資通安全業務重點工作

數位發展部資通安全署
112年12月14日

大綱

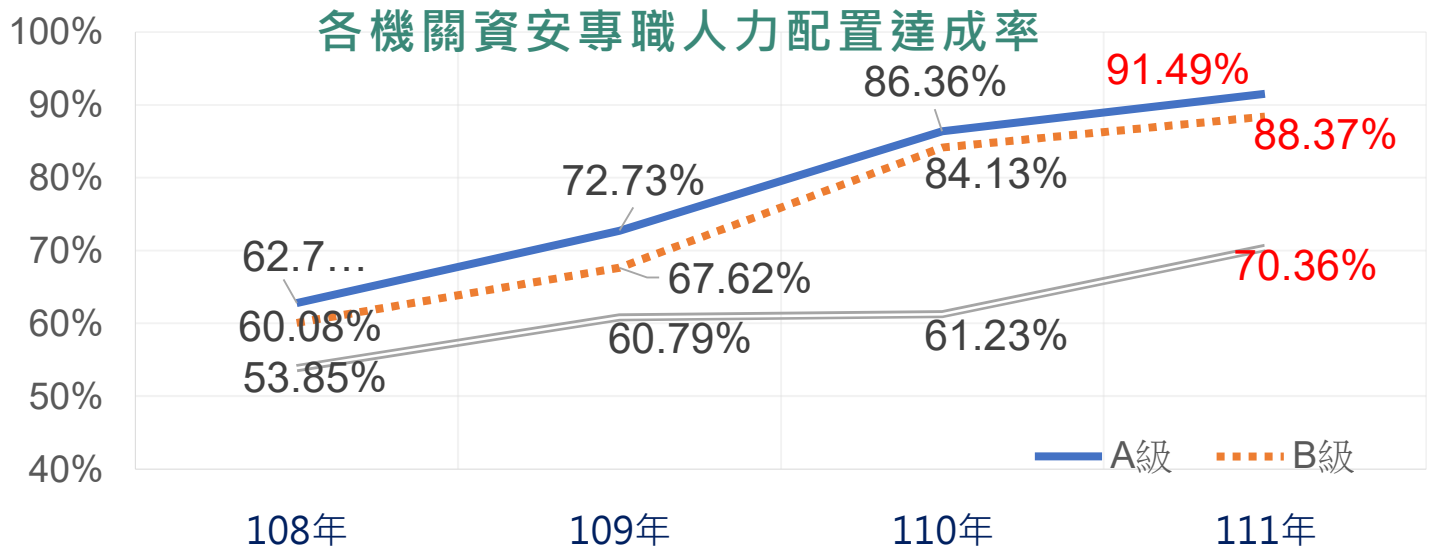
1、資通安全政策實施情形

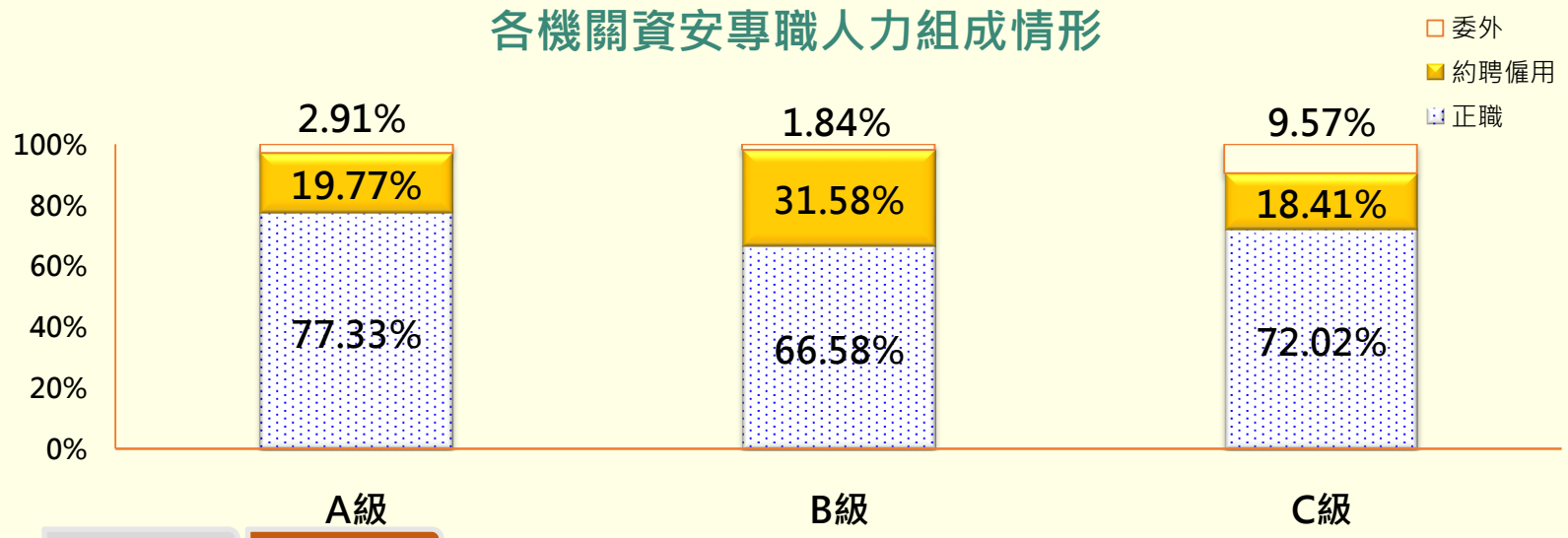
2、近期政府機關資安案例

