臺中市議會第 3 屆第 6 次定期會

# 資訊安全防制提升
# 專案報告

臺中市政府
TAICHUNG CITY GOVERNMENT

臺中市政府研究發展考核委員會
報告人：主任委員　吳皇昇

中華民國 110 年 10 月20 日

# 目錄

張議長、顏副議長、各位議員女士、先生：大家好！

欣逢貴會第三屆第六次定期會，本次應邀進行資訊安全防制提升情形專案報告，承蒙各位議員先進，諸多提點與指教，謹致上最誠摯的謝意。

以下專案報告內容將分別針對本府落實資安法應辦事項概況、系統、網路及機房向上集中情形、資安檢測監督及相關演練作為，以及爭取中央前瞻計畫經費強化防護等向各位議員先進說明，敬請各位議員惠予指教！

## 壹、本府資訊安全防制提升作為

### 一、落實資安法應辦事項

#### (一)本府資通安全推動組織

本府 108 年 8 月 12 日設置智慧創新推動委員會，委員會下設數位治理暨資訊安全推動工作小組(以下簡稱工作小組)，置召集人一人，由黃副市長擔任並兼任本府資通安全長一職，小組成員由本府各一級機關副首長或指派簡任人員一人兼任，小組任務為因應資通安全管理法、資通安全管理法施行細則及其相關子法施行之本府資通安全事項推動。

工作小組每年至少召開一次會議，本(110)年度因應 COVID-19 疫情期間，於 7 月 8 日採視訊方式辦理，本次會議除報告各機關法遵義務應辦事項進度外，亦說明大陸廠牌汰換進度及國家資通安全會報、中央資安長會議近期資安強化重點。

#### (二)本府現行機關資安責任等級分級

行政院衡酌公務機關及特定非公務機關業務之重要性

與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級，資通安全責任等級由高至低，分為A級至E級，機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級至少為C級。

依據「資通安全責任等級分級辦法」規定，本府暨所屬機關經行政院110年5月19日院臺護字第1100173803M號函核定機關責任等級結果，政府機關計有 202 個，8 個Ｂ級、40 個Ｃ級、118 個Ｄ級、36 個Ｅ級，包括本府、一級機關、二級機關(含和平區清潔隊、和平區圖書館及31個公有零售市場)；學校機關(含 22 個幼兒園)計有 350 個，349 個Ｄ級、1 個Ｅ級，行政機關加學校總計 552 個機關納入分級。

表 1 本府機關責任等級分級情形

| 機關屬性\等級 | B 級 | C 級 | D 級 | E 級 |
|---|---|---|---|---|
| 政府機關 | 8 | 40 | 118 | 36 |
| 學校 | - | - | 349 | 1 |

本府列Ｂ級機關為警察局、交通局、教育局、地政局、地稅局、社會局、圖書館及資訊中心，共 8 個機關。

### (三)應辦事項內容及各機關完成狀況

依「資通安全責任等級分級辦法」附表，個別機關責任等級有對應的應辦事項，責任等級最高者(A級)，應辦事項最多，本府最高責任等級機關屬於Ｂ級，應辦事項在管理面有 7 大項、技術面有 5 大項 13 小項，認知與訓練則有 2 大項(3 小項)。

