行政院資通安全會報第44次委員會議

資通安全業務重點工作

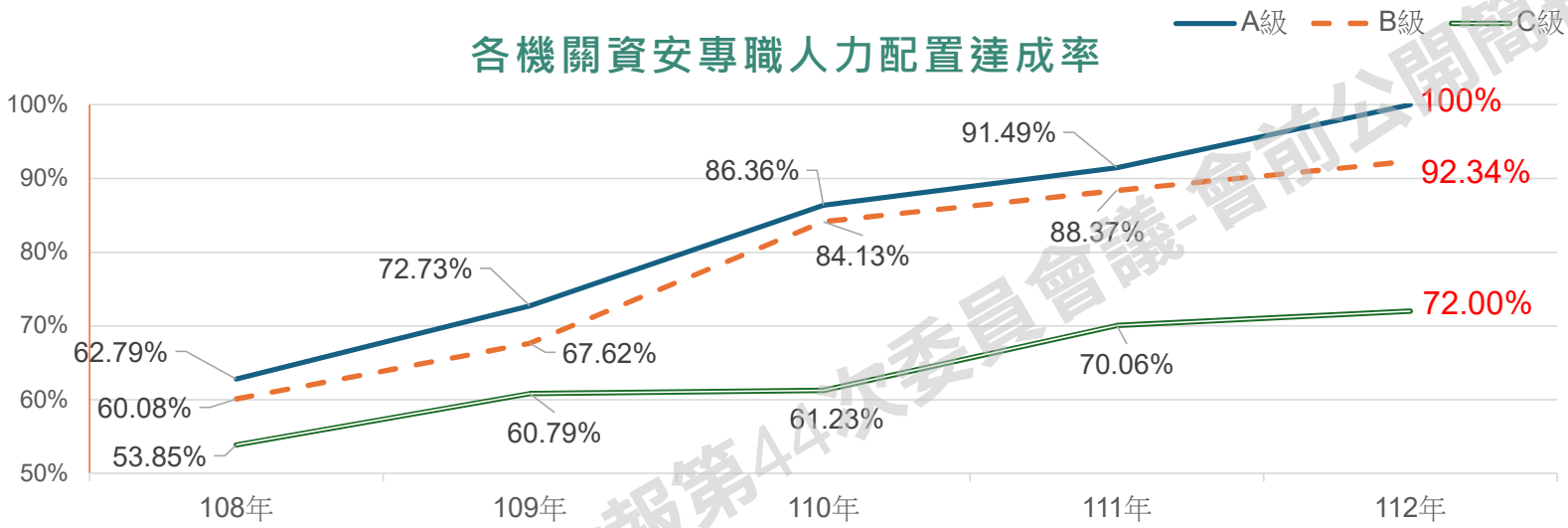
113年12月25日

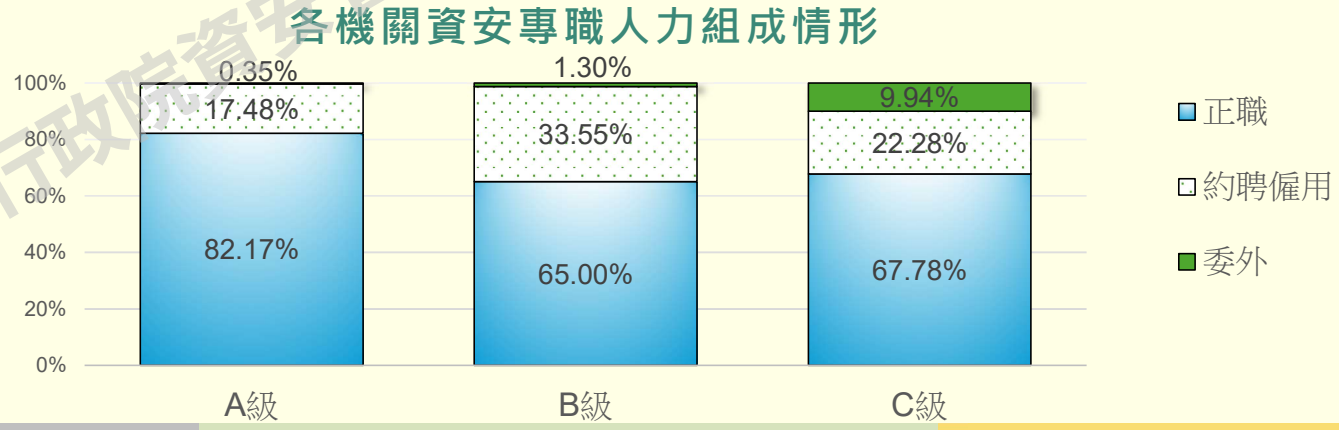
報告大綱

- 資通安全政策實施情形
- 重點工作及配合事項

資通安全政策實施情形

各機關資安人力配置情形





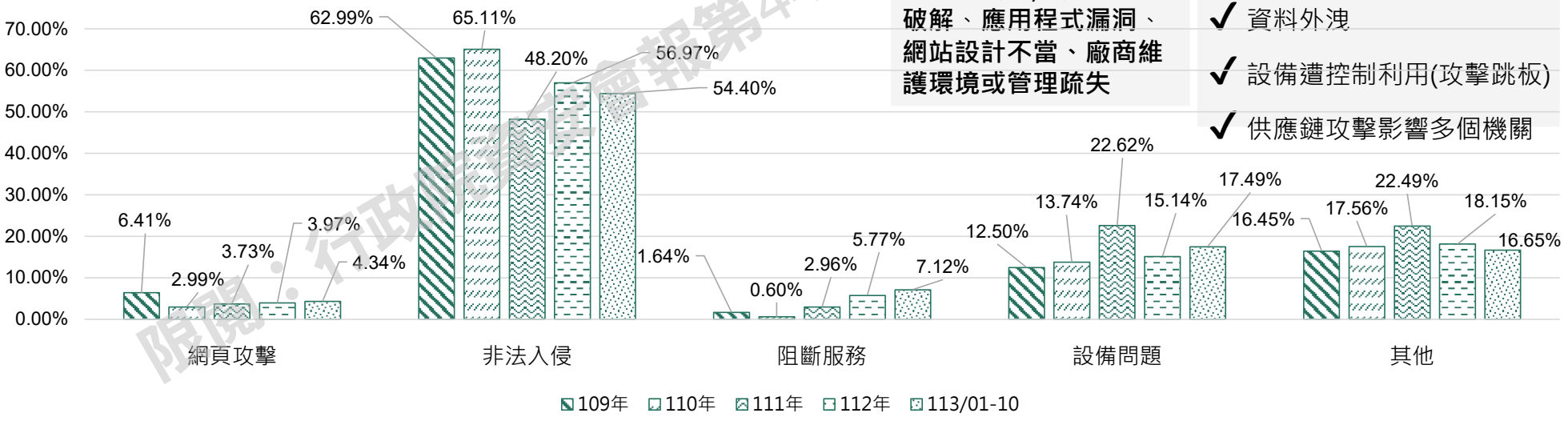
納管機關資安事件通報統計

數位發展部資通安全署
Administration for Cyber Security, moda

(統計範圍及對象：資安法納管對象不含實兵)

年度	事件數	1級事件	2級事件	3級事件	4級事件
109年	608	502	85	18	0
110年	837	719	96	20	0
111年	765	608	120	37	0
112年	830	655	149	26	0
113年1-10月	829	676	138	15	0

