考試院數位轉型委員會第 3 次會議紀錄

時間：中華民國 110 年 10 月 13 日(星期三)下午 2 時 30 分

地點：本院傳賢樓 10 樓會議室

出席者：黃主任委員榮村、周副主任委員弘憲、姚委員立德、許委員舒翔、周委員志宏、郝委員培芝、李委員漢銘、郭委員耀煌、蘇委員俊榮、陳委員正然

列席者：劉執行秘書建忻、袁副執行秘書自玉、呂組長理正、龔處長癸藝、周組長秋玲、熊組長忠勇、徐主任嘉臨、高執行秘書誓男、陳處長建華、方主任映鈞、羅主任家寧

出席者請假：廖委員婉君、朱委員斌妤

主席：黃主任委員榮村　　紀錄：翁淑慧

壹、報告事項

一、宣讀第2次會議紀錄。

決定：確定。

二、考試院數位轉型工作執行情形。

決定：洽悉。

三、書面報告

(一)考試院資訊室案陳「考試院資通安全強化規劃」一案，報請查照。

(二)考選部案陳「國家考試資安防護辦理情形」一案，報請查照。

(三)銓敘部案陳「銓敘部資通安全防護簡介」一案，報請查照。

郭委員耀煌：

1. 今日三份報告依資通安全管理法發布之各種指引，形式十分完備，如何依據PDCA落實，各階段仍須透過稽核或演練提出循證(evidence)，因為資安是永遠的戰爭，資安發生的形態會改變，需要不斷去檢視各種狀況，此牽涉明確的獎懲制度及組織文化，假設有資安事件發生或是提前防範資安事件，能有明確的制度處理及獎懲，以及資訊安全全員有責的組織文化，即能有效因應。現在資訊管理制度(Information Security Management System, ISMS)的範圍很多都侷限在資訊單位，似乎資安就是資訊單位的問題，但資安其實是整個組織的問題，建議後續可再加強全員資安意識。
2. 考試院早期開發的應用系統頗多，然攻擊應用系統的趨勢升高，因早期應用系統設計多無資安考量，資安漏洞多，許多組織即因早期應用系統發生資安事件。因此，加速改善早期應用系統之安全性與漏洞修補，極為重要。
3. 近年來，各機關為避免發生資安事件，購置許多資安設備，因此資安占資訊預算的比率不低，甚有逾50%者，其實整體資訊預算仍占機關預算仍然極低。考試院若欲加速數位轉型，提升數位化服務與作業，須考慮提高資訊預算比率，資安投入才可同步增加。
4. 近期許多資安事件發生在資訊委外管理部分，即機關資訊業務委外後，讓廠商遠端連線作業，繼而產生資安事件，若考試院及部會資訊業務仍須委外，須注意委外管理的問題。
5. 部分資安問題在委外稽核時並未找出，雖然委託專業機構進行資安稽核，應確實協助找出問題，但稽核有一定形式，且許多細節僅組織內部才能了解，因此資訊

安全最終仍須回歸己身，委外稽核及內部資安的落實須同時考量與進行，缺一不可。

蘇委員俊榮：

1. 考試院重要資料異地備援係建置於國家文官學院，低於資通安全會報建議異地備援之安全距離30公里，建議能提高異地備援距離。人事總處規劃明年將異地備援系統設於南投中興新村，尚有部分機櫃空間可供異地備份，建議考試院可考量建置至中興新村網路頻寬，由人事總處提供備份場所，以較低成本提高異地備援距離及安全性。此外，考試院明年將進行大幅度資訊硬體設備改善，建議於軟、硬體設備汰換升級前，仍應儘可能修補風險及弱點，以降低過渡期間發生資安事件之風險。
2. 國家考試資安防護各環節均有審慎完整考量，考選部實作經驗極為豐富，謹提以下建議：
   (1)資通安全內部稽核範圍可擴充至全機關，此牽涉組織文化，過去稽核範圍僅限資訊單位，但資訊安全及個資保護，須從整體機關規劃考量，另ISMS及專案管理資訊系統 (Project Management Information System，PMIS) 未來亦應予結合，否則兩系統部分重疊，管理成本較高。
   (2)考選部有網路報名系統及試務整合性管理系統兩個核心系統，試務整合性管理系統係使用Cluster(叢集)架構，建議可採 HA(高可用性)架構，以提升資料庫之保護及可用性。
   (3)有關傳輸層安全性協定(Transport Layer Security，TLS)之使用，人事總處規劃由TLS 1.1轉到TLS 1.2，建議考試院及考選部亦應強制使用TLS1.2(含)以上協定，以提升資料傳輸之安全性。

(4)有關個人電腦防毒頻率，經調查行政院等機關每日一次或每週一次掃描者均有之，人事總處目前個人電腦之防毒軟體每日中午均會自動全機掃描，以上僅提供參考。

3. 銓敘部目前有 6 個核心系統,每年針對不同情境進行業務持續運作演練，建議 6 個核心系統可分 4 至 6 天進行演練，每日僅進行 1 個核心系統或 2 個具關連性核心系統，若發現問題才能扎實因應。此外，銓敘部現有資安專職人員 2 人，目前持有 ISO27001:2013 主導稽核員(Lead Auditor)證書 1 張及資通安全職能評量證書 3 張，未來銓敘部若規劃成立資安科，相關資訊安全專業能力養成及資安證照之取得至為重要。