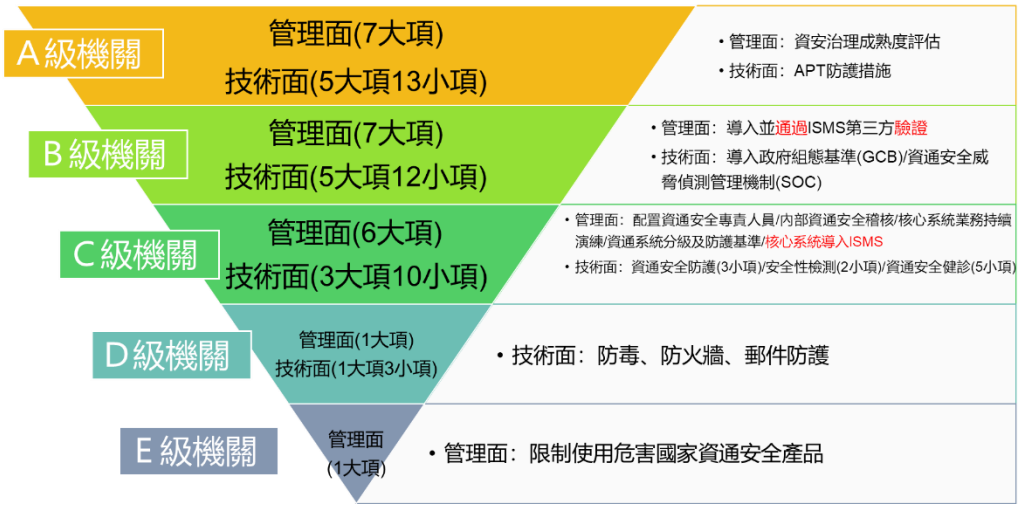


圖 1　資通安全責任等級分級辦法應辦事項

屬共構網路機關部分，本會(資訊中心)已統籌協助辦理 11 項應辦事項，主要是技術面的要求，有效降低各機關工作負擔。

少數機關因人員異動或是資安經費編列等情形，尚未完成資訊安全管理系統導入、通過第三方驗證(預計本年度可以完成)以及取得資安職能證書以外，其餘應辦事項都已經完成。

表 2　本府 B、C 級機關專業證照及職能證書取得情形

| 級別 | 應取得證照(書)機關數 | 國際專業證照機關數(未達法定) | 資安職能證書機關數(未達法定) |
|---|---|---|---|
| B 級<br>(各 2 張) | 8 | 1<br>(教育局) | 2<br>(教育局、市立圖書館) |
| C 級<br>(各 1 張) | 40 | 2<br>(經發局、客委會) | 3<br>客委會、經發局、文資處等，訂於 12 月考照 |

### (四)禁用大陸廠牌產品

行政院 108 年函頒「各機關對危害國家資通安全產品限制使用原則」，惟迄至今尚無公告禁用廠商或產品清單。

109 年 12 月行政院來函擴大盤點使用或採購大陸廠牌之軟硬體設備，並要求上網(資通安全會報管考系統)填報，經盤點發現，本府使用大陸廠牌產品以簡易型網路設備、監視器、空拍機/無人機等為主，係因設備功能滿足需求、價格低廉且限於機關經費有限所致；對於大陸廠牌產品之認定具有一定複雜度，各機關填報資料續經行政院整體評量，於 110 年 7 月 13 日函通知上述填報資料核定結果，本會(資訊中心)於同(110)年 7 月 23 日召開大陸廠牌資通訊產品(含軟體、硬體及服務)之後續應處說明會，請本府各機關務必依法於期限(110 年 12 月 31 日)內完成大陸廠牌資通訊產品汰換作業 (即自公務環境中移除)。

## 二、系統、網路及機房向上集中

### (一)統一建置共通性行政系統

為推動資訊資源向上集中，以提升資訊資源使用率、強化資訊系統資安防護機制，本會(資訊中心)已統一建置多套共通性行政系統，例如：各機關全球資訊網、公文整合資訊系統、公文電子交換、電子郵件系統、垃圾郵件過濾機制、差勤系統、服務 E 櫃台、志工媒合平台等系統，系統之維運遵循本會(資訊中心)資訊安全管理系統(簡稱 ISMS)及個人資料管理制度(簡稱 PIMS)，並已取得 ISO 27001、29100 國際標準雙認證，落實資安規範與資訊安全控管，以提供各機關同仁安全的作業環境。

## (二)建構市政共構網路

本府經臺中縣市合併，機關單位尚無法於單一地點辦公，各機關及所屬單位所在地理位置分散，鑒於數位化的根本是網路基礎設施，本府市政大樓於民國 100 年建置時期即一併規劃市政共構網路，統一收容外部機關(單位)進入新市政大樓共構機房使用公務行政資訊系統，因此，包括陽明市政大樓、前州廳、29 區公所、戶政事務所、地政事務所、清潔隊等等，均為共構網路的連線機關，統計連線機關(單位)數量已經超過 200 個，個人電腦上網頻寬超過 900Mbps，主機對外服務使用 200Mbps 頻寬。

共構網路提供一個整體的資安管制環境，在重要的邊境及節點均設置防火牆等資安設備進行管制及監控，避免網路被不當使用及電腦病毒擴散，重要的日誌資料也透過這個架構蒐集及送交專業 SOC 廠商協助監控。

## (三)提供虛擬化平台供市府機關使用

為整合運算、網路及儲存資源，使其具有擴充性與延展性，能快速及彈性調整運算資源，本府於 100 年起建置虛擬化平台，經過十年的推動，虛擬主機平台現已提供本府 28 個機關申請及使用達 330 台虛擬主機(GUEST)系統，運作於 13 台實體設備，集縮比約為 25，也就是一部實體機可以乘載約 25 台虛擬機，110 年 8 月工作報告資料顯示，該平台當月經過換算，估計為本府節省 45,532 瓩小時電力，相當減少 23,175 kg 碳排放量、相當電費節 159,362 元，其中整體硬體購置費用更是節省 52,885,894 元。

