美國公務機關電子機密資訊系統面對內部威脅之政策規範簡介

刊登期別 2012年04月15日

美國公務機關電子機密資訊系統面對內部威脅之政策規範簡介

科技法律研究所
102年04月01日

壹、事件摘要

根據一項網路入侵案件的統計分析，約有80%的案件事來自於機關或企業內部人員，或是至少與內部人員有關。[1]然而，對於資通訊安全與機密資訊的維護，機關單位與人員把大部分的重心放在防範外來的入侵者，也就是外部威脅，反而忽略了內部員工對於資訊可能產生的潛在危害。[2]這些入侵案件的行為人大部分擁有合法存取控制資訊系統的權限，也就是因為這樣，內部威脅不易被發現。這就好比擁有大門鑰匙一般，正當合法從大門出入，以及從事本來就可以做的事，而不易被發覺。美國由於維基解密（WikiLeaks）事件的爆發，使政府對於機密維護的焦點，從外在攻擊的防止，轉聚焦於內部威脅的防範。

在美國，內部威脅並不是一個新的概念，公務機關本具備一定的管理措施；惟在維基解密案爆發後，帶給美國政府極大的衝擊，美國也全面檢討與創制新的因應作法，並於政策面、制度面與技術面等不同面向，進行積極的研究與合作。以下將引介美國之制度設計，藉此提供公務機關因應內部威脅議題之政策之參考。

貳、重點說明

一、內部威脅的定義與事件

有關資訊的價值，近來因內部威脅所帶來的損害類型已經隨著對於財產的定義與價值觀而產生變化。以產業為例，智慧財產權與企業機密，儼然成為內部人員所竊取的主要類型。企業可能因為智慧財產權或企業機密的外洩，導致企業喪失競爭力或甚至破產而關閉。如果把企業模型放大至國家或公務機關，「機密」對內部人員即成為最有價值的財產與籌碼，而公務機關可能因為內部威脅將機密外洩，造成對於國家、機關或人民產生公共安全，甚至是國家安全的危機。

（一）內部威脅的定義

外部威脅（External threat）」[3]係與內部威脅相對應之概念；外部威脅係指該威脅非由組織內部發生，而是由組織外部之人員或其他組織，透過一般的網際網路、互聯網系統，以未經授權之方式，對該組織之資訊設備，以植入惡意程式、或以駭客入侵等方式，進行侵入式的資訊系統攻擊，其目的係在於由外部取得該組織「有價值」的資訊。

為因應威脅，「威脅識別（Threat Identification）」成為威脅防禦之首要任務，按形成威脅的原因加以區分，大抵可分為「外部威脅（External Threat）」與「內部威脅（Insider Threat 或Internal Threat）」兩類。內部威脅係指例內部竊盜、系統失敗、惡意破壞、不遵守安全準則或是使用非法軟體等；相對外部威脅，係指自然災害，例如火災與地震，以及來自外部的惡意攻擊，例如盜賊、駭客、惡意程式，以及網路病毒等。[4]

「內部威脅」雖然被認知為威脅的一個種類，但是我國目前尚無對於「內部威脅」一致的定義。檢視外國對於「內部威脅」的定義，通常係指員工(含約聘僱人員)、或委外廠商為了個人利益、間諜活動或報復之意圖（「惡意（Malicious）」），對於資訊進行不正當之存取控制。「美國電腦緊急應變團隊（Computer Emergency Readiness Team, CERT）」認為內部威脅係指一位或多位具備存取控制（Access）的個人，意圖利用弱點侵入公司、組織，或企業的系統、服務、產品或設施，對於內部造成傷害。[5]「美國國防部減緩內部威脅計畫結案報告（Final Report of the

Insider Threat Integrated Process Team, US Department of Defense, DoD Insider Threat Mitigation）」，內部威脅係指未經授權存取控制國防部資訊系統的人員，可能為軍事人員員工（Military Member）、國防部一般僱員（Civilian Employee ）、其他聯邦機構員工，以及私部門等。[6]