3、重點工作及配合事項

1、資通安全政策實施情形

各機關資安人力配置情形





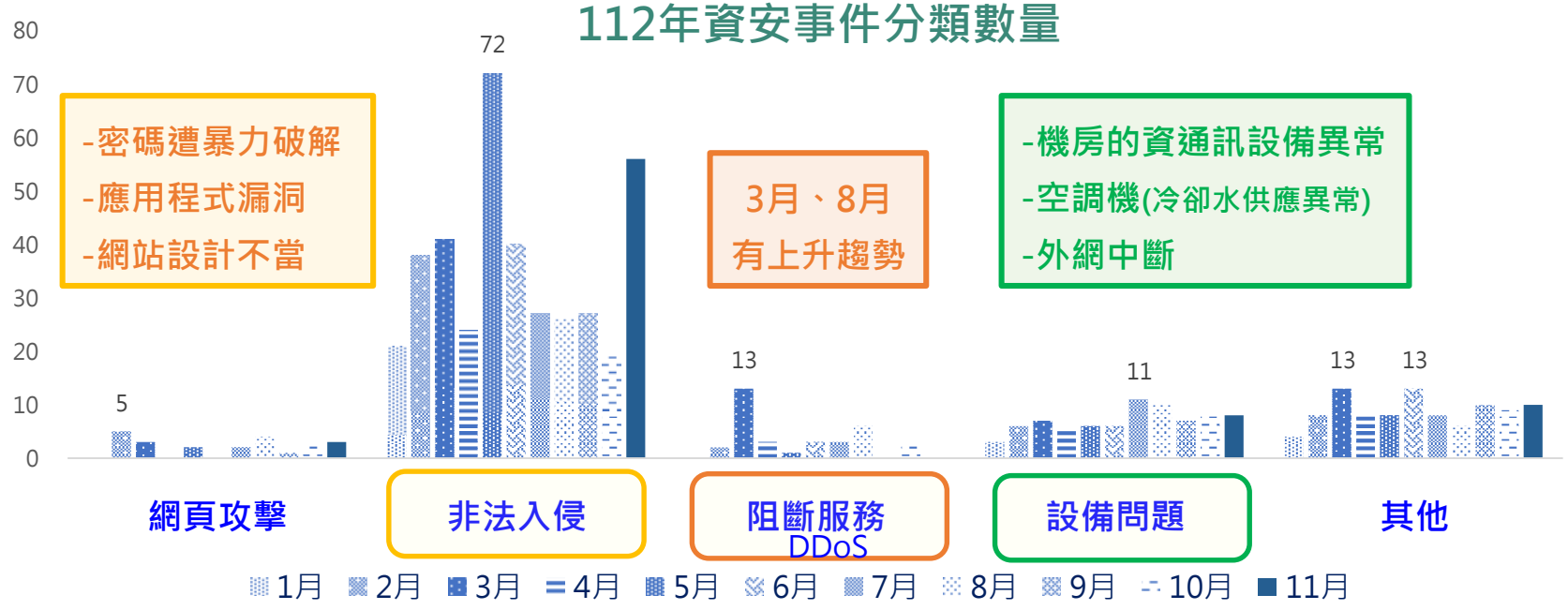
等級核定 實施情形

公務機關資安事件通報統計

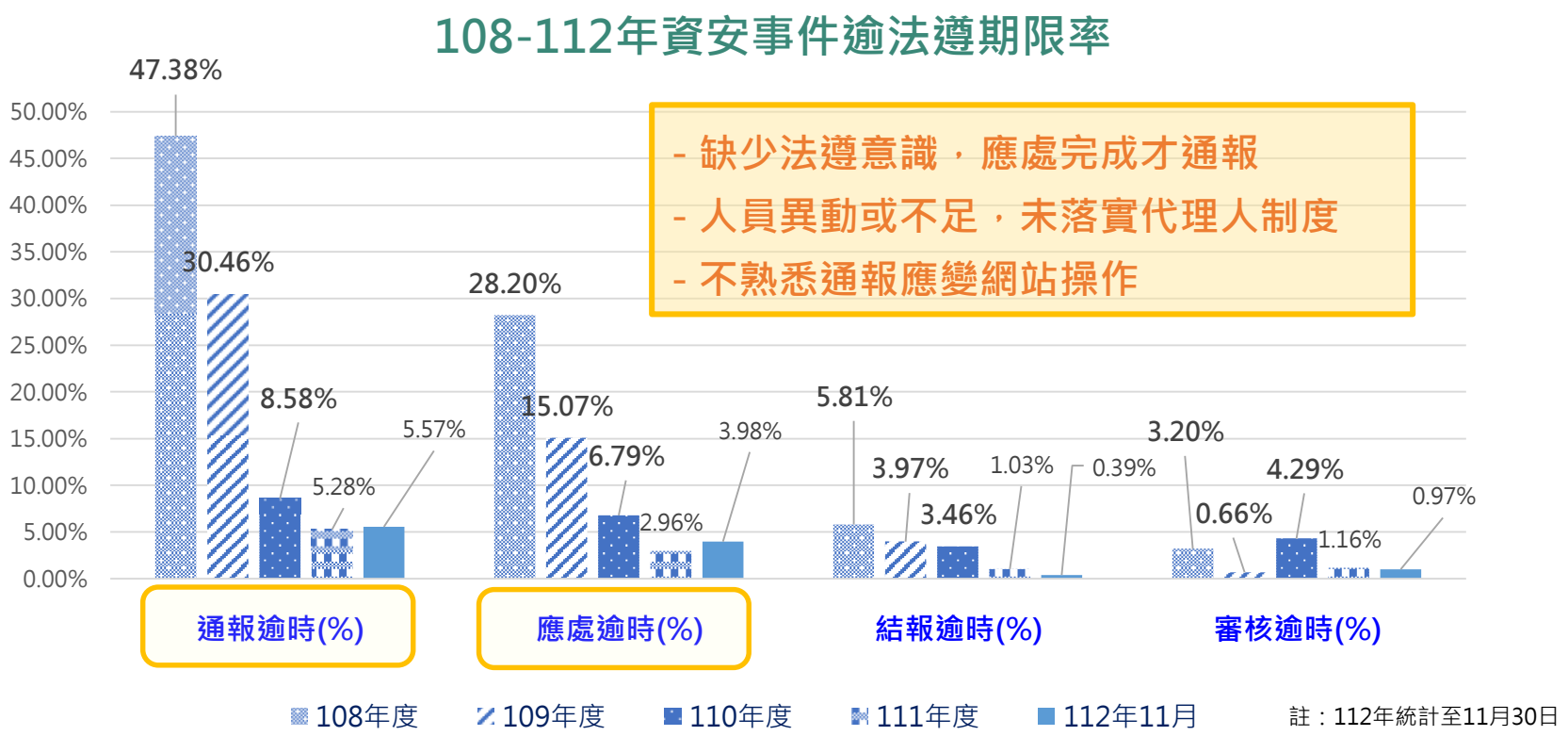
年度	事件數	1級事件	2級事件	3級事件	4級事件
108年	310	254	45	11	0
109年	525	451	65	9	0
110年	696	619	66	11	0
111年	557	453	94	10	0
112年(註)	622	507	101	14	0

