一九、量子運算及人工智慧崛起形成資安之挑戰，以及面對資安攻擊日益嚴峻，致資安風險持續攀升，允宜強化防護及人力培育措施，並儘速完備相關法令規範，以建構妥善之資安環境

隨著量子運算發展、人工智慧（artificial intelligence，AI）應用企業快速導入，以及資安攻擊日趨嚴峻，網路安全越趨複雜，風險亦大幅提高，為強化資通安全，相關部門需妥慎因應資安引發之威脅與挑戰。經查:

(一)中央政府114年度資安預算自113年度高峰下滑，各部會資安預算則各有增減

為因應全球網路攻擊頻繁及國內數位轉型需求影響，中央政府資安經費持續增加，由111年度之8億3,777萬6千元增至113年度之12億1,597萬3千元，反映政府對資安重視持續升高。然至114年度預算回落至11億4,014萬9千元(詳表1)，較113年減少7,582萬4千元，其中以國家發展委員會、內政部、國軍退除役官兵輔導委員會各減少2,171萬8千元、2,077萬1千元、1,783萬8千元為最；另法務部、行政院公共工程委員會、行政院主計總處之資安預算則各增加2,079萬2千元、830萬元、816萬1千元(詳表2)。在資安經費減少之部會中，或因系統升級或建置高峰期已過，爰回歸日常維運，惟在資安風險持續攀升下，允宜妥慎規劃，以避免因資安經費減少而影響我國長期資安防護能力。

表1　111至114年度各部會資安經費預算統計表　　單位:新臺幣千元

項目	111年度	112年度	113年度	114年度
預算數	837,776	1,020,115	1,215,973	1,140,149

說　　明：依資通安全署說明，本表格係由各機關於114年5月自行於該署系統所填報統計資料，111至113年度資料為決算數，114年度資料為預算數。政府各部門年度資安經費預算數係於當年度5月底前自行於系統填報，故尚未能提供115年度預算案數，且不含所屬機關之資安經費。

資料來源：整理資通安全署提供資料。

表2 中央政府各機關114年度資安經費預算數彙整表　單位:新臺幣千元

編號	機關名稱	113年度決算	114年度預算	編號	機關名稱	113年度決算	114年度預算
1	外交部	152,289	158,484	18	法務部	31,253	52,045
2	數位發展部	169,786	153,748	19	文化部	14,136	15,385
3	教育部	152,204	134,467	20	公平交易委員會	6,790	7,356
4	內政部	110,851	90,080	21	大陸委員會	6,747	8,942
5	國軍退除役官兵輔導委員會	64,597	46,759	22	行政院	12,625	12,287
6	經濟部	69,376	73,819	23	國立故宮博物院	11,290	3,284
7	勞動部	47,703	42,846	24	金融監督管理委員會	11,228	10,460
8	國家發展委員會	47,438	25,720	25	海洋委員會	11,755	13,841
9	行政院人事行政總處	41,749	35,609	26	中央選舉委員會	3,878	5,328
10	國家通訊傳播委員會	45,658	35,666	27	農業部	18,250	14,163
11	中央銀行	37,904	41,532	28	僑務委員會	9,516	7,903
12	衛生福利部	31,236	29,399	29	核能安全委員會	5,781	6,410
13	交通部	13,453	12,084	30	原住民族委員會	5,384	5,383
14	行政院公共工程委員會	16,379	24,679	31	客家委員會	7,409	4,786
15	行政院主計總處	28,208	36,369	32	環境部	4,500	5,700
16	國家科學及技術委員會	20,220	20,220	33	國家運輸安全調查委員會	1,303	1,829
17	財政部	4,210	2,699	34	不當黨產處理委員會	867	867

資料來源：同上。

(二)近年資安法納管單位資安通報事件與113年資安稽核概況

依據數發部統計資通安全管理法[1](以下簡稱資安法)納管機關及公立學校資安通報事件，近5年公務機關及特定非公務

[1] 資安法第14條規定略以，公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；另依資通安全事件通報及應變辦法第3條及第4條規定略以，事件發生後1小時內須線上通報資通安全署，內容包括事件描述及等級評估等項目（第一至四級，依影響程度遞增，第3條)。

機關資安通報事件數呈現上升趨勢(詳表 3)，以影響程度較大之 3 級通報事件統計觀之，公務機關 3 級通報事件數由 110 年度之 27 件增至 113 年度之 244 件，114 年 7 月為 41 件，反映資安威脅呈增加趨勢，另公立學校通報事件則呈減少趨勢，其 3 級事件通報數由 110 年度之 7 件下降至 114 年 7 月之 1 件，顯示校園資安防護相對獲得有效控制。