由上述定義可得知，內部威脅係來自於組織單位的「內部」，如以行為人之意圖區分，又可細分為「惡意（Malicious）」與「過失」。因人員之過失所造成之內部威脅，大部分原因為人員對於資訊系統與之使用與管理不當所造成，例如，人員使用Email或即時通訊軟體，受到社交工程之攻擊，導致電腦被植入惡意程式或間諜軟體。另一則為本文所要研究的「惡意的內部威脅（Malicious Insider）」，係指內部人員利用合法存取權限，為超出於其授權使用之對象、時間、範圍、目的，與用途等之行為，並意圖對於單位組織或是特定人、事、物等造成傷害，或是謀取不當利益。

依據惡意內部威脅事件，大約可分為以下各類型：[7]

1.IT破壞（IT Sabotage）

現任或前任僱員、承包商，或業務合作夥伴，以故意超過或誤用授權級別，而存取控制網路或資訊系統或資料的方式，意圖損害一個具體的個人或組織，或該組織的數據、系統或日常業務之運作。

2.為經濟利益而進行盜竊或修改（Theft or Modification for Financial Gain）

現任或前任僱員、承包商，或業務合作夥伴，以故意超過或誤用授權級別，而存取控制網路或資訊系統或資料的方式，為經濟利益意圖竊取或修改機密或專有資訊。

3.為取得業務優勢而進行竊盜或修改（Theft or Modification for Business Advantage）

現任或前任僱員、承包商，或業務合作夥伴，以故意超過或誤用授權級別，而存取控制網路或資訊系統或資料的方式，為取得業務優勢而進行竊盜或修改機密或專有資訊。

4.其他（Miscellaneous）

現任或前任僱員、承包商，或業務合作夥伴，以故意超過或誤用授權級別，而存取控制網路或資訊系統或資料的方式，為非基於經濟利益或業務優勢，而進行竊盜或修改機密或專有資訊。

或通常會涵蓋二種以上的類型，例如：員工先行對於IT系統進行破壞，然後再試圖敲詐僱主，以協助他們恢復系統為條件換取金錢。另曾有案例為，一名前副總裁於結束工作前，複製客戶數據庫與銷售手冊，再向其他外單位組織兜售。[8]

（二）內部威脅事件的發生與所造成的損失

依據CERT於2011年4月對於內部威脅控制的報告指出，以報告中123件資訊科技破壞（IT Sabotage）事件進行統計，內部威脅發生的時間為26%件事件發生於上班時間，35%發生於下班時間，另外39%件事件發生於不確定的時間。另外一項以內部威脅受到攻擊的地點來看，54%事件發生於進行遠端連線時，27%發生於公司所在地，另外19%發生於不特定之地點或場所。[9]

有關內部威脅對於公務機關機密維護所造成的危害嚴重程度很難估計，可能是因為內部威脅事件提報執法單位或是司法機關得比例較低。內部威脅事件通常因為證據不足、損害程度與花費於司法程序之時間、人力與費用無法平衡，或是因為提報對於公務機關的形象與信譽可能產生極大的負面影響，所以通常對於事件大抵只有表面上概略之描述。[10]

二、美國歐巴馬政府面對內部威脅之政策規範

美國傳統對於機密資訊由軍事單位依照軍事規定處理，不過，自從羅斯福總統於1940年發布第8381號行政命令，改變了這個機制。第8381號行政令，授權政府官員保護軍事與海軍基地。爾後，歷任總統以發布行政命令的方式，建置聯邦政府的機密分級標準。不過，羅斯福總統以經特定法規授權為由，後續總統則是以基於一般法律與憲法授權。[11]國會則不停的以其他立法，[12]設法平衡總統權利。

歐巴馬總統上任前歷經2001年911事件的壓力，[13]以及2010年維基解密等機密外洩事件，致使歐巴馬團隊對於資訊安全以及機密維護非常重視，除了推動開放政府（Open Government），促進政府政策更公開透明的民主治理外，對於資通訊安全（Cyber Security）、機密資訊外洩的通報機制，以及內部人員（Insider）所帶來的威脅，更是採取積極的作法。[14]