註：112年統計至11月30日

112年資安事件分類數量



112年資安事件通報應變逾時情形



	事件通報	應變處置	結報 (提交調查、處理及改善報告)	完成審核 (上級或監督機關)
起算時間點	知悉事件	知悉事件	完成應變處置	接獲通報
1、2級事件	1小時	72小時	1個月內	8小時
3、4級事件		36小時		2小時

行政院資安稽核及網路攻防演練

年度	行政院資安稽核	網路攻防演練
111年	**23場次** 行政院所屬機關、特定非公務機關	**66個機關** 含44個A級機關+22個地方政府
112年	**40場次** 稽核量能提升， 增加行政院所屬三級以下A級機關	**91個機關** 含47個A級機關+22個地方政府+3個三級事件機關+19個行政院所屬中央二級機關(B級、C級)
	40場次 關鍵基礎設施安全檢視	
113年	**規劃50場次** 配合法規調修，評估增加場次 並持續辦理關鍵基礎設施安全檢視	**90個機關** 含49個A級+22個地方政府+19個行政院所屬中央二級機關(B級、C級) **+GSN範圍內滲透測試**

- ✓ **稽核項目因應作業重點滾動修訂。**
- ✓ **共通發現於政府資通安全巡迴研討會說明。**

資安法修法期程及進度

全面檢視現行法規

專家研議

專家共同討論及法律意見書

部會協力

3~5月
機關意見回饋

凝聚共識

8~9月
6場修法工作坊

公民參與

9~11月
「公共政策網路參與平臺」徵詢民眾意見

10~11月
16場修法說明會
廣徵各界意見

WE ARE HERE

草案調修

數位部

法案審查

行政院

院會審查

立法院

審議

12月

計有1778人參與、
提出691則意見。
刻正綜整研析、
調修資安法草案。

資安法草案重要議題

具共識議題

- ✓ **主管機關調適**
- ✓ **國家資安會報設置入法**
- ✓ **明定資通安全維護計畫實施情形提出之對象**
- ✓ **特定非公務機關應置資安長、設置資安專職人員**
- ✓ **增訂中央目的事業主管機關行政調查之權限**(強化重大資通安全事件應處)
- ✓ **統籌培訓公務機關資安人力，互相支援**(重大資安事件)

意見不一

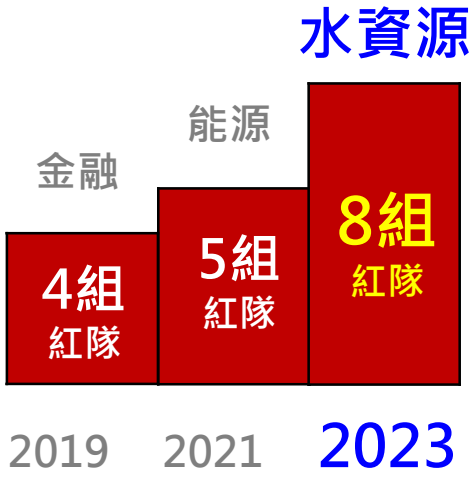
- ◆ **限制及使用危害國家資通安全產品入法**
  - 產品清單之認定
  - 公私部門皆要求公布產品清單
  - 恐涉及經貿議題、訴願及國賠等
- ◆ **主管機關公告關鍵基礎設施提供者(CIP)之指定基準、廢止條件及程序入法**
  - 依行政院「國家關鍵基礎設施安全防護指導綱要」，CI防護工作相關資訊應保持機敏性
  - 108年及110年已指定程序完成CIP之核定，納入資安法適用範圍

資安國際交流

● 跨國攻防演練 CODE

Cyber Offensive and Defensive Exercise

- ✓ **實兵演練**OT系統 (非情境式)
- ✓ **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