表 3 近 5 年納管機關及公立學校資安通報事件數量統計表 單位:件

年度	公務機關與特定非公務機關					公立學校					總計
	1 級事件	2 級事件	3 級事件	4 級事件	小計	1 級事件	2 級事件	3 級事件	4 級事件	小計	
110 年度	798	106	27	0	931	6,520	6	7	0	6,533	7,464
111 年度	840	153	64	0	1,057	3,098	1	8	0	3,107	4,164
112 年度	835	176	63	0	1,074	2,501	9	5	0	2,515	3,589
113 年度	1,044	213	244	0	1,501	1,696	6	5	0	1,707	3,208
114 年(統計至7月)	679	96	41	0	816	306	8	1	0	315	1,131

說　　明:資通安全署定期辦理資通系統實兵演練，檢視受測對象之警覺性及政府機關網站系統弱點，該實兵演練於 113 年度擴大演練，並針對 GSN 網段內全國公務機關對外服務系統進行演練，因此造成資安通報事件增加。

資料來源:數位發展部提供。

另政府部門依資安法及相關法令應遵事項之落實情形，經數位部於 113 年度針對 16 個公務機關進行稽核作業,發現主要缺失如下:

1. 技術檢測：113 年技術檢測項目為「使用者電腦安全檢測」、「物聯網設備檢測」、「網域主機安全防護檢測」、「資料庫安全檢測」、「核心資通系統安全檢測」、「網路架構檢測」、「組態設定安全檢測」及「網路惡意活動檢視」等 8 項。綜整檢測結果發現，機關可精進事項包括：強化電腦組態設定、落實作業系統安全性更新、提升網站安全性、網路服務妥適區

隔、避免使用預設通行碼及定期檢視防火牆設定等。

2. 實地稽核:數發部協助各機關持續強化資通安全防護韌性,彙整 113 年資通安全稽核共同發現事項如下：

(1)策略面：部分機關業務持續運作演練未切合實際，且未妥適規劃備份資料之復原程序；部分機關資通安全政策及目標未臻妥適，或目標、指標設定過低；部分機關持續精進及績效管理機制未確實執行。

(2)管理面：部分機關未落實監督及管理委外廠商工作；部分機關未完整盤點資通系統及資訊資產、未妥適界定核心系統及系統分級；部分機關之內部稽核辦理範圍、頻率及稽核項目規劃未臻妥適。

(3)技術面：部分機關未完成全部高風險弱點之修補，或完成修補前未加強管控或採行緩解措施；部分機關資安事件通報作業仍有未符規定情形；部分機關資安防護控制措施之執行未完備。

(三)量子運算崛起、人工智慧快速導入各類產業領域，惟屢見生成式 AI 產生個資外洩事件，致資安風險持續攀升，主管機關允宜積極研謀規劃因應措施

隨著量子運算與人工智慧（AI）的快速發展，全球產業快速導入應用，資安風險也隨之增加。生成式 AI 之應用雖可提高生產效率，卻屢傳營業資料與消費者個資外洩之事件，如三星員工將機密程式碼輸入 ChatGPT 導致營業資料外洩[2]，以及 ChatGPT 將用戶資料[3]及對話紀錄[4]暴露，影響民眾隱私等事件。

---

[2] 數位時代網站，https://www.bnext.com.tw/article/75096/samsung-ban-ai-gpt-may-23（最後瀏覽日 114 年 8 月 28 日）

[3] 資安趨勢部落格網站，https://blog.trendmicro.com.tw/?p=77418（最後瀏覽日 114 年 8 月 28 日）

[4] 聯合新聞網，https://udn.com/news/story/6811/8913932（最後瀏覽日 114

這些案例凸顯AI模型易受駭客攻擊，若AI模型對於訓練及對話資料管理不善，將增資料外洩風險。

而量子運算快速發展，已引起各國政府高度關注，量子運算之特性可快速破解傳統加密方式，威脅金融、醫療等領域的資料安全。例如駭客現在蒐集各種具價值之加密資料，待量子技術成熟後再加以破解，亦稱為「先蒐集、後破解」(HNDL)風險，對此，美國國家標準技術研究所(NIST)已發布後量子密碼（PQC）標準，要求各界啟動盤點與遷移。美國政府責任署（Government Accountability Office,GAO）2025 年報告[5]指出，可破解密碼學的量子電腦最快可能在10年內出現，屆時敏感資料恐遭破解，進而影響國家安全。

我國為因應人工智慧發展之國際趨勢，自107年開始推動「臺灣AI行動計畫」，續於112年開始執行「臺灣AI行動方案2.0」，期加速實現臺灣成為全球AI新銳之願景。並於112年10月3日發布「行政院及所屬機關(構)使用生成式AI參考指引」，數發部亦研擬「公部門人工智慧應用參考手冊(草案)」，自114年1月1日起進行為期一年之試辦作業，以供各機關參考並建置AI服務。在立法方面，行政部門版本之人工智慧基本法(草案)亦於114年8月28日於行政院院會通過，將儘速送本院併委員版本審議。