針對內部人員對於國家安全與機密外洩的問題，歐巴馬政權立即採取相對應的措施，於2011年發布第13587號行政命令：「增進機密網路安全與機密資訊有責分享及安全維護的結構性改革（Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information）」，與因應第13587號行政命令所規範之「內部威脅」議題，於2012年11月21日發布「國家內部威脅政策和機關內部威脅方案的最低標準（National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs）」的總統備忘錄。

部會或機關紛紛對於內部威脅採取相關防範措施，例如國務院（Department of State）對於涉及機密的網路，採用新的審查與監控的工具，而在國防部（Department of Defense）也開始開發自動偵測內部威脅的辨識系統。在情報系統方面，商務部（Department of Commerce）國家標準與技術中心（National Institute of Standards and Technology, NIST）與司法部（Department of Justice）聯邦調查局（Federal Bureau of Investigation, FBI）也訂立內部威脅指引，提供企業與機關單位遵循。情報系統委託Carnegie Mellon University的電腦緊急應變團隊（Computer Emergency Readiness Team，以下簡稱CERT）內部威脅中心（CERT Insider Threat Center）進行多項內部威脅的研究。

至今為止，歐巴馬政權對於內部威脅的防範，於法制政策提出下列各項規範：

（一）總統第13587號行政命令：「增進機密網路安全與機密資訊有則分享及安全維護的結構性改革」

由於維基解密事件的爆發，使美國將機密的維護，從對於防止外在的攻擊，轉聚焦於機密資訊的內部威脅。事件發生後，國家安全人員馬上成立跨機關小組，檢視處理機密資訊的政策與實務作法，希望可以提出解決行政部門可共用的機制，以減少類似的事件再度發生。

跨機關小組歷時七個多月的檢討後，對於機密資訊的保護，與涉及機密資訊人員或機關間合理使用與分享資訊提出下列原則：加強跨機關資訊有責共享的重要性；確保政策、流程與技術的安全解決方案，與監督和組織文化的發展；強調聯邦政府對於資訊必須實施一致的作法；與確保隱私、公民權和自由的保護。[15]

歐巴馬團隊將上述原則落實至第13587行政命令，[16]成立監督的架構，發展與落實涉及機密的網路與資訊共享的政策與標準。指示各機關必須負起安全與機密維護的責任，並加強跨機關資訊的流通與保護，包括電腦網路的安全，與內部威脅的機制，以減低未來國家安全機密外洩的風險。

第13587號行政命令大抵分為下列各大項，除此之外，聯邦政府同時已經採行增進機密資訊網路與人員的控管，例如拆卸式媒體、網路身分管理、內部威脅方案（Insider Threat Program）、存取控制的管控（Access Control）、機密網路的審核，[17]項目分為：

1.機密資訊電腦網路系統之安全維護各機關單位負擔重要的責任；

2.設置「資深資訊分享與安全維護推動小組（Senior Information Sharing and Safeguarding Steering Office）」；
3.成立「機密資訊流通與保護局（Classified Information Sharing and Safeguarding Office, CISSO）」；
4.設置「維護網路機密資訊執行秘書」(Executive Agent for Safeguarding Classified Information on Computer Networks)；與
5.設置「內部威脅專責小組（Insider Threat Task Force）」。

其中有關「內部威脅專責小組」的部分，跨機關的內部威脅專責小組將負責制定一個廣泛適用於公務機關內部威脅的方案。該方案的目標係為防止、檢測和減輕，包括利用、損害，或其他未經授權揭露機密資訊的內部威脅，並同時考量各機關單位所涉及的風險層級、業務與系統需求。解決方案亦應包含因應內部威脅的政策目標，建立和整合機關內部的安全與反間諜，用戶審查和監控等優先事項，以及其它機關的實作發展和保護能力。[18]除此之外，內部威脅專責小組還必須與相關單位合作，以促成政策的草擬與可行。[19]