此外，虛擬平台設有完整備份機制，並抄寫至陽明異

地機房，每日原始備份量達 17TBytes，如：台中 e 指通、台中交通卡、社福系統、差勤系統及市府電子郵件系統等本府重要系統，都納入虛擬平台運作，提高系統可用性及資安防護力。

## 三、檢測及監督

### (一)統一提供防毒授權，定期檢討各機關中毒情形

防毒是資安的基礎，由本會(資訊中心)統一採購伺服器及用戶端授權以提供臺灣大道市政中心(臺灣大道)、陽明大樓(陽明街)、都發局及環保局(文心路)、地政局 (三民路)、交通局(民權路)、公訓中心(東興路)、29 區公所、29 戶政事務所、11 地政事務所、文化局、臺中市孔廟忠烈祠聯合管理所、臺中市生命禮儀管理所、臺中市家庭教育中心、臺中市動物保護防疫處、臺中市文化資產管理中心、臺中市海岸資源漁業發展所、臺中市車輛行車事故鑑定委員會、消防局、衛生局等機關使用，用戶端授權總數量為 12,000 台。

每月本會(資訊中心)定期檢討各機關端點電腦發現中毒情形，並確保納管設備病毒碼、掃描引擎更新狀態正常，防毒系統對於發現使用者不當行為及駭客入侵有很大的幫助，因此，除個人電腦以外，會要求進入共構機房之主機系統都必須安裝防毒軟體。

### (二) 辦理主機、網站弱掃

依據「資通安全責任等級分級辦法」，C 級以上公務機關須於法定期間針對核心資通系統辦理弱點掃描檢測作業，為使本府資通系統能於每年維持基本資安防護強

度，每年協助對外服務網站不分等級與核心資通系統執行一次網站弱點掃描，於本府共構網路內部公務系統亦協助一次系統弱點掃描，110 年網站弱掃共檢測 284 個對外網站、內部亦檢測 1,936 台系統與設備，並將檢出結果提供各網站系統轄管機關作為後續漏洞修補、強化資安防護方向之參考。

**(三)整體資安防護架構及檢測成效**

本府資安防護架構由兩大防護建設組成：

1. 資安防護基礎建設：

   透過外部防火牆、內部防火牆、入侵偵測防禦系統、應用程式防火牆及防毒軟體建構由端點至骨幹網路逐層過濾管制，形成辦公室網路、對外服務網路、內部公務網路、府外據點收納網路等不同風險區塊的運行管制要求及區隔。

2. 進階持續性威脅(APT)之資安網路閘道偵測及分析：

   為補強傳統資安防護設備單一防護功能面向不足，以即時對於複合性威脅攻擊型態進行辨識與反應，透過 SOC、網路威脅偵測服務、沙箱分析、APT 郵件攔截等機制，建立以動態分析及專家服務務分析提供 APT 攻擊規則的引入與入侵威脅指標(IOC)的辨識，支援資安防護與網路設備進行惡意網路行為的阻斷，縮短內部攻擊擴散的反應時間，降低或避免進一步損害範圍的擴大。

3. 資安防護檢測成效：

透過兩大資安防護建設相輔相成，並配合資安團隊不斷調校資安設備防護規則、異常事件處理列管、資安事件(直/間接)介入調查，以防微杜漸的態度，逐步強化惡意行為辨識阻斷的準確率並降低重大資安事件發生的機率。

**(四)辦理社交工程演練**

電子郵件社交工程是假冒正常的寄件者寄送電子郵件，並在郵件內容中夾帶惡意網址連結、圖片或惡意附加檔案，誘使收件者去點擊瀏覽，目的在當收件者去開啟或點擊郵件內的相關連結或檔案時，即有可能被植入木馬程式竊取相關電腦資料，或被駭客放置的惡意連結網址或偽造的網站，而造成個人使用的相關帳號密碼遭竊取，除造成個人存放在電腦內的機密資料有外洩的可能外，也有可能造成單位或個人金錢上的損失。

電子郵件社交工程測試係利用各種種類的郵件，搭配網頁型、圖檔型或檔案型附件內容，誘使受測同仁開啟信件並點選附檔，經由統計可了解同仁對於日常郵件之使用及閱讀之行為或習慣，並加強宣導和提升相關資安意識。

本府每年辦理二次社交工程演練，於上、下半年各一次，採延長演練期程、不預先告知演練期間及納入時事類情境等方式辦理。110 年上半年本府整體比率及各機關均達到預定目標(開啟率 6%以下、點閱率 5%以下)。

**(五)個資保護**

歐盟 GDPR (General Data Protection Regulation)個資保護法規從 2018 年 5 月 25 日強制執行，其目的與主旨為規範個人資料處理與資料自由流通，保護個人基本權與自由，

