考試院第 12 屆第 79 次會議考選部重要業務報告

民國 105 年 3 月 24 日

壹、 考選行政

考選部個資保護及資安防護之推動情形

一、前言

本部辦理國家考試，依法運用應考人報名資料、學者專家典試人力資料，各項考試期間亦聘用監場、入闈及臨時工作人員，爰保有個資項目及數量甚多，前揭個資蒐集、處理及利用皆需符合法制規範及特定目的。

依個人資料保護法規定，個資外洩每人每件可求償新臺幣 500 元至 2 萬元，同一事件最高求償總額達 2 億元。個資保護客體擴大為電子檔案及紙本資料，對政府機關管理處罰課責衝擊甚鉅，爰本部積極加強落實個資保護及確保資料安全，以維護國家考試公信力。

二、個資保護推動情形

本部為推動個資保護，辦理下列安全維護措施：

（一）**設置個資管理組織與人員**：訂定本部個人資料保護管理要點，由政務次長擔任召集人，並成立執行小組，負責本部個資保護管理之規劃、執行及適法性之檢視、審議等事項，同時納入資安防護議題，檢討資安及個資稽核執行情形；由各單位指派專人，負責單位個資管理事項；指定聯絡窗口，負責個資保護業務與行政院之協調聯繫及緊急應變通報。

（二）**界定個資範圍及蒐集、處理與利用之管理程序**：

1. **定期盤點及公告個資保管項目**：本部全球資訊網 104 年公告保管個資計 103 項，其中考選部專屬特定目的為「試務行政」類別計 49 項。
2. **推動個資最小化原則**：檢視資訊系統與業務之關聯性、資料庫儲存個資之必要性，採資訊系統簡併、刪除資料庫欄位、報表輔以隱碼方式呈現個資等措施。

3. **限制考選資料公開（Open Data）項目：**配合政府數位資料開放政策，排除具有個資辨識性及資料存放容量太大者。目前本部全球資訊網提供各種考試統計及最近 10 年之 12 項考試開放資料，並於行政院政府資料開放平臺置有 83 筆開放資料集。

4. **界定智慧型手機傳輸公務訊息項目及程序：**訂定國家考試臨時性 Line 群組作業注意事項，規範考試期間試務工作通報訊息，並嚴禁傳送機敏性（含個資）資訊。

（三）**強化設備安全管理機制：**規範系統使用者密碼長度及更換頻率、造冊列管隨身碟及公務電腦嚴禁安裝 Line 電腦版軟體，並修訂資訊設備管理及使用規範。

（四）**設置資料庫稽核系統：**為強化使用紀錄及數位鑑識保存，典試人力管理系統、試務整合性管理系統及網路報名系統業建置資料庫稽核系統，追蹤所有存取行為，防止未經授權即予變更。

（五）**建立定期個資稽核模式：**組成稽核小組辦理審議稽核計畫及進行稽核，內稽重點為個人電腦安全防護、個資保護管理、個資事件因應及資安政策落實情形等。

（六）**導入個資風險評估及管理機制：**建立風險量化標準，辦理講習輔導各單位分析個資風險，並將風險處理情形，納入年度個資稽核要項，藉由 PDCA 循環模式持續改善。

（七）**持續認知宣導及教育訓練：**建置資安宣導網，納入資安全員訓練教材，宣導個資及資安防護事項，並以電子郵件即時通報資安新知，深化同仁認知意識。

三、資安防護推動情形

本部為資安責任等級 A 級機關，為達到最高資安防護等級要求，積極作為如下：

（一）**健全資安組織：**由政務次長擔任資安長，各單位主管組成資訊安全推行小組，統籌規劃資安推動方向，並針對核心資訊

系統，設置網路報名及試務整合資訊安全處理小組，定期進行外部專家及內部稽核作業。

（二）**落實資訊系統分級**：依行政院資通安全辦公室資訊系統分級與資安防護基準作業規定，辦理資訊系統分級及風險評鑑作業，並採行適當安全控制措施。

（三）**導入國際資訊安全管理系統**：95 年國家考試網路報名系統、99 年試務整合性管理系統，先後通過國家資訊安全 CNS 27001 認證及國際資訊安全 ISO 27001 認證，每年持續辦理業務營運演練、內部稽核制度及第三方外部稽核等作業。

（四）**提升資安人員專業職能**：每年指派資安人員接受 12 小時以上專業課程訓練或資安職能訓練，目前本部資訊管理處通過國際資安專業證照 9 張及資安職能訓練證書 2 張。

（五）**定期資安訓練及社交工程演練**：每年辦理 2 梯次全員訓練課程及隨堂測驗，並自 97 年起，每年模擬駭客以電子郵件方式，辦理 2 階段社交工程演練，未通過測試人員，據統計 97 年為 82 人，至 104 年僅剩 2 人，顯見本部同仁已養成不隨意開啟不明電子郵件之良好習慣。

（六）**強化資安監控及防護縱深**

1. **外部防護**：布署全年 24 小時資安監控中心（SOC, Security Operation Center）及建立緊急應變程序。
2. **內部防護**：布署網路防護（防火牆、入侵偵測系統）、郵件防護（郵件過濾裝置、進階持續性滲透攻擊防禦）、防毒系統（即時更新病毒碼、定時掃毒）及主機系統（強制派送資安原則及存取權限、自動修補安全性漏洞）等防護裝置，並設計機敏資料加密存放、獨立安全作業網域、使用者帳號密碼管制及機房門禁出入管制等防護機制。本部 104 年度計攔截 66,679 封垃圾郵件，並成功阻擋 87,695 次資安攻擊事件。
3. **特定應用系統加強防護**：全球資訊網建置反插旗作業，以防止歡迎頁、首頁被竄改；試務整合性管理資訊系統採實

體網路隔離，未連接外部網路服務；網路報名系統設主分站異地備援機制，提供 24 小時報名不中斷服務。

（七）**定期執行資安檢測**：每季檢視路由器存取控制規則、每半年檢視防火牆政策、每年辦理資訊系統滲透測試、主機弱點掃描及木馬檢測、網頁弱點掃描及源碼檢測等作業，並定期召開資安季會，納入 SOC 監控報告及最新資安議題，研提應變措施，以確保資訊系統之安全防護水準。

四、結語

網際網路使用無國界，復以新資訊科技大幅創新應用，近幾年資通訊安全事件層出不窮，坊間個資外洩屢有所聞，加以駭客不斷更新網路攻擊與竊取資料之手法，是以，個資保護及資通訊安全議題更顯重要。本部將持續檢視業務管控流程及相關法制處理措施，加強人員個資保護意識與資安防範能力，並強化資通訊安全基礎建設，核實管控個資風險，俾完善管理本部保有之各項國家考試試務資料。