化單位資安防護能量。

(三)為發展與提升產業資安量能，數位部於臺南市沙崙打造全國首座資安攻防演訓實證場域－沙崙資安服務基地，建置主題產業實戰場域，運用攻防演訓劇本與沙崙基地之實作平臺，提供企業進行資安產品驗測與舉辦相關人才培訓活動，除幫助企業了解自身產品進而優化與提升產品效能，亦協助國內關鍵基礎設施從業人員、資安工程師、資安管理人員等，透過攻防演訓實務訓練，提升人員應變與實務能力，培育產業所需之資安專才，以協助國內資安產業研發能量及產業資安防護能量。

(四)綜上，數位部與國家資通安全研究院被賦予培育與訓練資安人才之重要責任，面臨產業資安需求擴大，對於產業資安人才之養成、訓練及實戰演練等，允宜與時俱進持續規劃相關培訓課程，並善用全國首座資安攻防演訓實證場域，培育產業所需之資安專才，協助國內資安產業研發能量，藉以提升企業資安意識，充實與厚植我國資安實戰人才與防護能量。

九、各政府機關進用資安業務人才，乃透過國家考試任用或機關自行招募，且多由資訊人員辦理，查國家考試進用資安人員，僅有「資訊處理職系」與資安相關，然兩者所需職能存有顯著差異。甚且，國家考試以筆試為主，難以評鑑受測人員實作能力，與實務工作性質有間，以及在面對持續不斷變動之新型資安威脅與挑戰，尚難隨時補充人力，數位部與考選部允宜重新思考穩健擘劃資安人員國家考試制度，設計出符合我國政府資安專業人員之進用方式

(一)在政府推動「資安即國安」的國家戰略下，將資安提升至國安防護層級，可見其重要性，隨著資通訊新興科技的發展，已在民眾生活、企業經營及政府運作等層面，產生莫大變化，因此全球先進國家已將推動數位政府，作為提高國家競爭力的重要策略，有關政府資訊人才進用管道，依據公務人員任用法相關規定，目前管道大致可區分為2類：

1、國家考試任用：依據公務人員任用法第9條第1項第1款「公務人員之任用，應依法考試及格」及公務人員考試法第1條「公務人員之任用，依本法以考試定其資格」規定，配合用人機關需要，由用人機關提出需用名額，再由考選部辦理初任公務人員之國家考試，包括高等、普通考試及特種考

試2大類，其考試類科則以資訊處理類科為主。

2、機關自行招募：依據公務人員任用法第36條規定「各機關以契約定期聘用之專業或技術人員，其聘用另以法律定之」，機關可因組織業務需要，獨立辦理相關領域之專業人才（如資訊人員）招募作業，由機關訂定招募目的與設定用人需求數，並確定工作職稱、目的、義務、責任及應徵者需應具有之資格、技術、知識、能力等條件，透過正式管道（如出缺機關網站、行政院人事行政總處網站、民間求職網站等），刊登求才訊息，並以面試或筆試等方式篩選適格人選，成為機關之資訊約聘僱人員或臨時人員。

(二)另查，有關資訊處理職系公務人力詳下表[44]，資訊處理職系人員計3,506人，僅占1.82%，相較於美國政府資訊人力平均約4%，我國政府資訊人力明顯出現落差。

圖14　國家考試資安處理職系公務人力情形

單位：人；%

年度	有職系歸類者(A)	資訊處理職系(B)	資訊人力占比(C) C=B/A*100%
106	188,668	3,398	1.80
107	192,441	3,476	1.81
108	194,035	3,547	1.83
109	194,742	3,567	1.83
110	192,981	3,542	1.84
平均	192,573	3,506	1.82

備註：

1.人數統計不包含約聘僱與臨時人員。

2.依法歸系人員指依公務人員任用法任用，並依第8條予以歸系人員。

資料來源：國家人力資源論壇

[44] 資料來源：余慶杉，公務人員考試資訊處理類科辦理情形分析，國家人力資源論壇，第21期，取自網址：https://www.exam.gov.tw/NHRF/News_EpaperContent.aspx?n=3778&s=45832&type=A9DCC80FC8CC7601。

