國際個資保護發展趨勢與標準規範

國家資通安全會報技術服務中心

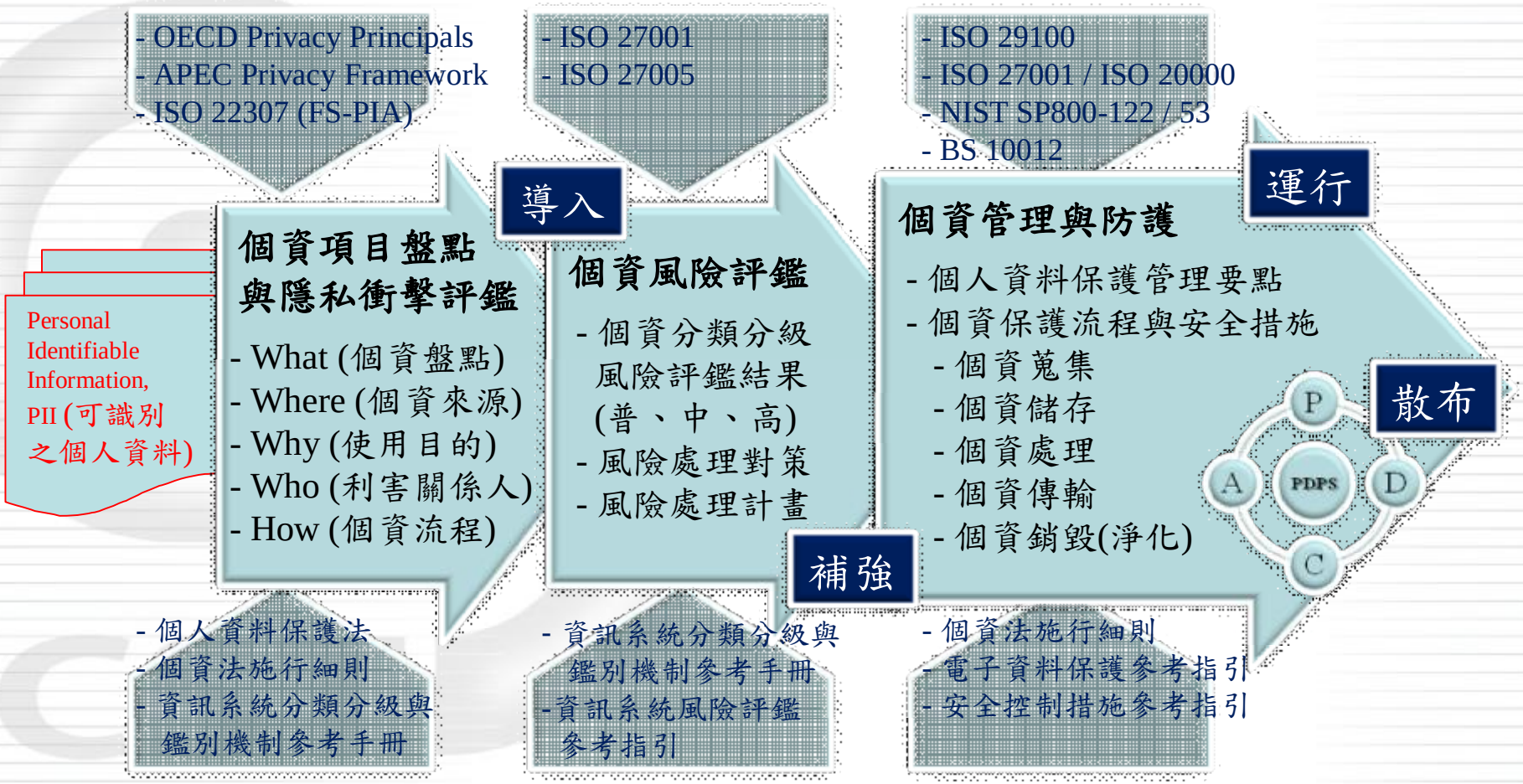
101/04/13

大綱

- 個資保護發展趨勢與標準規範
- APEC隱私保護9項原則
- OECD隱私保護及個人資料之國際傳輸指導方針預期效益
- ISO 29100隱私架構
- BS 10012
- SP800-122
- 結論