在量子運算方面，據數發部陳復，因應量子電腦對現有加密系統威脅日增，該部資安署於第七期「國家資通安全發展方案(114-117年)」，將針對各國後量子密碼相關推行政策、發展

年8月28日）

[5] 美國政府責任署，https://www.gao.gov/blog/next-big-cyber-threat-could-come -quantum-computers-government-ready（最後瀏覽日114年8月27日）

情形及相關重要國際趨勢進行研究，規劃政府整體推展方式，研擬政府後量子密碼之推動策略及工作重點並將逐步推動相關作業。此外，該部為協助我國資安產業發展後量子密碼相關解決方案、推動各產業接軌國際密碼標準，該部數產署亦已發布後量子密碼遷移指引，供產業參考。

（四）公私部門對資安專業人才需求持續增加，惟政府機關資安專業人力之配置有所不足，缺額人數占比仍逾一成

隨著網路攻擊增加，公私部門對資安專業人才需求持續增長，依據資安署統計顯示，113 年中央及地方政府資安專職人員依法應配置人數 1,493 人(詳表 4)，正式人員 1,132 人，占依法應配置人數之 75.82%，非正式人員(約聘、約僱、約用及委外人員)150 人，占比 10.05%，尚有缺額 211 人，占比 14.13%，顯見政府機關資安專業人力之配置仍有所不足。

表 4 112 至 113 年中央及地方政府資安專職人員配置情形表

單位:人數；%

項目		依法應配置人數 A+B+C	正式人員 A		非正式人員 B		缺額 C	
			人數	%	人數	%	人數	%
中央政府	112 年	783	468	59.77	249	31.80	66	8.43
	113 年	764	580	75.92	124	16.23	60	7.85
地方政府	112 年	750	471	62.80	106	14.13	173	23.07
	113 年	729	552	75.72	26	3.57	151	20.71
合計	112 年	1,533	939	61.25	355	23.16	239	15.59
	113 年	1,493	1,132	75.82	150	10.05	211	14.13

說　　明：1.資料來源為各機關填報之 113 年資通安全維護計畫實施情形（截至 114 年 6 月 10 日填報情形)，惟各機關配置人員將可能於填報後隨時變動。

2.依資通安全責任等級分級辦法規定，A 級、B 級、C 級之公務機關應配置資安專職人員數分別為 4 人、2 人、1 人，本表所列為 C 級以上機關。

3.機關實際配置之資安專職人員數，倘超過法遵，則以法遵人數計算。

資料來源：資通安全署提供。

有關政府機關資安人力供不應求之改善情形，據數發部陳

復業採取以下補實（攬才）措施：(一)於公務人員高等考試增設資通安全類科，期透過考試遴選制度增加公務機關選才管道，延攬該等人才進入公務體系；(二)推動政府資安人力職能轉換訓練，協助具意願之現職公務人員參加資訊處理職系專長訓練，投入政府資安工作，供用人機關彈性補充資安人力缺口。此外，針對資安人力培育之技能與實際需求之學用落差，該部經就資安專職人員進行課程需求調查，對於「稽核實務」、「資安事件通報應變」、「資訊委外作業」等需求程度高之課程，於資安職能訓練、增能專業培訓課程中，強化該等課程之安排。另對資安技術高階菁英人才講授最新威脅趨勢及攻擊手法，並於課後辦理網威競賽等評量，俾透過功防演練以確保實戰專業能力之精進。

鑒於現行資安人力供需失衡，主管機關允宜妥為規劃資安培育課程及加強資安教育職業訓練，建置更具吸引力之職場環境，以留住吸引資安人才投入相關領域。

(五)主管機關允宜加強資安法修法溝通、及早完備法令規範，並確實執行，俾建構完善之國家資通安全環境

資安法自 108 年 1 月 1 日施行迄今尚未修正，經數發部提出資安法修正草案，已於 113 年 7 月 4 日經行政院會通過，修正重點包括明確機關權責，強化合作協力、強化納管機關資安管理及資安人員管理(支援、配置及獎懲)等項，並經本院於 8 月 29 日三讀通過，該部允宜儘速推動相關子法研修作業，以完備法令規範，建構完善之國家資通安全環境。

資安法規之制定與推動，攸關資安環境發展至為重要，為因應當前嚴峻之資安威脅，除需制定合宜之法規規範，以保障公私部門資訊安全外，尚須行政部門確實執行方能有效落實。

綜上，近年資通訊科技快速發展、量子運算及人工智慧崛起形成資安之挑戰，以及面對資安攻擊日益嚴峻、致資安風險持續攀升，行政院允宜賡續掌握資安情勢，妥慎瞭解未來資安環境所面臨之挑戰，並積極強化防護及人力培育措施，並儘速完備相關法令規範，以建構妥善之資安環境。

（分機：1913 許福添）