● 前瞻資安探索會議 ACE

Advanced Cybersecurity Exploration Conference

- ✓ 來自**18國**國際資安組織
- ✓ 分享**地緣政治與新興威脅**、**網路安全重要性**、風險管理政策等議題

2、近期政府機關資安案例

勒索病毒攻擊風險增加

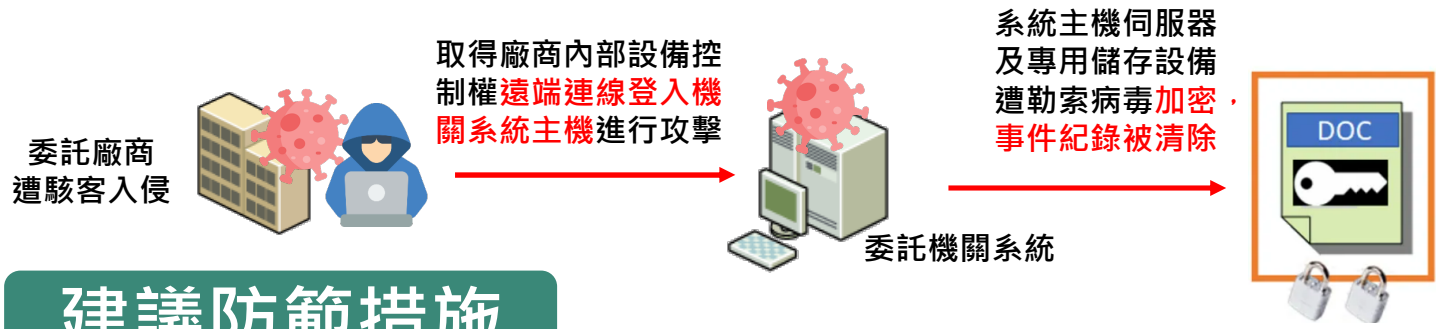
- 機關A疑似透過**社交工程郵件感染勒索病毒**，以致**內部系統或主機資料遭加密**，造成機關服務受到影響，又因該體系網路互通，進而發生**橫向**擴散情事。
- 機關B內部系統因**弱密碼**導致遭駭客破解，並成功入侵植入**勒索病毒**，又機關內部未做網段區隔，導致橫向擴散至其他系統及OA辦公主機，影響造成機關營運影響。

建議防範措施

- 加強內部同仁資安觀念，**勿瀏覽不明網頁或點擊惡意連結**
- 系統密碼應落實**GCB**密碼複雜度等身分驗證管理機制。
- **定期**執行資料**備份**(離線備份)及異地備份(**3-2-1備份原則**)，以確保營運不中斷。
- 妥適網路**區段分割**，限縮受影響範圍。

供應商遠端連線議題

- 機關委託廠商之內部主機，遭攻擊者取得設備控制權，以遠端登錄連線機關系統作業主機進行攻擊，因遠端連線僅**需登入帳號密碼，未有其他驗證機制**，致機關系統主機伺服器及專用儲存設備遭勒索病毒加密，事件紀錄被清除。



建議防範措施

- 遠端連線**原則禁止，例外允許**，原則以**短天期**為限，並建立異常行為管理機制
- 採**VPN、SSH等加密**方式進行遠端連線
- 建議採行**雙因子**認證機制
- **落實委外廠商管理**，必要時進行資安查核

網通設備產品漏洞攻擊

- C牌網通設備存在高風險安全漏洞(CVE-2023-20198)，此**漏洞CVSS風險評分高達10分**，允許遠端攻擊者在未經身分鑑別情況下，建立具有最高權限等級帳戶，取得受影響系統之控制權。若啟用網頁介面(Web UI)功能皆會受到影響，包含交換器、無線網路控制器、無線基地台及路由器等。
- 經調查已有機關疑似有被漏洞利用並侵入跡象(10/19發INT警訊)，以及網通設備存在該漏洞(10/19發EWA警訊，未遭駭)，**112年10月20日全面發送ANA漏洞警訊，提供緩解措施供機關應處。**

建議防範措施

- 官方112年11月18日已發布修補更新，**請儘速完成更新**
  https://s.moda.gov.tw/i2TPkMAoVsuL
- 若無法完成更新，可先進行緩解措施關閉HTTP Server功能
  https://s.moda.gov.tw/r2NNZ4D41MSt
- 落實系統廠牌盤點，掌握機關內部所管設備資訊。
- **關注資通設備漏洞資訊及本署發出設備漏洞情資，盡速應處**