個資保護發展趨勢與標準規範

國際個資管理發展趨勢、標準、作法



國內個資相關法律、規範、標準、指引

OECD隱私保護及個人資料之國際傳輸指導方針

ÿ 1980年9月23日經濟合作暨發展組織(OECD)發布「 OECD 隱私保護及個人資料之國傳輸指導方針」，該方針已成為各國制定隱私權保護法案之依據，主要原則如下：

限制蒐集原則(Collection Limitation Principle)

對於個人資料的蒐集應有所限制，且應以合法、公正的手段，並經當事人同意始得蒐集

資料品質原則(Data Quality Principle)

個人資料之利用預符合蒐集目的，並保持正確性與完整性，當內容異動時即時進行更新

目的明確原則(Purpose Specification Principle)

蒐集個人資料之目的應於蒐集時即明確指定，且使用上不得有不符目的之情況產生

限制利用原則(Use Limitation Principle)

除當事人同意或法律另有規定外，個人資料之利用不得為特定目的以外之利用

安全保護原則(Security Safeguards Principle)

個人資料應受合理的保護，以防範因資料遺失、損壞、未授權存取/使用/變更/揭露等造成之風險

公開原則(Openness Principle)

對於個人資料的蒐集、處理及政策制定，應以公開為原則。資料管理人聯絡資料、資料種類及使用目的，亦需公開並容易取得

個人參與原則(Individual Participation Principle)

當事人有權從資料管理者取得或確認是否擁有自己的資料、瞭解個資內容，並可請求刪除或更正資料內容

責任原則(Accountability Principle)

