考試院第 12 屆第 219 次會議考選部重要業務報告

民國 107 年 12 月 27 日

壹、 考選行政

107 年國家考試資安防護機制辦理情形

一、前言

本部為資安責任等級 A 級機關，多年來積極落實資安防護應辦事項，本（107）年除陸續更新骨幹網路多項資安網管設備外，所有對外服務系統全面採用 HTTPS 安全連線，網路報名及試務整合性管理 2 項核心資訊系統，持續維持國際資訊安全 ISO 27001 認證之有效性，國家考試 APP 並依經濟部工業局資安檢測基準，通過 iOS、Android 兩種版本資安檢測。此外，更進一步導入個人資訊管理系統之個資保護作法，以有效落實國家考試資安防護及個人資料保護與管理。

二、資安防護辦理事項

（一）資通系統分級防護：盤點本部現行試務及行政 38 項資訊系統安全，並依資訊系統等級，辦理各項風險評鑑及採行適當之安全控制措施。

（二）網路資安威脅偵測、防護及管理

1. 監控機制：部署全年 24 小時遠端監控中心，監控駭客攻擊與入侵事件，並落實緊急應變程序即時處理，以降低資安危害風險。
2. 防護機制
   (1)骨幹網路部署防火牆、網路入侵偵測防禦系統、防毒系統，阻絕外部惡意網路刺探及攻擊威脅，每月平均阻擋約 10,800 次資安攻擊事件。
   (2)電子郵件系統建置垃圾郵件過濾及進階持續性攻擊防禦機制，有效防阻駭客利用社交工程郵件攻擊威脅，本年計攔截約 6 萬筆垃圾郵件及隔離 79 筆疑似惡意攻擊郵件。
   (3)完成軟硬體設備更新及備援演練作業，並持續廣納資安科技新知，俾整體提升資安防護能力。

3. 管理機制

(1)網路端點管控：內部網路建置網路 IP 管控機制，防止未經授權之端點設備接入，以強化網路使用安全。

(2)獨立安全作業網域：試務整合性管理系統、題庫整合資訊系統及電腦化測驗系統，均採封閉式網路架構，不提供對外服務，並落實使用者權限管制及機房門禁管理。

（三）定期資安檢測

1. 應用系統:進行滲透測試、網頁弱點掃描及源碼檢測。
2. 伺服主機:執行作業系統修補程式更新、弱點掃描及惡意木馬程式檢測。
3. 骨幹網路:防火牆政策及路由器存取控制規則檢視。
4. 資安健診:依年度健診報告，調整及加強各項資安防護措施，以確保安全防護水準。

（四）所有對外服務系統採用資訊安全連線：本年上線之行動化服務官網、國家考試 APP、線上問卷及新版公文電子交換系統、置於雲端之考選部公報、查榜及考畢試題查詢平臺等，全面採用 HTTPS 加密傳輸機制，落實政府機關網站安控規定。

（五）持續維持 ISO 27001 認證有效性：網路報名及試務整合性管理 2 項核心資訊系統，定期召開管理審查會，實施風險評鑑與內部稽核、異地備援、備份與業務持續營運演練，並將國家考試 APP 納入驗證範圍，以符合國際資安標準 ISO 27001 要求。

（六）人員資安認知與訓練

1. 資安教育訓練：全員 3 小時資安教育訓練，並針對缺課或社交工程演練未通過者，辦理再教育訓練，以提升同仁資安意識。
2. 資安專責人員訓練:資訊管理處同仁每年接受 12 小時以上之資通安全專業課程或職能訓練，本部計通過國際資安主導稽核員專業證照 8 張及資安職能訓練證書 4 張。
3. 電子郵件社交工程演練：首度比照行政院演練模式，採全年常態性及非預警方式,並提高擬真程度,爰誘騙成功率較往年高，亦將持續辦理並加強宣導，以強化同仁收取電子郵件警覺性。
4. 資安訊息宣導:相關資安防護訊息、資安事件及最新資安議題，不定期透過本部資安宣導網於電腦開機時主動推播宣導。

三、完備個資保護機制

（一）導入個資保護制度：訂定個資檔案風險評鑑作業計畫，輔導各單位運用風險評鑑技術,量化個資風險程度,並據以有效改善。

（二）辦理個資稽核：稽核重點為個資資料及風險之完整識別，並強化個資管理程序及個資盤點廣度。

（三）召開個資小組會議：確定個資保管公告項目及強化試務工作場所電腦安裝軟體管理措施，並分享近期個資外洩案例及重要資安議題。

（四）強化網路報名及國家考試 APP 個資防護：網路報名資訊系統啟用電郵信箱確認機制，當應考人於報名時，經系統檢核通過 Email 認證，即關閉「線上即時取得初始密碼」，未來僅能透過 Email 取得密碼，以加強應考人個資安全之防護範圍。此外，國家考試APP純以提供考試訊息為主,未提供個資維護及查詢，並納入應考人修改密碼、行動裝置遺失或以其他行動裝置重複登入時，啟用限縮登入效期及使用功能之安全保護機制。

（五）持續落實資料庫儲存個資最小化原則：資訊系統僅留必要個資欄位，機敏欄位採密文及去識別化處理，並運用資料庫稽核系統，以完整保存使用者之系統操作軌跡。

四、結語

資通安全管理法業於本年 6 月 6 日公布,六子法亦於 11 月 21 日訂定發布，並定於明(108)年元月份施行，本部業務涉及全國性民眾服務，屬新法規範之資通安全責任等級 A 級機關，將依鈞院規定期程完成資安維護計畫、資通安全事件通報應變程序及提報實施情形，同時落實資通安全事件通報、調查、處理及改善作業，以有效提升國家考試資安防護工作。