註：113年統計至10月31日

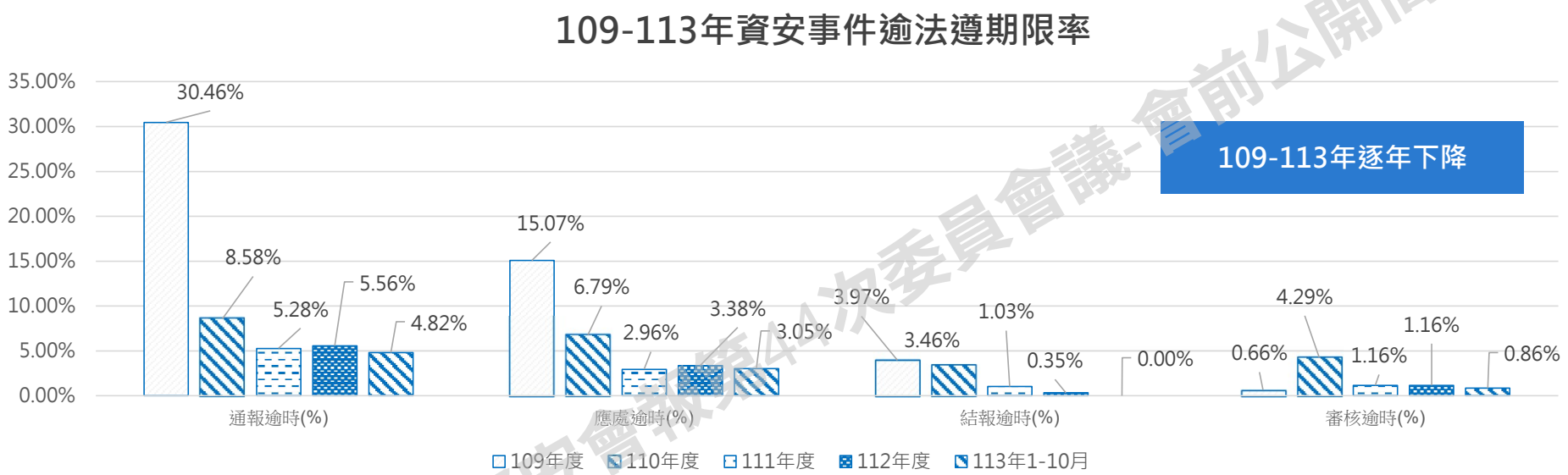


非法入侵為大宗主因：
多為**弱密碼/密碼遭暴力破解、應用程式漏洞、網站設計不當、廠商維護環境或管理疏失**

可能造成衝擊：

- ✓ 資料外洩
- ✓ 設備遭控制利用(攻擊跳板)
- ✓ 供應鏈攻擊影響多個機關

資安事件通報應變逾時情形



逾時原因

1. **未有法遵意識**如應處完成後才進行通報
2. 業務人員異動，**未落實業務交接**
3. **不熟悉**通報應變網站操作
4. **未落實代理人制度**