專責小組的職責應包括下列：
1.制定並與行政機關協調，阻止、檢測和減輕內部威脅的政策，並提交至督導委員會檢閱；
2.與適當的機關合作，制定行政機關內部威脅方案的政策指引和最低標準，並於一年內發布，該相關指引和最低標準對於行政部門具拘束力；
3.如果有足夠的經費或經授權，繼續與適當單位合作，於一年之後，增修相關指引與最低標準；
4.如果沒有獲得足夠的經費或授權，建議由預算辦公室（Office of Management and Budget）或國家檔案與記錄管理局（National Archives and Records Administration）的資訊安全監督辦公室（Information Security Oversight Office, ISSO）於一年之後頒布相關指引與最低標準的增修版本；
5.如仍有任何未解決的問題，以致於延宕最低標準的公布，應將問題提交給督導委員會（Steering Committee）；
6.按照專責小組所制定之方案，獨立評估相關機關單位是否適當的落實既定的政策和最低標準，並將評估結果向督導委員會提報；
7.提供機關單位援助，包括提供最佳實作案例以供參考；與
8.提供美國政府所分析的內部威脅新的困難與挑戰。

由上可見，第18537號行政命令勾勒出美國政府對於增進涉及機密網路與機密資訊網路的結構性改革。不但成立跨機關的內部威脅專責小組負責草擬內部威脅的政策，機關亦必須依照指示時程，落實內部威脅政策的偵測方案，以及監控其運作是否符合政策的目標。

（二）「國家內部威脅政策和機關內部威脅方案的最低標準」總統備忘錄[20]

雖然第13587號行政命令規定機關針對內部威脅將組成跨機關內部威脅小組，負責偵測與避免內部威脅，以增進對於機密資訊的保護，以及減低機密資訊被未經授權的存取控制或揭露的潛在弱點。然而，機關應該如何施行的細項尚未有細緻規範，仍需等待歐巴馬團隊進一步制定，以落實於聯邦政府所屬的公務機關。

緣此，美國總統歐巴馬於2012年11月21日發布「國家內部威脅政策和機關內部威脅方案的最低標準的備忘錄（National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs）」，主要提供行政部門於防止、偵測與減低內部人員可能造成國家安全的威脅相關遵循方向與指引。因應內部威脅的能力將增進行政部門對於機密資訊的保護，並加強危及國家安全的敵對勢力或內部威脅的防禦。

這些威脅包括潛在的間諜活動，對國家或機關單位的暴力行為，以及未經授權揭露機密資訊，包括透過的美國政府互聯的電腦網路和系統處理的大量機密資料。該標準將提供機關單位建立有效的內部威脅所必要的要素。

目前標準的詳細內容尚未發布，不過，依據備忘錄大約可分為下列各項：
1.蒐集、整合、集中分析和應變主要威脅相關的資訊；
2.監控人員對於機密網路的使用；
3.提供人員對於內部威脅意識的培訓；
4.保護人員的公民、自由和隱私權。

參、事件評析

觀察美國一連串的改革，顯見維基解密事件對於美國政府產生非常大的衝擊，更加凸顯監控內部威脅對於國家與公務機關及其機密維護之重要性。歐巴馬團隊不但全面檢視其機密資訊管理與保護政策與法制，對機密資訊的管理與「內部威脅」的防範進行全面檢討，並對於配套標準及措施進行增修。

除對於傳統以人員監督威脅的存在外，應利用科技技術監控或查核人員的「異常」行為(如短期內大流量下載檔案/進入系統的紀錄、大流量轉出有附件的信件、近日來消費能力顯著高於所得或情緒異常低落或起伏極大等)或預定特定的現象作為潛在威脅的表徵證據，再進一步因應與確認內部威脅的存在。