(三)承前所及，目前國家考試進用資安人員，依現行公務人員職系僅有「資訊處理職系」與資安相關，然二者所需職能顯有差異，資安人員面對各種駭客入侵攻擊，需要有即時應處能力，因此為國選才時也需評鑑受測人員之實作能力、上機考試之實作測驗有其必要；然資安人員國家考試以筆試作為主要測驗方式，未見上機考試。本院歷次履勘與座談會時，數位部、資安署、產業署表示，現階段招募約聘人員，以上機測驗作為遴選方式之一，可有效鑑別遴選者之能力與經驗。

(四)有關政府資訊人才進用之挑戰，本研究歷次履勘與座談會闕次長河鳴、鄭副署長欣明分別表示略以：「目前積極與考試院討論，可參考資安院人員徵選機制（辦理上機考試，進階篩選實戰能力）。期未來增加資安職系，不過目前在資訊職系與資安職系尚需釐清其差異性，及考量國內學校的教學科目是否足夠應付」、「資安院未成立前，其人員由資安署代為招募徵選，除透過書審資格、筆試、面試外，還需上機考試評估資安能力，經層層關卡後方能錄取，總錄取率約75%」。另本院諮詢學者認為，未來可設置資安稽核師，以國家考試方式，培養「資安架構師」之通才。綜上所述，有關公部門人力需求將隨著政府組織任務與型態發展不同，而有所調整改變，目前政府資訊專業人才之進用與培訓，正面臨下列幾項挑戰，考選部資訊管理處專門委員余慶杉指出：

1、機關員額限制：受限於政府機關預算員額配置與資訊正式人力編制侷限，較難彈性提出額外需用名額，據以辦理國家考試，滿足政府數位發展之大幅人力需求。

2、企業人才競爭：政府資訊人力講求通才，企業資訊人力則重視專才，由於我國資訊領域產業發達，民間徵才待遇優渥，使得政府須面對與民間人才及薪資嚴重競爭之現象。

3、人才淘汰快速：考試進用僅為敲門磚，身處資訊科技快速變化之時代，須持續學習資通訊專業技能，才能跟上數位創新腳步。

4、資訊專業度高：因應資訊領域不同、資訊產業執業要求及證照變動幅度快速與多樣，資訊專業證照、職能訓練、專業課程多由國內外資訊業者與民間專業機構提供為主，政府機關難全面主導。

(五)惟長遠而言，政府資安人員之進用方式，除約聘人員外，仍應併採國家考試途徑，在面對持續不斷變動新型之資安威脅與挑戰，適時補充人力，且因應人才進入政府機關後一段時間，隨即遭民間公司高薪挖角，有關資安職系之專業加給設計制度，亦應從優考量，方可增加資安專業人員投入政府機關之意願。為配合政府資訊化發展腳步，近年來有關資訊類公務人員考試取才之方法與內容，考選部允宜適時進行調整並積極研酌，參據該部資訊管理處專門委員余慶杉提出以下看法：

1、檢討高普考試不合時宜應試專業科目：考量時代變遷，機關用人需求與業務特性有所改變，考選部於109年提出在應試科目數不變原則下，應試專業科目修正議題，徵詢中央各部會、地方縣市政府及用人機關意見，並賡續針對部分尚未獲共識之類科，邀集機關代表及相關專業領域學者專家研商，於同年完成公務人員高等考試三級考試暨普通考試規則修正，在維持現行科目數之原則下，計修正資訊處理等15類科之應試專業科目，

並自111年施行。

2、國家安全情報人員特考增設公職資訊技師：為配合特殊用人機關期望引進民間有經驗的專業人才，投入國家資安工作，國家安全情報人員特考新增公職資訊技師組，除年齡及學歷限制外，並規定應領有資訊技師證書及具2年以上資訊相關工作經驗者始得報考，其考科僅列考2項專業科目，通過筆試後再加考體能測驗及口試，以考選遴用具資通安全專門技術相關人才。