機關經營公務社群平台帳號管理

- 機關FB粉絲專頁圖片遭到置換，經同仁發現後立即將圖片下架，後續調查發現應為**離職員工之帳號密碼外洩**導致被盜用。
- 機關FB粉絲專業管理人員因**誤點社交工程郵件**，導致管理者帳號密碼被盜取，該機關因辦理活動，粉專私訊對話內留有民眾報名個資，故有個資外洩之疑慮。

建議防範措施

- 機關應建立**帳號管理機制**，落實帳號申請、建立、修改、啟用、停用及刪除之程序，並**定期審核**，**不限於機關自建系統**，應包含：**社群平台**(FB、IG、Youtube等)、**網站平台**(協作平台、blog等)，並建立**複雜性密碼**(勿用懶人密碼)。
- 人員若有異動**(離職)**應將帳號**停用或刪除**。
- 加強內部同仁資安觀念，勿瀏覽不明網頁或點擊惡意連結

3、重點工作及配合事項

資通安全業務績效評核及獎勵

機關	人員
資通安全責任等級B級以上 **公務機關、直轄市及縣(市)政府**	資通安全責任等級C級以上 公務機關的**資安專職人員**

評核項目

- ✓ 資通安全管理法法遵應辦事項執行情形
- ✓ 資通安全管理作業執行情形
- ✓ 其他資通安全管理業務促進活動或特殊創新作為

法遵落實

創新作為

獎勵方式

視評核結果，得頒發獎座(牌)、獎勵金

獎勵對象

資通安全長、資安(訊)主管及主要人員

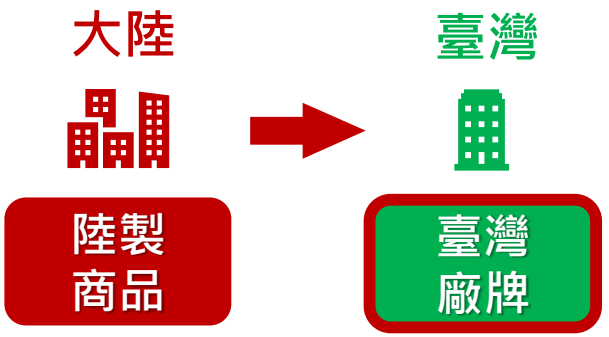