最重要的是，該制度與措施要求全國公務機關一起合作落實，以及分享潛在內部威脅的異常警訊，才能真正達成減低公務機關對於內部威脅的防範。

[1]行政院退除役官兵輔導委員會，張維平，*日晷第4期認識公務機關資訊安全問題*，取自http://www.vac.gov.tw/files/Sundial-4Th_17.pdf（最後瀏覽日：2012年11月30日）。與公務機密維護宣導 --【從資安看如何防止公務機密資料外洩】近年來，隨著間諜軟體、木馬程式、釣魚網站等惡意攻擊日漸猖獗，世界各地傳出多起嚴重的資料外洩事件，當然台灣也不能倖免。外洩的資料包羅萬象，而其中最主要的內容是個人資料。資料外洩的起因不僅止於駭客所發動的各種資安攻擊，另外還有最令機關防不勝防的內賊。只要有心，要在機關內部竊取資料很容易，從辦公桌上亂放的機密文件、電子郵件、即時通軟體、網路硬碟、隨身碟，都可當作工具，如果機關（各單位）沒有危機意識，採取防範措施，資料外洩在所難免。鑑此，籲請各單位安全連絡員，加強單位自主管理，協助單位主管加強責任區安全檢查，共同維護機關公務機密與安全。
[2]中廣新聞網，*海軍共諜案，國防部：才在發展階段，影響有限*，（2012年10月29日），取自http://tw.news.yahoo.com/%E6%B5%B7%E8%BB%8D%E5%85%B1%E8%AB%9C%E6%A1%88-%E5%9C%8B%E9%98%B2%E9%83%A8-%E6%89%8D%E5%9C%A8%E7%99%BC%E5%B1%95%E9%9A%8E%E6%AE%B5-%E5%BD%B1%E9%9F%BF%E6%9C%89%E9%99%90-023752078.html（最後瀏覽日：2012年11月30日）。
國防部軍事發言人羅紹和表示，涉案的海軍大氣海洋局前政戰處長張祉鑫，在退役後透過友人介紹，認識中共官方人員，然後再透過軍中舊識，「謀取不法利益」，保防安全部門在今年三月間接獲檢舉，依法由反情報單位展開調查行動，並移請檢調單位協助調查，順利破獲本案。
[3]IT Law Wiki , *External Threat* , available at http://itlaw.wikia.com/wiki/External_threat (last accessed Jan. 12, 2013).
[4]碁峰資訊，*資訊安全概論與實務*，取自http://epaper.gotop.com.tw/pdf/AEE030900.pdf（最後瀏覽日：2012年11月30日）。