尤其是保護個人資料之權利。

我國已訂定「個人資料保護法」(以下簡稱個資法)，行政機關如有蒐集、處理及利用個資情形，均應依個資法相關規定進行必要告知、通知、取得同意等，並確實依據個資法安全維護措施確保個資的安全性。如發生個資外洩相關事件，應及時進行損害控制、復原並通知受影響之當事人，並請各機關落實辦理下列事項：

1. 加強宣導「臺中市政府及所屬機關新進人員資安宣導單」第 11 點「有資安疑慮或異常時，應即時通報資安窗口」，並強化內部橫向連繫。

2. 參照資通安全管理法第九條及資通安全管理法施行細則第四條規定，落實選商(受託者資安能力)及監督工作，並課以系統維運、監控及事件通報責任。

## 四、爭取中央前瞻計畫經費，提昇市府整體資安

### (一)建置及導入政府組態基準

行政院為強化資通終端設備的一致性安全性設定，於「資通安全責任等級分級辦法」規定 B、C 級以上機關應導入政府組態基準(GCB)，本府資訊中心於 107 至 109 年爭取前瞻計畫經費，分階段輔導本府所屬機關完成政府組態基準導入及管理系統建置作業，包含臺灣大道市政大樓、陽明市政大樓、各區公所、戶政事務所與地政事務所等，統計至今共 125 個所屬機關、16,062 台電腦完成導入作業，有效降低資訊作業的潛在風險，提升資通安全管理效能。

國家資通安全會報技術服務中心每年會評估及公布資通終端設備之組態基準項目，為持續更新本府資通終端設

備的組態基準項目及用戶端軟體(Agent)版本，本府資訊中心每年會統一編列預算取得原廠技術支援與更新授權，以賡續維護本府各機關資安作業環境，建全資安防護網。

**(二)建置網頁應用程式防火牆**

「資通安全管理法」於 108 年正式實施，其中「資通安全責任等級分級辦法」附表一、三「資通安全責任等級資通安全責任等級」規定 A、B 級公務機關應對具有對外服務之核心資通系統，建置應用程式防火牆(Web Application Firewall, 以下簡稱 WAF)，以提供一定的防護攻擊能力。

本府共構機房除已佈署之網路防火牆(FireWall)、入侵偵測系統(Intrusion Detection System，IDS)及入侵防禦系統(Intrusion Prevention System，IPS)等設備針對網路不正常封包或行為進行過濾阻擋，更於 107 年度超前佈署，建置本府「網頁應用程式防火牆」(WAF)，並配合各應用(便民服務)程式網站環境調校設定，主要是協助本府各對外應用程式網站過濾(阻擋)已知的駭客攻擊指令，或是於未補修漏洞期間，提供即時防護，避免造成民眾隱私洩漏或機關聲譽受損害。

現該設備迄今計容納本府 21 個機關之 261 個網站，而依 110 年 9 月資料統計，每日阻擋可疑攻擊行為平均約為 22 萬 4 千多次(單日最低計有 3 萬 2 千多次、最高計有 40 萬 6 千多次)，大幅降低人力負擔及提升本府應用(便民服務)系統的防護能力。

**(三)規劃 B 級機關導入弱點通報機制(VANS)**

電腦系統漏洞常成為駭客利用的目標，尤其是重大漏

洞所造成的風險更高，現行國際上已有完整的漏洞通報機制，而如何盡速盤點系統漏洞及修補便成為資安防護的要項。

依 110 年 8 月 23 日頒布之「資通安全責任等級分級辦法」修正條文，資通安全責任等級 A 級與 B 級之公務機關應於初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。

本府聯合鄰近縣市(彰化、南投)爭取中央「110 年強化政府基層機關資安防護計畫」補助，獲得 501.1 萬元補助，規劃協助本府所屬 8 個資安責任等級 B 級機關具備執行資訊資產弱點管理與安全性更新檢測之能力，落實掌握關鍵資訊系統之潛在弱點，縮短資安盤查及風險掌握時間，降低資安弱點導致資安風險。

## 貳、結語

資安防護沒有百分百，所有人都可能是駭客攻擊目標，無人可以置身事外，近年來公私產業遭駭客勒索情形不斷，例如近幾個月美國主要燃料供應商 Colonial Pipeline 遭攻擊以致停業數日，造成重要燃油供給問題，網路安全顯然已經成為國家安全和經濟問題。

資安相關規範及作業繁多且複雜，需要人力及經費辦理，本會(資訊中心)除整合系統、網路融入資安治理方法以外，也積極向中央爭取補助經費，惟駭客攻擊技術及手法與日俱進，未來將依 PDCA 精神，持續檢討精進。