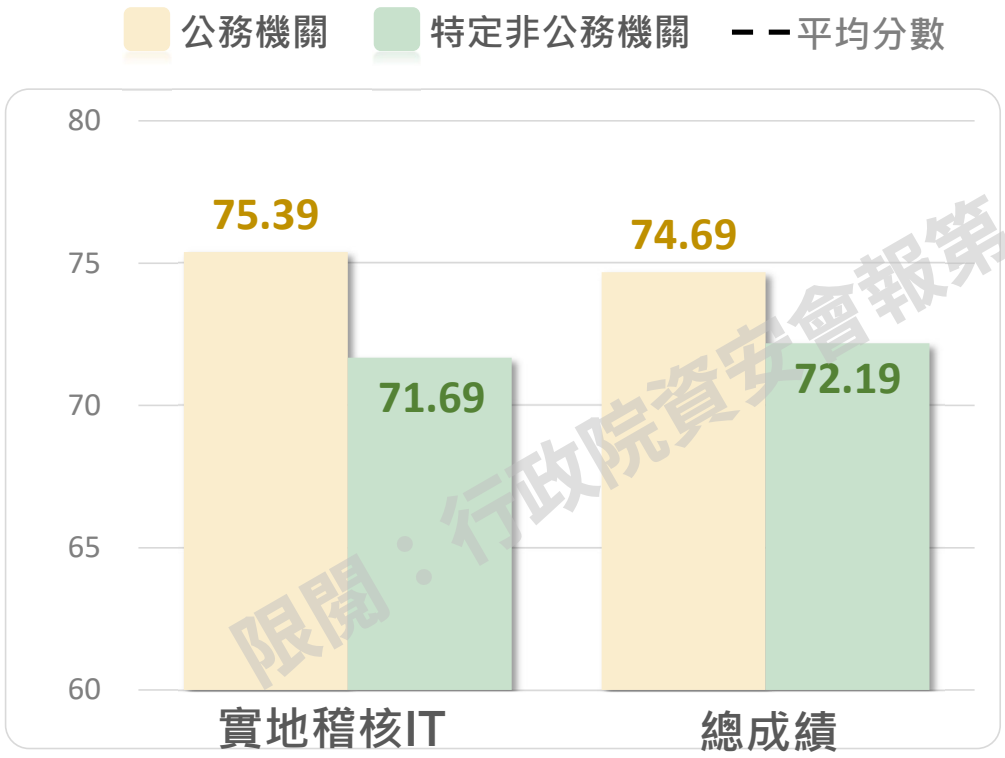
建議措施

1. **加強法遵意識**
2. **落實職務異動交接**
3. **可參考網站操作手冊及落實教育訓練**
4. **落實代理人制度**

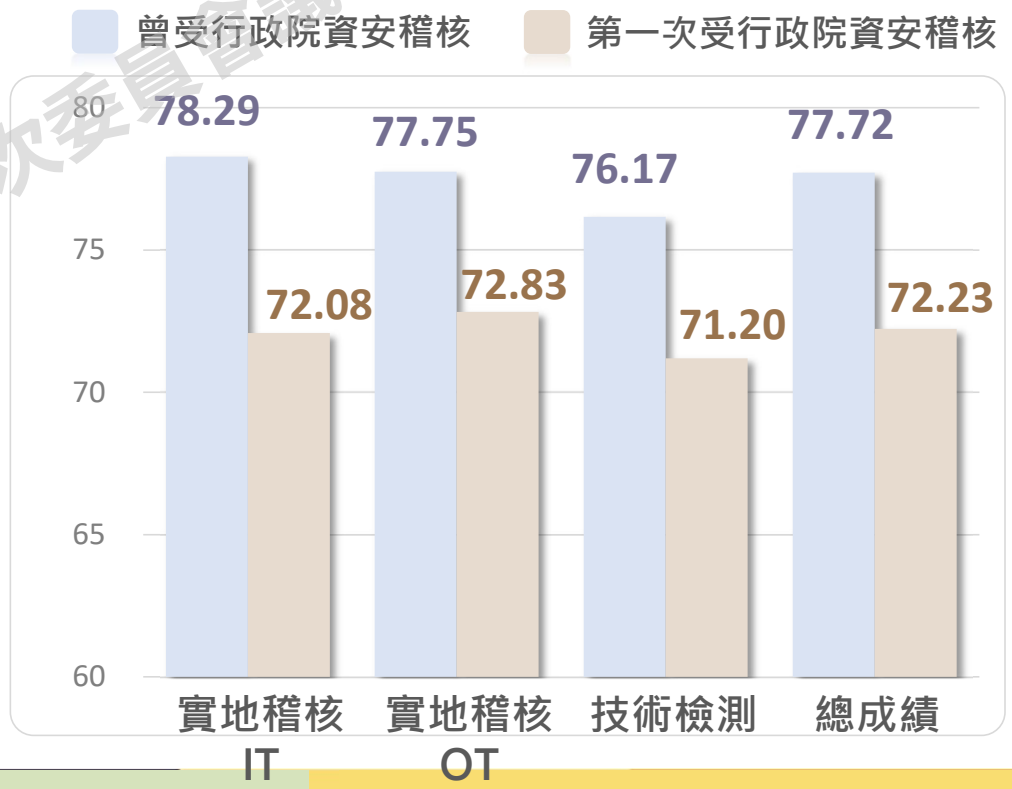
113年行政院資安稽核結果(1/2)