4. 有關院部會資安聯防議題,宜先有整體性政策管理機制後再分工，此可分為兩階段，第一階段為考試院、保訓會及監理會，第二階段可評估考選部及銓敘部適當整合，整合方式包含實體整合與成立委員會，就如考試院院區包含考選部、銓敘部、保訓會、監理會及院本部等多個出入口,維護院區安全是以聯合警衛概念，如此人力使用較為精簡,否則機關各自進行資安維護，人力調度運作恐較吃緊。另補充人事總處資安人力含約聘僱計 37 人，提供委員會參考。

李委員漢銘：

1. 考試院資安作為在整體政府部門應為優等生,提醒落實執行最為重要；另外，常有資料加密後怕影響效能，又再開放而發生資料外洩的情形，因此考試院資料庫重要欄位是否加密及使用何種方式加密，建議應確實檢視。

2. 院部會通案性資安問題改善，如汰換升級資通系統、提升全員資安法遵意識訓練等，建議由考試院規劃逐年改進。
3. ISMS 攸關資訊安全，應確實落實所提規劃。
4. 委外確為近期資安事件的破口之一，例如委外客戶服務中心為聯繫及資料串接，或者委外廠商為維護方便，在組織外部多拉一條線，造成資安破口，甚至有驗收時發現程式碼包含簡體字，才得知委外廠商連線 IP 來自中國，許多委外廠商為了省錢，Code 都交由中國開發，所以部分是簡體字的 Code，因委外廠商多數比我們專業，管理不易。更為困難的部分，因台灣廠商為網通全球供應鏈，如網通設備有弱點，就容易遭受攻擊，自己的防護做的再好都會出問題，所以要隨時要注意弱點漏洞的通報，隨時更新，如果設備早已通報卻未處理，容易造成更大問題，大家可互相關注處理，資安聯防通報與人才互動確實至關重要。
5. 有關資安員額部分，按資通安全管理法及資通安全責任等級分級辦法規定，資安責任等級 A 至 C 級公務機關與國營事業、財團法人、關鍵基礎設施提供者等特定非公務機關，應分別至少配置 4 名、2 名、1 名資安專職或專責人員。

陳委員正然：

1. 資安工作是否完善且落實，仍待後續追蹤管制，例如資安演練發生狀況後續相關處理。一般單位社交工程比率較高，院部會社交工程比率低，顯示內部宣導與教育訓練極佳，但若同仁能預先得知演練時段而特別注意，就無法達到實際效應。
2. 資通安全未來將成為常態，尤其是後疫情時代，國際重要組織都在倡議一項標準，就是組織的資訊韌性一定

有包含資通安全，未來無論是工作型態轉變，或是加速推動數位轉型，會有越來越多業務及資料在網路上傳遞，有價值的東西越多，就會遭遇到跟以前不一樣的等級、頻度與程度的攻擊，資安計畫與防範的要求就會有所不同，因此人員教育訓練及資安稽核須涵蓋全員，建議院部會後續都能加強推動。

3. 有關委外管理部分，不能僅強調加強管理承包商，必須有標準與依據可供依循，在尚無國家級標準時，建議可參考美國國防部所發表的《網路安全成熟度模型認證 1.0 》（ Cybersecurity Maturity Model Certification，CMMC)，承包商必須依據專案的機密性，取得不同等級的安全認證，目前美國國防部將 CMMC 分為五個等級，從第一等級的基本網路防護(Basic)、中等網路防護(Intermediate)、良好網路防護(Good)、主動防護（Proactive），到第五等級的進階防護（Advanced)。台積電等大企業已參照上開 CMMC 精神要求承包商及開發商人員，委外管理需有標準可依循，否則後續管理恐是各說各話。

4. 假定本院及所屬單位發生資安事件，相關通報及應變的作業程序將如何處理？行政院訂有資安事件通報程序，若考試院發生資安事件，相關通報機制及規定須明確規範，才會有利於後續資安事件處理及明確化作業的依據。

5. 考試院現行資安推動組織為個人資料保護暨資訊安全管理委員會，但成員多為內部同仁，建議一定比例納入外部學者專家，以提供資安專業意見；並應建立資安專家資料庫，以在發生各種資安事件時提供諮詢協助。