[5]NIAC, *The National Infrastructure Advisory Council's Final Report and Recommendations on The Insider Threat to Critical Infrastructure* , (April 8, 2008), last available http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf (last accessed Jan. 12, 2013).
[6]US Department of Defense, *DoD Insider Threat Mitigation-Final Report of the Insider Threat Integrated Process Team* , available at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380 (last accessed Jan. 12, 2013).
[7]Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J.Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition-Version 3.1,* at 11, (Jan. 2009), available at www.cert.org/archive/pdf/CSG-V3.pdf(last accessed Jan. 12, 2013).
[8]Dawn Cappelli, Andrew Moore, Randall Trzeciak, and Timothy J.Shimeall, *Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition-Version 3.1* , at 12, (Jan. 2009), available at www.cert.org/archive/pdf/CSG-V3.pdf(last accessed Jan. 12, 2013).
[9]The Cyber Adviser, *Invensys Critical Infrastructure & Security Practice,* at 1, (Dec. 2011), available at http://iom.invensys.com/EN/pdfLibrary/CISP_Dec2011_vol3_Newsletter.pdf (last visited Jan. 10, 2013).
[10]U.S. Secret Service and CERT/SEI, (Jan. 2008), *Insider Threat Study: Illicit Cyber Activity in the Government Sector* , at 5, available at www.cert.org/archive/pdf/ insiderthreat _gov2008.pdf (last visited Nov. 30, 2012)
[11]Jennifer K. Elsea, *The Protection of Classified Information: The Legal Framework,* CONGRESSIONAL RESEARCH SERVICES, at 1, Jan. 10, 2011, available at www.fas.org/sgp/crs/secrecy/RS21900.pdf(last visited Nov. 30, 2012).
[12]Id., at 2, 例如「1966年政府資訊公開法 (Freedom of Information, FOIA)」，「1995年情報授權法 (Intelligence Authorization Act)」、「2000年公共利益解密法 (Public Interest Declassification Act)」，與「2012年減少過度加密法 (Reducing Over-Classification Act)」。
[13]Paul Kenyon, *The Enemy Within: Obama's Insider Task Force*, Forbes, (Apr. 13, 2012), available at http://www.forbes.com/sites/ciocentral/2012/04/13/the-enemy-within-obamas-insider-threat-task-force/ (last visited Nov. 30, 2012).
[14]FEDERATION OF AMERICAN SCIENTISTS, *Obama Administration Documents on Secrecy Policy* , available at http://www.fas.org/sgp/obama/index.html (last visited Nov. 30, 2012). 歐巴馬政權針對機密資訊發布多項正式文件，以年度區分，截至2012年11月30日止，包括下列：1.2009年：「機密資訊和受管控的非機密資訊的總統備忘錄 (Presidential Memorandum on Classified Information and Controlled Unclassified Information, May. 27, 2009)」、「第13526號行政命令-國家安全機密資訊 (Executive Order 13526: Classified National Security Information, Dec. 29, 2012)」，與「國家安全機密資訊施行令的總統備忘錄 (Presidential Memorandum on Implementation of the Executive Order on Classified National Security Information, Dec. 29, 2009)」；2.2010年：「第13549號行政命令-國家、地方、部落，和私部門實體的國家機密方案 (Executive Order 13549: Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, Aug. 18, 2010)」與「第13556號行政命令-受管控的非機密資訊 (Executive Order 13556: Controlled Unclassified Information, Nov. 4, 2010)」；3.2011年：「第13587號行政命令-增進機密網路安全與機密資訊有責分享及安全維護的結構性改革 (Executive Order 13587: Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Oct. 7, 2011)」；4.2012年：「國家內部威脅政策和機關內部威脅方案的最低標準備忘錄 (National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 21, 2012)」。
[15]THE WHITE HOUSE, *Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks,* (Nov.2011), available at http://www.whitehouse.gov/the-press-office/2011/10/07/fact-sheet-safeguarding-us-governments-classified-information-and-networ (last visited Nov. 30, 2012).
[16]Exec. Order No. 13,587 (2011), available at http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks- (last visited Nov. 30, 2012).
[17]THE WHITE HOUSE, *Fact Sheet: Safeguarding the U.S. Government's Classified Information and Networks,* available at http://www.whitehouse.gov/the-press-office/2011/10/07/fact-sheet-safeguarding-us-governments-classified-information-and-networ(last visited Nov. 30, 2012).
[18]Exec. Order No. 13,587 (2011), available at http://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-structural-reforms-improve-security-classified-networks-(last visited Nov. 30, 2012).
[19]Id. 專責小組應該與總檢察長（Attorney General）與國家情報局主任（Director of National Intelligence）或指定人共同擔任主席。內部威脅專責小組成員應該由國務院（Department of State）、國防部（Department of Defense）、司法部（Department of Justice）、能源部（Department of Energy）、國土安全部（Department of Homeland Security）部長所指定的人員，以及國家情報局主任（Director of National Intelligence）、中央情報局（Central Intelligence Agency），和國家檔案與記錄管理局（National Archives and Records Administration）的資訊安全監督辦公室（Information Security Oversight Office, ISOO）等所組成。工作人員必須由聯邦調查局和國家反情報辦公室長官（Office of the National Counterintelligence Executive, ONCIX）和其他機構，於法律所允許的範圍內配置。這些人員必須是官員，或是兼職或終身全職的美國員工。國家反情報辦公室必須提供內部威脅專責小組適當的工作場所，以及行政支援。
[20]美國總統依美國憲章擁有直接發布據法律效力的文件（Document），文件的種類根據事務類型之不同分為三大類：Executive orders（有連續編碼的行政命令）、Proclamation（公告）、Administration orders（無編號的行政命令），其下尚有不同的子分類，備忘錄則屬Administration orders下的子分類之一，總統所發布的文件效力相同，並無位階之分，http://www.archives.gov/presidential-libraries/research/guide.html（最後瀏覽日：2013年1月12日）。

許慧瑩 編譯整理

上稿時間：2013年06月

推薦文章