- 113年實地稽核 **40個** 機關

公務機關整體表現優於特定非公務機關



曾受行政院資安稽核機關整體表現優於第一次受稽機關



113年行政院資安稽核結果(2/2)

- 共通性發現

策略面
- 業務持續運作**演練**未切合實際
- 未落實持續**精進**及**績效**管理
- 資通安全**政策**及**目標**未臻妥適

管理面
- 未落實**委外管理**
- 未完整**盤點**資產、未妥適系統分級
- **內部稽核**規劃未臻妥適

技術面
- 未落實**弱點修補**
- 資安事件**通報**未符規定
- 未落實資安防護**控制措施**

OT
- 未完整**盤點**資產
- 未落實資安防護**控制措施**
- 未落實系統**帳號**管理

資安法各子法草案修正重點

資安法修法(母法):

- **(預估)113年12月立法院三讀通過**
- **(預估)114年1月總統公布**

序	類型	法規名稱	修正重點
1	修正	資通安全管理法施行細則	1.修正委外人員適任性查核準用規定 2.定明母法第14條無上級機關提出稽核改善報告執行情形。
2	修正	資通安全責任等級分級辦法	1.修正責任等級提報流程及核定依據 2.特定類型防護基準擴大適用 3.附表修正、應辦事項法遵期限調整
3	修正	資通安全維護計畫實施情形稽核辦法	定明資安署、上級機關、中央目的事業主管機關稽核相關事項。
4	修正	資通安全事件通報及應變辦法	1.權責機關調整 2.演練作業調修 3.特非機關資安事件等級審核作業調整
5	修正	資通安全情資分享辦法	權責機關調整
6	修正	公務機關所屬人員辦理資通安全事項管理辦法	定明**調度支援**、適任性查核、職能訓練規定
7	新增	危害國家資通安全產品情資審查及分享程序辦法	**定明危害產品審查作業及情資分享程序**
8	新增	國家資通安全會報設置辦法	定明國家資通安全會報組織入法

資安國際交流

➢ 前瞻資安探索會議 ACE

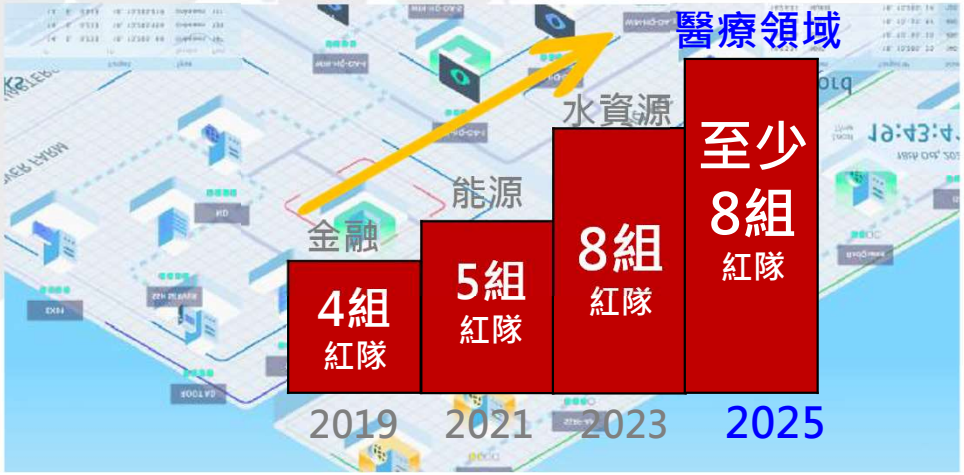
Advanced Cybersecurity Exploration Conference

- 本年12月9日至11日舉辦(第2次)
- 邀請至少16個**國家**及**國際組織**
- 國內產官學**資安專家**
- 聚焦**網路韌性**及**資安治理**

