考試院第 12 屆第 267 次會議考選部重要業務報告

民國 108 年 12 月 26 日

壹、 考選行政

108 年國家考試資通訊安全防護機制辦理情形

一、前言

資通安全管理法自本（108）年元月起施行，本部業務涉及全國性民眾服務，屬資通安全責任等級 A 級機關，除依規定完成資通安全維護計畫、資通安全事件通報及應變管理程序函報鈞院及行政院核備，亦積極落實資安防護應辦事項，其中網路報名及試務整合性管理 2 項核心資訊系統通過國際資安 ISO 27001 認證及持續進行相關安控作業，並依個人資料保護政策及管理程序，辦理個資講習、盤點、風險評鑑及稽核，以提升國家考試整體資安防護及個資管理與保護能力。

二、資安防護事項

（一）**資通安全工作計畫**：依年度計畫期程落實各項資通安全防護應辦事項。

（二）**資通系統分級防護**：盤點本部試務及行政資訊系統安全風險程度，並依系統等級辦理風險評鑑及安控措施。

（三）**資通安全演練**：辦理資通安全事件通報、核心資訊系統業務持續營運、資料庫備份還原、骨幹網路及核心交換器備援演練，提升資安應變處置能力。

（四）**資安治理成熟度評估**：完成年度資安治理成熟度防護指標能力自評，透過 PDCA 管理模式，持續改善及優化機關資安治理能力。

（五）**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，監控駭客攻擊與防堵入侵事件，以降低資安危害風險。
2. 防護機制
   (1) 骨幹網路部署防火牆、網路入侵偵測與防禦系統及防毒系統，每月平均阻擋約 1 萬次資安攻擊事件。

(2) 電子郵件系統建置電郵過濾及防禦機制，本年計攔截約 7 萬筆垃圾郵件及隔離惡意攻擊郵件。

3. 管理機制

(1) 網路端點管控：強制內部網路 IP 位置管控，阻絕未經授權之外來設備擅自私接本部網路環境。

(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。

(3) 部署政府機關安控設定：強制規範電腦機房伺服主機及個人電腦具一致性安全設定及操作環境，以降低駭客入侵管道。

（六）定期資安檢測及弱點修補

1. 應用系統:針對核心、對外服務之 E 化系統，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:檢視與調整防火牆政策及路由器存取控制規則。
4. 資安健診:經由實機分析散置各處之個人電腦、伺服主機及網路架構防護措施，進行後續資安防護水準調校作業。

（七）人員資安認知與訓練

1. 資安教育訓練：每年全員 3 小時資安教育訓練，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：持續提升資訊管理處同仁資安專業能力，本年計通過國際資安主導稽核員專業證照 3 張及資安職能訓練證書 5 張。
3. 電子郵件社交工程演練：採全年常態、非預警及提高擬真程度方式，強化同仁收取電郵警覺性。
4. 資安訊息公告:相關資安防護訊息、資安事件及最新資安議題，每日透過本部資安宣導網於電腦開機過程主動推播宣達，並輔以電郵即時通知。

三、個資保護事項

（一）落實個資管理

1. 召開管理會議：檢視資安及個資稽核執行成效，確認國考個資

公告項目保管概況及調整試務作業安控指標。

2. 完備保護管理制度：訂定個資保護政策、安全控管、當事人之權利聲明及風險評鑑管理等作業文件。
3. 風險評估管理：依個資檔案風險評鑑及稽核計畫，建立定期個資稽核模式及風險量化標準，並將量化個資風險處理情形，納入年度個資稽核要項。

（二）強化資安防護

1. 內外部 E 化環境實體區隔：劃分網際網路外部使用端與試務內部專用工作網段，以阻擋駭客入侵管道及避免資料外洩造成資安事件發生。
2. 落實個資最小化儲存原則：資訊系統僅留必要個資欄位，特定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。
3. 電子郵件寄送安全服務：研議 109 年啟用電子郵件數位簽章機制，佐證考試通知書及成績通知之郵件及附檔係來自考選部寄發，以強化應考人收受安全電郵來源端之確認機制。

四、結語

國家考試資通訊安全防護機制，涵括資通安全管理法及其子法、個人資料保護法及考試法規等要求，本部業部署多層次防護機制，以確保國家考試業務持續安全運作。未來，本部亦將協同行政院主管機關之資安威脅情資分享機制，主動提供網路安全監控及防護情資等資訊，以共同提升政府機關資安聯防成效，並配合行政院於 109 年到部進行資通安全稽核作業，以協助檢視本部資通安全防護工作之完整性及有效性，俾持續精進各項國家考試 E 化防護措施，降低資通訊安全風險。

附件

考選部108年國家考試資通訊安全防護機制辦理情形

項目		安控執行事項	時程
政府機關資安聯防		1. 資通安全維護計畫、資通安全事件通報及應變管理程序函報考試院	1月
		2. 資訊系統分級及清冊核定	2月
		3. 政府網路攻防及社交工程、資通安全事件通報及應變演練	第2-4季
		4. 資通安全威脅情資回傳	12月
資通安全A級機關應辦		1. 全員資安通識教育訓練	3月
		2. 資安專責人員接受資通安全職能訓練及取得證書	第2-4季
		3. 資訊人員參加國際資安主導稽核員訓練及取得證照	
		4. 資安治理成熟度自評	10月
		5. 資安健診	第4季
		6. 資訊系統安控作業	全年
		7. 政府組態基準（GCB）	
		8. 資訊安全監控中心（SOC）	
		9. 24小時遠端監控、網路防火牆、網路入侵偵測及防禦、防毒、電郵過濾及防禦機制	
		10. 資安危害產品採購限制	
核心資通系統	試務整合	1. 資訊安全管理系統（ISMS）四階文件修訂 2. 風險評鑑 3. 內部稽核 4. 系統滲透測試 5. 網站安全弱點檢測 6. 業務持續運作演練（BCP） 7. 核心資料庫DAM監控與安全防護 8. 管理審查會 9. 第三方外部稽核及持續通過驗證	全年
	網路報名		
個資保護管理		1. 修訂個資保護政策、安全控管、當事人之權利聲明及風險評鑑管理等作業文件	5月
		2. 辦理個資風險評鑑講習、個資盤點、風險評鑑及稽核作業	第3-4季
		3. 核定個資清冊、全球資訊網公告個資保有項目	12月