資料管理者必須遵守上述各項原則

APEC隱私保護9項原則

Ÿ 緣起於1998年電子商務行動計畫，要實踐電子商務相關技術與政策，必須建立安全、保密且可信賴的通資訊及傳輸環境，並重視隱私議題。主要原則如下：

預防損害

防止個人資料遭到濫用而造成當事人之損害。因此，對於個資蒐集、利用及傳輸時，受到威脅損害的可能性與嚴重性，應有適當的改善措施

告知

個資管理者對於所蒐集與持有的個資，應向當事人提供清楚且容易取得的隱私保護政策聲明。並確保當事人佔已知悉個資已被蒐集與利用目的

蒐集限制

個資蒐集應限於與蒐集目的相關的範圍，依合法與正當方法為之，並在適當的情況下告知當事人或取得其同意

個人資料之利用

個資利用限與蒐集目的一致或相關範圍，惟以下情況不在此限：

- 當事人同意
- 法律明文規定
- 應當事人要求所提供的服務或產品所必要者

當事人自主

個資管理者應提供當事人可就其個資之蒐集、利用及揭露，進行選擇的機制。此機制可以電子、書面或其他方式為之

個人資料之完整性

個資管理者有義務維持個人資料的正確性與完整性，並更新個人資料

安全管理

個資管理者應妥善保護個人資料之安全，並應定期檢視與重新評估該保護措施

查閱和更正

當事人有權查詢與更正其個人資料，除非有下列情形：

- 基於法律或安全理由
- 為保護商業秘密而不應揭露
- 他人之隱私會受到侵害

責任

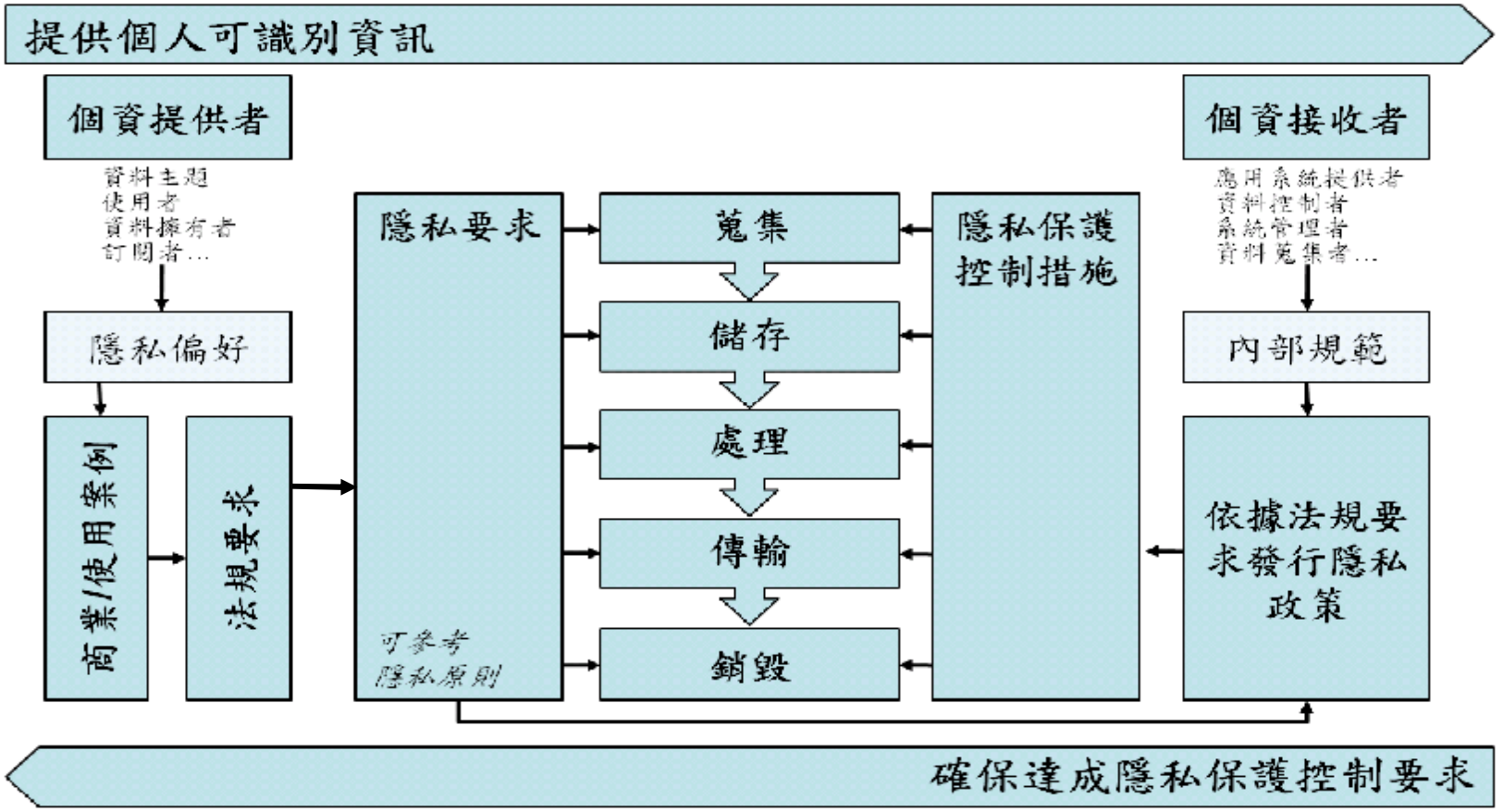
個資管理者應負責維保以上原則之實施；於傳輸至第三方時，應取得當事人同意或盡力確保第三方會採取以上原則保護個人資料

個資法與APEC隱私保護原則之對照

APEC資訊隱私保護9項原則	個資法條款
預防損害(Preventing Harm)	§12、§18、§27~§40
告知(Notice)	§7~§9
蒐集限制(Collection Limitations)	§6、§15、§19、§53
個人資料之利用(Uses of Personal Information)	§5、§16、§20
當事人自主(Choice)	§3、§10、§11、§13
個人資料之完整性(Integrity of Personal Information)	§11
安全管理(Security Safeguards)	§27
查閱和更正(Access and Correction)	§3、§10~§11、§13、§17
責任(Accountability)	§21