➢ 跨國攻防演練 CODE

Cyber Offensive and Defensive Exercise

- 2025年舉辦
- **實兵演練**OT系統 (醫療領域)
- **即時**紅藍隊攻防對抗
- 國際**資安專業技術**與**應變能力**交流平台



擴大政府資安人力進用管道

人力進用策略

非資訊處理職系現職公務人員轉任

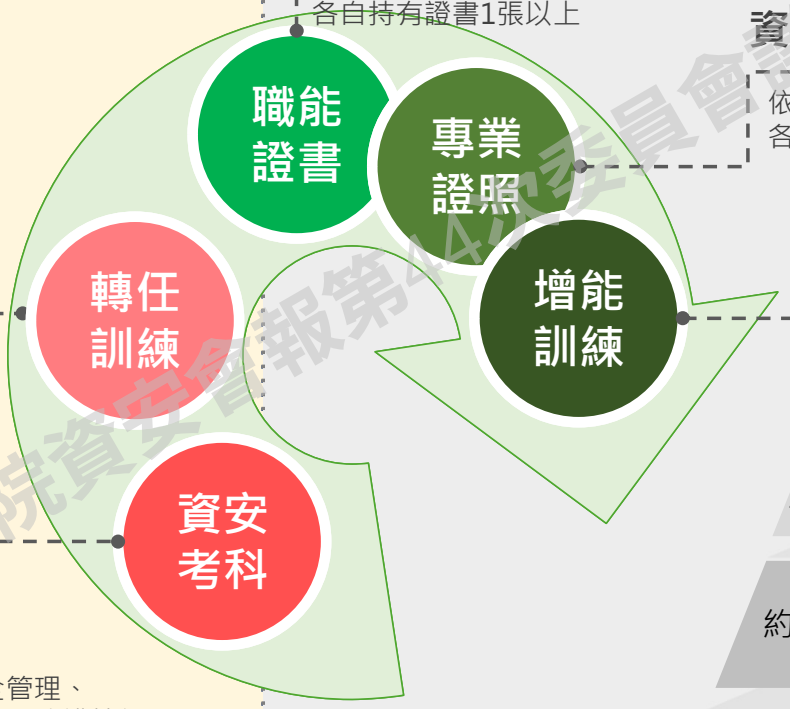
目標培訓1,000人，優先投入政府資安工作

政府資安人力職能轉換訓練計畫

高考三級新增資通安全類科

透過國家考試取才

包含資通安全概論、資通安全管理、資通安全法令與規範、資通安全防護技術等4科專業科目



人才培訓規劃

資安職能訓練證書

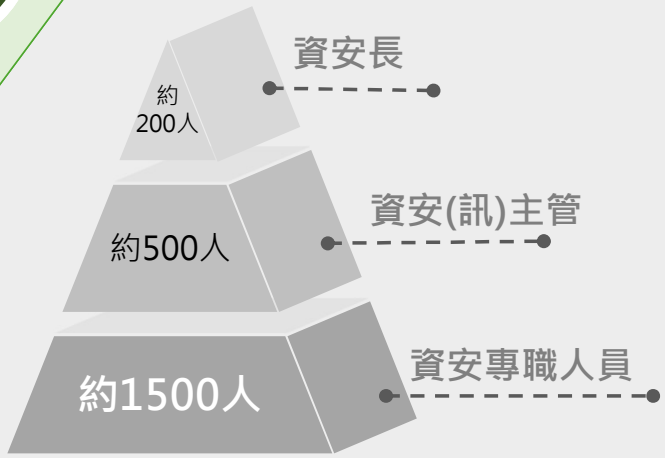
依資安法規定，資安專職人員應各自持有證書1張以上

資安專業證照

依資安法規定，資安專職人員應各自持有證照1張以上

資安增能訓練

依資安法規定，資安專職人員每人每年應至少接受12小時以上專業訓練



政府採購供應鏈資安管理_數產署

行動應用App資安認驗證機制

建立機制

數產署參考國際標準，訂定並推動「行動應用App基本資安自主檢測推動制度」，引導並鼓勵行動應用App開發商及平台業者自主管理，透過公正的第三方檢測實驗室進行App資安檢測。

App資安業務分工*

政府機關開發之App資安	數發部數政司
手機出廠內建軟體(App)資安	數發部韌性司
特定領域App資安 (如網銀、健康照護)	各目的事業主管機關
共通性非特定領域App基礎安全	數發部數產署