(六)綜上，各政府機關進用資安業務人才，乃透過國家考試任用或機關自行招募，且多由資訊人員辦理，查國家考試進用資安人員，僅有「資訊處理職系」與資安相關，然兩者所需職能存有顯著差異。甚且，國家考試以筆試為主，難以評鑑受測人員實作能力，與實務工作性質有間，以及在面對持續不斷變動之新型資安威脅與挑戰，尚難隨時補充人力，數位部與考選部允宜重新思考穩健擘劃資安人員國家考試制度，設計出符合我國政府資安專業人員之進用方式。

十、我國因地緣關係因素，資安領域平時即為戰時，對岸龐大網軍無時差入侵，造就國際企業願與我國資安公司合作，中央資安主管機關允宜與時俱進，持續推動符合潮流之政策，引領國內資安新創公司發展並邁向世界，提升我國資安產業質量並進及創造產值，揆諸以色列「資訊安全生態園區」，提供人才與創新科技之發展平台，作為網路資安產業之協調機構，形成產、官、學、研間之完整生態圈作法，殊值我國借鏡

(一)參照第五期國家資通安全發展方案(106年至109年)

[45]之推動策略之一，為推升「資安產業自主能量」，我國資安產業自主發展、提高國內自主率等事宜，行政院於108年11月28日公布「資通安全自主產品採購原則」，鼓勵中央與地方機關(構)、公立學校、公營事業及行政法人依政府採購法採用資通安全自主產品，進而帶動資通安全產業發展及強化國家資通安全防護能量。另經濟部為協助我國資安業者提升中長期競爭力，建置資安整合服務平臺(SecPaaS)，推動國產資安產品與服務媒合服務，供給方為可提供資安服務的廠商，如安全軟體開發工具商、滲透測試服務供應商、新興資安產品供應商，其產品與服務經審核通過後即可上架。需求方為場域代表或產品整合商，如系統整合服務商、解決方案提供商。透過平台協助媒合需求方場域導入資安產品試煉與實證，以期建推動垂直整合領域資安解決方案。目前數位部刻正推動第六期國家資通安全發展方案（110年至113年）[46]，連結國家防衛自主需求，發展國內資安產業生態系亦為現階段推動策略，其中提供具備內對內、內對外及跨機關網路導流作業，以強化政府網際服務網(Government Service Network，GSN)之內部資通安全性，配合資訊資源向上集中，推動政府機關網路出口集中至上級機關。強化政府大內網之主動防禦能量，及時阻擋惡意攻擊等，由前揭可見，目前政府對於資安產業有相關措施來協助渠等推動。

(二)基此，為加速我國資安產業發展，政府投入資源為

[45] 數位部資通安全署，國家資通安全發展方案（106年至109年），取自網址：chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www-api.moda.gov.tw/File/Get/acs/zh-tw/cYa9VkznxWRvmqR。

[46] 數位部資通安全署，國家資通安全發展方案（110年至113年），取自網址：https://moda.gov.tw/ACS/operations/policies-and-regulations/648。

我國資安業者創造有利條件及發展環境，使業者於發展初期快速蓄積多方面能量並獲得成長空間。並結合資安新創社群，辦理技術聚會、工作坊，建立產學研界資安趨勢與技術交流環境，串接國內資安研發能量，讓資安技術向下紮根，同時扶植新創公司或帶動大企業進行投資；然而，政府推動資安產業，不僅限於國內發展，更需推動資安產業規模化、國際化，達到資安產業自主能力，近年新成立的新創資安公司已逾百家、推動75件場域或產品實測，以建立資安解決方案，更跨出國際，與美國、日本、盧森堡、荷蘭、以色列等國家市場，安排實體商機媒合活動，使我國資安業者、新創公司與國外買家進行合作，展現臺灣資安實力與擴大資安產業規模。本研究在綜觀國際資通安全防護政策、規範與發展趨勢，擇定以色列作為國外實地考察國別，該國透過產、官、學、研共同協作，打造出世界級的先進技術園區，吸引來自全球各地創新科技人才與研發機構，摘錄112年3月24日赴以色列考察Cyber Spark[47]資訊安全生態園區所習經驗如下：

