行政院第3574次會議會後記者會

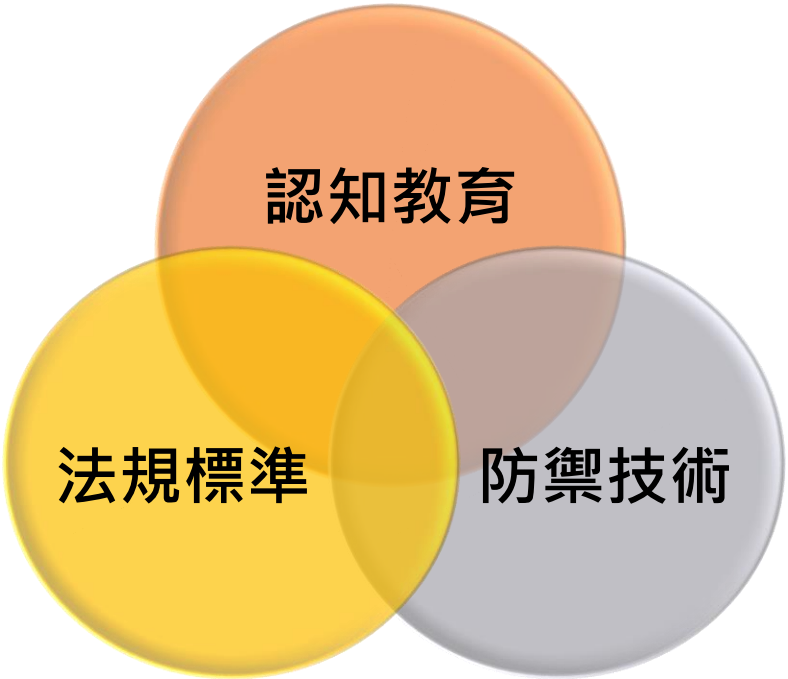
當前資安情勢分析

行政院資通安全處
報告人：簡處長宏偉
106年11月2日

政府資安推動機制

✓各機關每年辦理1次通報演練及2次電子郵件社交工程演練
✓資安會報每年擇選30個機關(構)辦理資安外部稽核，持續改善並降低資安風險
✓政府機關(構)資安專責人力不足，擴大資安職能及教育訓練，培育所需資安人才

✓推動「資通安全管理法」立法，完善各項資安法制環境
✓訂定「國家資通安全發展方案(106至109年)」，奠基國家未來資安發展
✓新興資安標準規範部分，由經濟部、通傳會等發展IoT相關檢測標準及技術



✓各政府機關網路防護監控、技服中心聯防監控及政府網際服務網(GSN)整體偵測防護形成縱深防禦
✓建置資安資訊分享平台(ISAC)、資安通報(CERT)及資安聯防監控(SOC)之資安聯防
✓透過攻防演練，主動發現網站系統弱點

國際資安威脅趨勢

- 世界經濟論壇2017全球風險調查報告指出10大可能風險

1.極端氣侯	6.網路攻擊
2.大規模難民移民	7.非法貿易
3.自然災害	8.人為環境災害
4.恐怖攻擊	9.國家衝突
5.資料欺詐或盜竊	10.國家治理失靈

- 勒索軟體成長驚人
  - 國外著名資安顧問公司2017年資安威脅報告：勒索軟體成長167倍
  - 勒索軟體WannaCry於今年5月間全球肆虐，國內僅少部分的醫院、電力公司、學校及政府機關受影響(數量約185部電腦)
- 大型分散式阻斷攻擊加遽
  - 近期大型分散式阻斷服務(DDoS)攻擊案例大多為混合式攻擊，發動來源皆以物聯網(IoT)設備為主，所占比例與日俱增
  - 國外防毒公司2017年第二季報告指出，於86國由駭客掌握殭屍網路參與DDoS攻擊

國內近期重大資安事件媒體報導

遠東商銀於106年10月3日上午發現電腦遭到惡意程式攻擊，目前合計美金5,800萬元已返回遠銀帳上，美金194萬8千元已被凍結，損失金額已降至美金15萬6千元。

遠東商銀SWIFT入侵事件

- 遠東商銀於106年10月3日上午發現電腦遭到惡意程式攻擊，駭客假冒遠銀名義透過SWIFT(環球銀行金融電信協會)組織系統發出7個電文，使遠銀境外分行之外幣帳戶依據電文內容，執行付款至斯里蘭卡、柬埔寨及美國等地銀行帳戶，遭駭金額計有美金6,010萬4,000元，折合新臺幣約18億餘元
- 經由迅速通報、聯合防護等措施，目前合計美金5,800萬元已返回遠銀帳上，194萬8,000元已被凍結，損失金額已降至美金15萬6,000元(約新台幣468萬餘)，實際損失不到0.3%，並於駭客提款當地緝捕人犯到案
- 本院於106年10月18日邀集遠銀、金管會及刑事警察局召開本案第1次專案會議，充分掌握本案應處作為，近期將召開第2次專案會議研商持續防範措施

未來策進作為-三度防護

- 廣度
  - 透過資安旗艦計畫及前瞻基礎建設計畫，建構政府機關、關鍵基礎設施及地方政府區域治理等多重資安聯防體系
  - 結合大數據分析及人工智慧技術(AI)，預測資安攻擊趨勢
- 深度
  - 強化內外網縱深防禦，持續提升人員資安防護意識，減少誤開郵件及駭客入侵情事
  - 擴大資安稽核及資安健診之檢測方式，主動發現並改善問題
- 速度
  - 各機關策訂資安計畫，落實辦理各項資安應辦事項，提升資安事件偵測及反應速度
  - 透過資安通報及網路攻防等各項演練，提升資安事件應變速度