*註: 依行政院國家資通安全會報103/6/24第26次委員會議決議

IoT設備資安產業標準認驗證機制

106年起由經濟部與國家通訊傳播委員會齊力推動「物聯網設備資安產業標準與檢測認驗證」，於111年部會組織改造後，數產署主責推動具有線介面之物聯網終端產品資安檢測。

應用系統	涵蓋範圍	國家標準採用情形
共通指引	物聯網設備共通資安指引	
影像監控系統	網路攝影機、影像錄影機、網路儲存裝置、監控平台共4項	108/11/29「影像監控系統 系列標準」由經濟部標檢局公告為國家標準(CNS 16120)
智慧巴士資訊系統	巴士車載機、智慧站牌共2項	113/6/13「智慧巴士資訊系統系列標準」由經濟部標檢局公告為國家標準(CNS 16230)
智慧路燈系統	智慧路燈及智慧照明共2項	已函送經濟部標檢局作為國家標準制定參考
消費性網路攝影機	消費性網路攝影機共1項	已函送經濟部標檢局作為國家標準制定參考
感測裝置	空氣品質微型感測裝置、聯網型地震儀、水位計共3項	已函送經濟部標檢局，刻正進行國家標準審查程序
門禁系統	門禁管理平台、門禁閘道控制器、門禁讀取器、智慧門鎖及人臉辨識門禁裝置	112/10/27「門禁系統系列標準」由經濟部標檢局公告為國家標準(CNS 16217)

網際網路內容管理基本規範及分工原則-通傳會

➢ 宗旨

釐清中央各主管機關對於**網際網路內容相關權責分工**，並提高政府行政效能，及時處理民眾相關疑義。

➢ 管理方式

為統一事權，網路內容管理所衍伸爭議比照**實體社會**，原則由實體社會之**各目的事業主管機關**依其主管之作用法處理。(表二 中央各主管機關對於網際網路內容管理權責分工表)

- **農業部**依野生動物保育法，處理**網路交易**陸域保育類野生動物及產製品相關事宜。
- **交通部(觀光署)**管理**國外訂房網站**服務管理問題，例如：agoda、booking.com、trivago等。

表二：中央各主管機關對於網際網路內容管理權責分工表

主管機關	相關權責
各中央目的事業主管機關	消費者保護相關事項。
內政部	一、警政署：依據警察法及刑事訴訟法相關法令，查緝於透過網路途徑實施之犯罪行為（如：詐欺/騙；散布、播送或販賣猥褻物品；販售毒品、槍砲彈藥/含教學；販售贓物；教唆或幫助他人自殺；賭博；妨害電腦使用罪；違反兒童及少年性剝削防制條例等）。 二、移民署： （一）跨國（境）婚姻媒合廣告； （二）揭露人口販運受害者身分資訊。
衛生福利部	一、保護服務司： （一）揭露性侵害、性騷擾或兒少性剝削受害者身分資訊；

行政院國家資通安全會報-各組運作情形

網際防護體系						網際犯罪偵防體系	
關鍵資訊基礎設施安全管理組 (資安署)	**產業發展組** (數產署)	**資通安全防護組** (資安署)	**法規及標準規範組** (資安署)	**認知教育及人才培育組** (教育部)	**外館網際防護組** (外交部)	**防治網路犯罪組** (內政部/法務部)	**資通訊環境及網際內容安全組** (通傳會)
111年11月28日、112年12月25日、113年6月19日、113年12月5日定期召開「**國家資安資訊分享與分析中心(N-ISAC)年會**」，邀請會員分享資安威脅趨勢及實務案例、安排模擬情資實作。	配合國發會、國科會、資安署等機關管考，定期回報推動資安產業發展之辦理情形，或奉派至行政院國家資通安全會報委員會議報告。	111-113年分別辦理23場、40場、40場「**行政院資安稽核**」，督導落實資安法遵事項。 112年辦理「**網路攻防演練**」(受測機關95個)，督導落實資安防護及通報應變。另，辦理4場次「**跨國網路攻防實兵演練(CODE)**」。	「**資通安全管理法**」**113年7月4日行政院會通過函請立法院審議，7月12日一讀會交付委員會審查中** 增修資安相關等3份參考指引。	刻正規劃於明(114)年1月至2月召開會議。	111年6月7日、112年4月24日、112年12月27日、113年7月30日、113年12月18日定期召開會議，討論「**外館網際防護組作業規範**」等法規相應條文修正事宜。	111年6月27日、111年6月27日、112年6月28日、113年1月25日、113年9月4日定期召開會議，並以**跨部會協商平臺**名義，邀請相關部會進行報告，並安排綜合討論。	111年4月14日、112年12月7日、113年9月5日定期召開會議，進行**網路內容防護機構(iWIN)**工作成果報告，並討論「**網際網路內容管理規範及分工原則**」修正事宜。