1、政策決心及具體行動：由總理府展現決心，承諾將以色列國防軍、其他情報與技術機構搬遷至此地，業界看到政府有決心及具體行動，讓該區有機會成為全球頂尖資安中心。

2、專業經營且充滿商機：園區由具備建置及營運高

[47] 網路星火產業園區（CyberSpark）：此為中央政府、地方政府、大學及企業共同合作在該地設立高科技園區，幾年下來已逐步轉型為全球知名的高科技與新創城市。該園區結合本古里安大學(Ben-Gurion University)、國家網路資安緊急應變團隊(CERT-IL)、新創公司、學研機構及國防部等，吸引多家跨國企業研發中心進駐，形成產、官、學、研間的完整生態圈。迄今已吸引約70多家國際大型企業進駐，超過2,500名工程師在此工作(約86%為當地居民)，預計至2029年為該地區創造超過1萬個高科技就業機會（資料來源：駐以色列代表處科技組官方網站，取自網址：https://www.nstc.gov.tw/israel/ch/detail/341fee19-e131-4ddb-be2a-185ac9c463ce）。

科技園區豐富經驗之Gav-Yam地產企業經營，開發時程考量搭配政策時間表，更重視各辦公大樓攸關營運損益之招商成效，深知唯有創造世界一流之工作環境，方能吸引世界頂級公司進駐。

3、民間參與公共建設模式（Public-Private Partnership，PPP）及分進合擊：園區採取PPP合作模式，由中央政府、地方政府、大學、園區運營專業地產開發公司及利害相關企業共同合作，通力分工吸引資安機構、新創公司及跨國企業進駐，有關產、官、學、研間之合作方式可參考下（三）之敘述。

(三)承前，以色列在國土環境上國小地貧，在政治國安上強敵環繞，以色列當局深知要在國際上占有一席之地，勢必發展高技術產業，且其國安問題以及政治威脅持續紛擾，導致以色列全民皆兵的現況，而戰爭的威脅也擴展至網路世界，爰該國視資訊安全即國安，致力於發展資訊安全產業，以禦外敵入侵，另參考以色列資訊安全政策推動分析報告[48]指出，1.資訊安全產業推動是以國家網路局為核心，協調公、私及各部門的合作，在國家資訊安全防禦機制、人才培養及建立資訊安全生態園區上，皆扮演重要的角色，負責出資、整合各部門及成立團隊。2.在國家防禦機制上，納入學術界、網路研發、防禦等領域的專家，成立國家緊急防禦團隊；資訊安全生態園區負責出資，並給予薪資補助吸引企業進駐，以及引入學術研究、政府單位進入園區。再者，本次出國考察時發現，以色列透過軍隊訓練提供資訊

[48] 資料來源：劉家委（106），以色列資訊安全政策推動分析，取自網址：https://mic.iii.org.tw/AISP/ReportS?docid=CDOC20171221003。

安全人才，在軍中依能力給予系統性之訓練，讓資訊安全觀念在學習階段即建立，從人才選測到部隊特別訓練，過程累積實戰經驗，退伍後進入資安產業。然而，我國為提升我國資訊作戰能力，國防部有相似編制，成立資通電軍，已將內部的資訊部門升級至作戰部隊層級，主要任務為電子作戰、資訊作戰、網路管理及軍線（軍用電話線）維護管理，積極整合資源、培育資通電人才，發揮領頭之前導角色，相較以色列國防結合新員選用、後備訓練、產業發展之人才流動生態系統，軍方成為科技人才及新創公司之重要孕育搖籃，其作法亦可作為參考。

(四)綜上，我國因地緣關係因素，資安領域平時即為戰時，對岸龐大網軍無時差入侵，造就國際企業願與我國資安公司合作，中央資安主管機關允宜與時俱進，持續推動符合潮流之政策，引領國內資安新創公司發展並邁向世界，提升我國資安產業質量並進及創造產值，揆諸以色列「資訊安全生態園區」，提供人才與創新科技之發展平台，作為網路資安產業之協調機構，形成產、官、學、研間之完整生態圈作法，殊值我國借鏡。

參、處理辦法：

一、函請行政院督請所屬參處。

二、通案性案件調查研究結論與建議上網公告。

三、檢附派查函及相關附件，送請交通及採購委員會處理。

調查研究委員：王麗珍

葉宜津

施錦芳

范巽綠

賴鼎銘

蕭自佑

林郁容

王美玉

中 華 民 國　　１１２　　年　　7　　月　　１１　　日