不含 數位發展部、資通安全署、數位產業署、國家資通安全研究院

限制使用陸牌資通產品處理情形

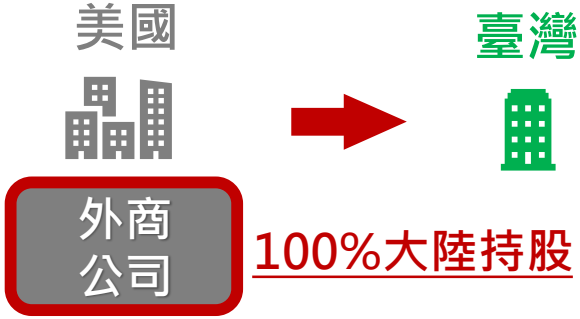
盤點結果

- ✓ 使用大陸廠牌資通訊產品之汰換率 61%，所餘279個皆要求機關加強資安管控作為，並儘速汰換。
- ✓ 經雙資安長同意並報核准使用計有 5個機關。

存摺印表機&智慧黑板



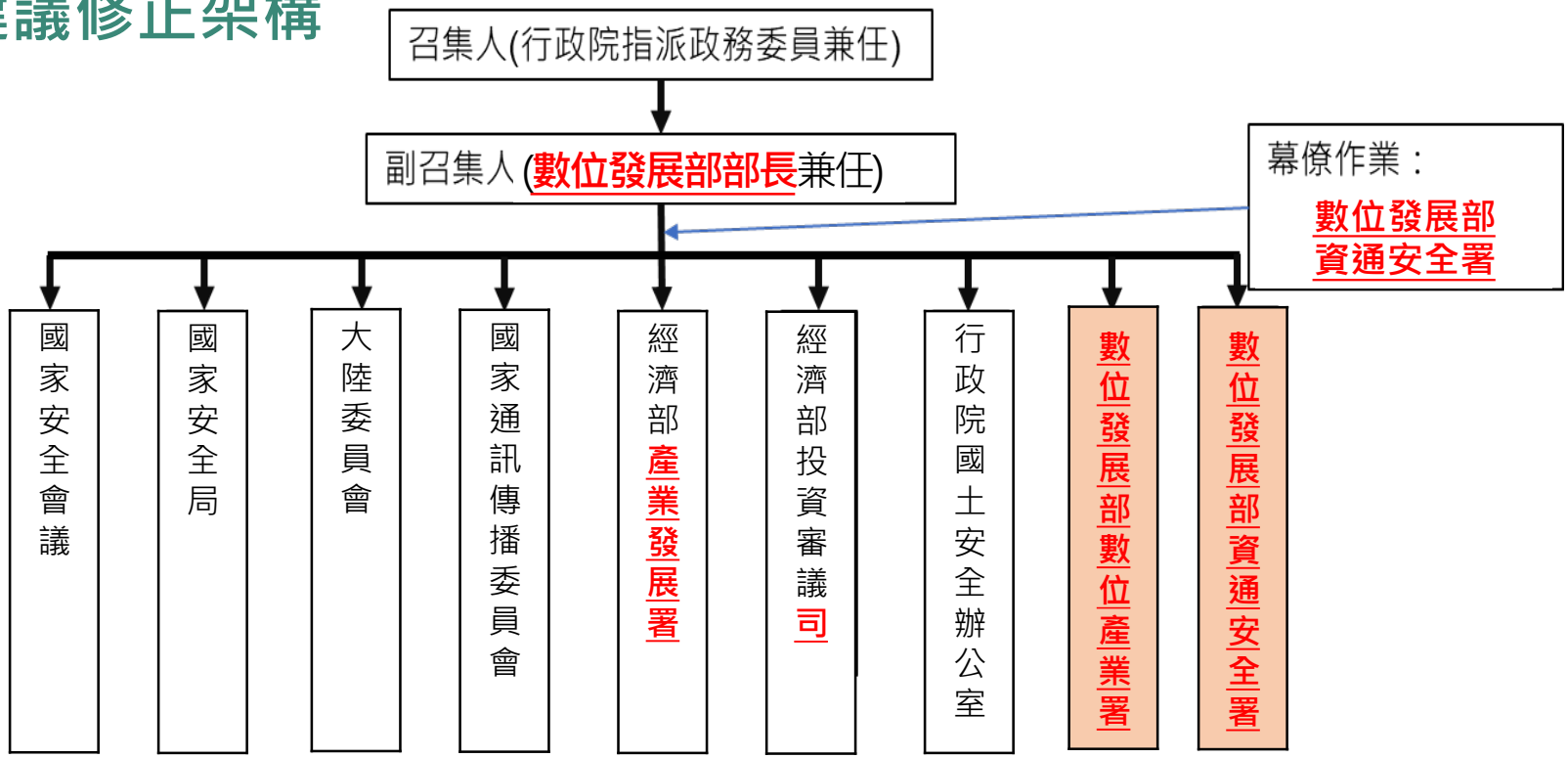
無人機



採購資通訊產品時，須請廠商說明其與大陸關聯性

危害國家資通安全產品審查小組

- 建議修正架構



- ✓ 配合組改，目前規劃增修如**紅色**標記，後續辦理院簽作業
- ✓ 未來將視議題需要，邀請相關單位參加，請各部會配合

重點注意事項

- 加強內部同仁資安觀念，勿瀏覽不明網頁或點擊惡意連結，落實**備份**機制及**網段區隔**。
- 落實資訊作業委外資安管理，遠端維護作業應採**原則禁止、例外允許**，如需開放應以**短天期**為限，並建立連線行為管理機制。
- 關注資通訊設備漏洞情資(漏洞資訊、零時差攻擊)，適時**更新韌體版本**或採必要之防護設定。
- **社群平台**應建立並落實**帳號管理機制**，設定**複雜性密碼**。
- 採購資通訊產品時，請廠商說明其與大陸關聯性**(如公司持股、產品的生產/設計/製造)**

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