近期政府機關資安案例

帳號盜用遭點數異常兌換

- 近期○○公司發現部分○○會員帳戶遭異常兌換，經調查局追查，發現駭客購買大量外洩帳密後，**採「撞庫攻擊」**盜用點數兌換商品券，於購買商品後變賣牟利。

建議防範措施

1. 使用者經常在多個帳戶採用相同密碼以利管理，因此應**定期更新密碼**、**增強密碼強度**，並且避免在不同平臺間使用相同之帳號與密碼，遭撞庫攻擊與盜用。
2. 系統方面，建議強化使用者登入機制，如系統要求使用者**設置強密碼**、**採多因子驗證**、**限制登入次數**等防範措施，以提升系統使用安全。

FB粉絲專頁遭盜用

- 機關FB粉絲專頁遭盜用，經查該專頁管理者為在職員工申請之**私人帳號**，未妥善管理帳號遭盜用(機關已向Meta申訴處理)。

建議防範措施

- 建立**社群平臺帳號管理機制**並**定期審核與帳號清查**，範圍包含機關自建系統、社群平台(FB、IG等)、網站平台(協作平台、blog等)。
- **避免使用弱密碼**，啟用**雙重驗證機制**，並定期更換密碼。
- 定時檢視登入紀錄是否有異常情形。
- 人員異動(離職)**應移除帳號權限**。

帳號盜用佐證建議作法

1.至FB官方網頁依指引**取回帳號**(https://s.moda.gov.tw/j9jav2Urbi27)

2.**下載登入紀錄方式**(報案佐證)

1) 登入狀態下進入
https://s.moda.gov.tw/CitLheAbVVZA

2) 選擇「帳號安全和登入資訊」，將「你登入的位置」或「登入和登出」中遭盜用時段的登入紀錄畫面擷圖

重點工作及配合事項

114年行政院資安稽核規劃預告

- 以資安法施行後未受稽核之A級機關為優先
- 以行政院所屬2級機關之稽核頻率2年1次為原則
- 參考EASM檢測結果

受稽機關遴選機制

檢核項目調修

- 配合資安法修法通過調修查核項目
- 參考ISO/IEC 27001:2022控制項調修查核基準

- 參考ISO/IEC 17021及27006規範精神，訂定委員遴選原則
- 增加CI領域委員

稽核委員遴選機制

觀察員培訓機制

- 113年觀察員參加實習階段
- 114年觀察員參加見習階段

加速增補資安人力

透過現職公務人員轉任

鼓勵

- **鼓勵現職公務員參加專長訓練課程**
  非資訊處理職系轉任，完訓後**得優先於原機關服務**

放寬

- **放寬徵人條件**
  公務人員高等考試三級或相當等級之特種考試及格，**具資訊處理職系任用資格** (X經銓敘審定合格實授)

盤點

- **盤點機關內部之員額**
  檢視與釋出機關內部員額，將其**調整為資訊處理職系**職缺

透過國家考試進用

報缺

- **評估「資通安全」類科報缺**
  循程序**依需提報**高考三級「**資通安全**」類科職缺

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理