行政院主計處電子處理資料中心　函

地址：臺北市廣州街2號
聯絡人及電話：林光勳（02）23803860

受文者：教育部

發文日期：中華民國98年2月26日
發文字號：中審字第0980000177號
速別：最速件
密等及解密條件或保密期限：
附件：九十七年度資通安全稽核報告

主旨：檢送「九十七年度資通安全稽核報告」乙份，報告所提綜合意見如說明三，請轉知所屬落實辦理。

說明：

一、對於各受稽單位之建議事項，請各主管機關督促改善並督導所屬落實辦理資安內部稽核。

二、對於推動辦理資安稽核著有績效人員，建請各機關本於權責予以敘獎。

三、綜合意見：

（一）重要及機敏資料在傳輸或儲存中，以加密、認證技術、實體隔離之方式處理時，應制定相關作業程序，管制資料之繕打、處理及儲存應於隔離區作業，並定期檢核控管，確保處理資訊之安全。

（二）儲存機敏資料之可攜式媒體，應律定明確之政策及管理規定，嚴禁與連網環境接觸，並定期或不定期實施稽核，加強管制。

（三）建議訂定敏感性資訊資產系統之日誌檔案管理稽查機制，以強化系統及資料之監控與後續追蹤。

（四）機密性或敏感性資訊存取權限應適當分散權責，避免集中部分人員管理，以降低可能之風險。

（五）對於各項防護措施應訂定量化之指標，以檢測風

險處理計畫實施的有效性。

（六）使用SOC/NOC監控平台對網路相關設備與使用行為進行即時監督與反應，宜將資安控制的要求作自動化處理，以確保控制的有效性。

（七）系統開發與維護業務大量委外時，對委外廠商依賴度高，應對其是否遵守保密條款、資安協定、資安事件責任及作業程序等，加強規範並落實執行。

（八）應用系統如採自行開發時，建議加強軟體安全檢測，並建立安全軟體開發作業程序(SSDLC)。

（九）若經費許可，可考量對外服務網站之應用系統進行原碼檢測與修護之可行性，以防護如SQL Injection及XSS等常見網站弱點。

（十）建議透過側錄系統保全資安事件相關證據資料，以作法律依據，並對資安事件紀錄進行統計及根因分析，以作為資安防護改善之參考，且於資安事件處理後，宜建立事件學習檢討機制，以預防事件再次發生。

（十一）營運持續計畫之規劃，建議先進行業務衝擊分析（BIA：Business Impact Analysis)，BIA之結果需與復原計畫相互勾稽，並應定期進行各情境的演練；營運持續計畫應對重要等級之資訊系統，訂定幾項指標，如：系統可容忍失效時間(RTO)、系統支援之業務可容忍中斷時間(MTPD)、回復目標時間點(RPO)等，作為營運備援與復原的時效要求。

（十二）天然災害及系統回復作業計畫，應依關鍵性業務排定優先次序，逐項規劃其細部作業程序及業務單位之應變作為，予以整合成完整之營運持續計畫，再定期擇項測試演練，並定期審查

及更新，以確保計畫有效可行。

（十三）營運持續計畫可增列事件造成營運中斷機率之評估，以作為事件處理時資源分配評估依據。

（十四）目前「個人資料保護法」已送立法院審議，建議提早規劃因應，並增加數位鑑識（電腦鑑識、網路鑑識、軟體鑑識、檔案鑑識）的教育訓練與處理能力。

正本：行政院各部會行處局署、省市政府及各縣(市)政府

副本：總統府第二局、立法院資訊處、司法院資訊管理處、考試院資訊室、考選部資訊管理處、銓敘部資訊室、監察院資訊室、審計部資訊管理組、經濟部國營事業委員會、行政院金融監督管理委員會證券期貨局、國家資通安全會報綜合規劃組及各受稽單位(皆含附件)

主任 劉勝秉

副主任 潘城武 代行