姚委員立德：

1. 委外開發程式碼的撰寫方式可能造成資安漏洞，因此越來越多單位要求委外開發程式需通過資安掃描，本院及所屬部會未來針對委外廠商開發應訂定此需求規格，自己也需有能力進行資安掃描，建議本院與所屬部會合購資安掃描軟體，才能確定委外開發軟體有無漏洞。
2. 院部現有開發軟體系統多數為委外開發，廠商開發人員須維護及定期更新軟體，其工作環境與方式，例如是否允許從外部連線維護等，亦應有所規範。
3. 電腦作業系統有完善的防衛系統，但手機多無，一旦手機被植入惡意程式，而電腦允許與手機資料同步，極可能導致從內部發生資安事件，提醒電腦與手機同步方式應加以限制並採購軟硬體防範。
4. 為避免內部環境被植入惡意程式造成資安事件，偵測與隔離措施也須規範，以大學實驗室為例，電腦若被植入惡意程式即停權若干天,進行澈底掃毒及檢查後，才允許重新上線。建議建構機關內部自動偵測惡意程式與研擬使用適當軟硬體隔離措施。
5. 政府資安人力急缺，高考三級和普考皆設有資訊處理類科，資訊人員就職後，尚需取得國際證照，才能正式成為資安人員，如無特殊加給誘因，恐仍難以吸引專業人才投入。現在國家需才孔亟，建議銓敘部審酌設置資安防護專業加給，以此吸引優秀人員加入，保障資訊安全。

徐主任嘉臨：本院資料庫均有加密，尤其電子證書系統，因涉及個資，均依規定加密。有關老舊系統的汰換升級、充實資安專職人力及委外管理等，將分階段完成。另補充委外管理部分，目前委外開發系統規範，政府機關委外時，須要求開放系統應導入安全軟體開發生命週期

(Secure Software Development Life Cycle, SSDLC)，也就是要求廠商安全的程式碼開發，我們要求廠商交付程式時，也會要求並確保不能有開放網路軟體安全計畫的十大弱點（Open Web Application Security Project, OWASP Top 10)，本院每半年會找第三方針對核心系統滲透測試，每年也會適當地換不同廠商來做第三方測試，避免單一廠商產生盲點。針對委外開發部分，無論是系統維護人員、開發人員的工作環境要求，遠端登入是原則禁止，例外開放，到院維護僅能在特定位置進行，且該位置不能連網，避免遭植入程式感染本院環境。至於手機與電腦同步部分，本院規範是不允許手機與電腦同步，因非常容易受到感染，如何強制不允許同步，需要技術性規範，此即安全及便利之間如何平衡的問題。至於委員建議院部會建立資安專家資料庫，此建議頗佳，將納入未來推動參考。

方主任映鈞：考試院及考選部、銓敘部資料庫均有加密，加密等級均為資料庫等級，即加密所有資料，若整個資料庫都被盜走也不易復原。銓敘部在資安事件發生後曾研究，希望能在程式等級加密，類似購物網輸入地址資料或姓名欄位顯示遮罩，但實際執行並不容易，業務單位並不習慣在承辦業務時畫面是隱碼或遮罩，若要更進一步處理，需要工作調適及法規的支持；或考量在法定清冊(如考績清冊或考績通知書等)以明文顯示，而在一般業務處理畫面遮罩，業務單位接受度亦極低，因此以程式等級加密仍待突破。

陳處長建華：政府資訊專案常透過委外開發方式辦理，惟就考選部而言，並不允許委外廠商逕從外部連線進入，對於廠商駐部作業環境，也特別要求必須在特定場所與電腦工作平台，程式開發僅限使用測試系統環境，無法

接觸國家考試正式系統平台之實際機敏性資料，相關電腦主機設施並備有嚴謹門禁管制措施。

周委員志宏：有關因應政府資安人才需求，因考試及格新進公務人員職等較低，待遇不高，無法吸引資安人才，至於擬增設資安類科，也會因初任公職職等及待遇偏低而有相同情形，因此對中高層級技術層面人才的需求，只能透過進用聘用人員方式，因此聘用人員薪點轉換薪額比率就不能過低，此次調整雖稍有增加，但整體待遇並不高，能否以此聘到優秀資安人員，仍有疑慮。

許委員舒翔：有關擬增設資安類科，並非由考選部規劃，而是由用人機關提出增設考試類科需求，再由本部提報院會審查。

李委員漢銘：有關政府資安人力短缺，目前暫時不先推行資安職系，而先以資訊職系人員接受資安訓練後擔任專職資安工作，但資訊專業加給並不高，行政院刻正規劃依據資安業務等級提供資安工作獎金，過去公立大專院校可直接以稀少性專業人員聘用資訊人員，碩士畢業比照講師薪水約五萬多元，現在政府資安人力短缺，或可研議以稀少性專業人員聘用。

主席：

1. 本院及所屬部會資訊單位人數合計約 60 多人，各資訊單位均有人力不足與須處理資料眾多的情形，若能增加員額固然極佳，但若無法增加員額，就須考量鑑別資料的重要性、取捨並排定優先處理順序，關涉資訊同仁核心能力的培養與訓練，請保訓會研處。
2. 本院及所屬部會之資訊處理、委外管理及資安聯防等資訊業務，亟需互相協調統合辦理，請秘書長協調相關人力資源整合。

決定：1. 為提升本院及所屬部會資訊同仁核心能力，請保訓

會研辦相關訓練。

2. 請秘書長協調本院及所屬部會資訊業務相關人力資源整合。

貳、討論事項（無）

參、臨時動議（無）

散會：下午 4 時 55 分

主席　黃　榮　村