ISO 29100隱私架構

- 公布日期: 2011年12月5日。
- 規劃個資提供者與接收者之間，有關個資蒐集、儲存、處理、傳輸及銷毀等作業流程內容



BS 10012:2009(1/2)

- 公布日期：2009年5月
- 主要依循自英國資料保護法，應用「Plan」、「Do」、「Check」及「Act」循環，提供一個保持與提升符合資料保護之法規與良好實踐之架構
- 規劃PIMS(Planning for a Personal Information Management System)：
  - 定義組織中PIMS的範圍與目的：例如建立個人資料保護要點
  - 建立個資管理政策：政策應聲明適用範圍，例如全組織或部分單位
  - 指派適當人員角色職責：例如指派一至多位專業人員負責平時運作
  - 提供足夠的資源：組織在建置、實施、運作及維護PIMS過程中，應提供所需的資源
  - 將PIMS與組織文化契合：例如與組織現有的管理制度、程序進行整合運作，降低對人員日常作業的衝擊影響
- 建置與運作PIMS ：
  - 指派負責人員：確保組織依據其個資管理政策，指派適當的負責人員
  - 識別與記錄個資的用途：個資之識別可從業務流程或服務目錄著手，主要辨別個資對於流程與活動利害關係人的風險，分析個資的類別，在其不同生命週期的型態、相關文件、支援系統及彼此間的介面，做為後續風險評鑑的重要輸入來源
  - 教育與認知：確保所有人員能夠認知其在處理個資時的職責

BS 10012:2009(2/2)

－風險評鑑：確保組織認知當在處理特定類型的個資時之相關風險

－其他PIMS日常運作活動：包括公平與合法的處理個資、告知流程、維持PIMS為最新狀態、當事人權利、個資保留與銷毀、委外處理流程、對第三方揭露、安全議題及資料正確性等資料

Ÿ監督與檢視PIMS ：

－內部稽核：例如稽核規劃、稽核員選擇及稽核要求等

－管理審查：審查項目應來自個資管理系統使用者之回饋意見、人員所發現並呈報之風險、稽核結果、程序審查紀錄、技術升級或更換的結果、主管機關的正式評鑑要求、抱怨處理及已發生的違反安全事故等

Ÿ改善PIMS ：

－預防措施與矯正行動：所有變更或改善的建議，應於實施前進行評估，以符合政策上的要求

－持續改善活動：透過稽核結果、矯正預防措施及定期檢視的作法，以持續改善PIMS的有效性

SP800-122摘要說明(1/7)

- 公布日期：2010年4月
- 公布機關：美國國家標準與技術局(National Institute of Standards and Technology, NIST)
- 說明
  - 提供聯邦政府機關及其相關委外單位，於執行個資保護時之參考建議
  - 除說明個資防護的重要性外，並以風險為基礎，建議各項防護措施與事故回應計畫(Incident Response Plan)
  - 第1章是介紹文件的目的與範圍、使用對象及文件架構
  - 第2章則是描述何謂個資，並如何找出組織所維護的個資
  - 第3章則說明當個資遭到不當的存取、使用及揭露時，如何決定衝擊等級因素
  - 第4章則提供保護個資機密性的控制措施，以降低個資被洩漏的風險(技術控制措施建議出自於SP800-53)
  - 第5章則提出如何發展個資事故回應計畫，並整合至組織現有的事故回應計畫中

SP800-122摘要說明(2/7)

- 個資辨識
  - 所謂個資乃由機關(Agency)所維護的個人任何資訊，包括用來區隔或追蹤個人身分的資訊，例如姓名、社會安全號碼、出生日期與地點、生物特徵(Biometric)紀錄等;任何已連結或可連結到個人的資訊，如醫療、教育、金融及雇用資訊
    - 個人身分號碼，例如社會安全號碼、護照號碼、駕照號碼、納稅人身分號碼、金融帳號及信用卡號等
    - 地址資訊，例如住家地址、電子郵件地址等
    - 個人特徵，例如影像、指紋、筆跡或其他生物特徵資料(如視網膜、聲音)等
  - 儘可能辨識出個資的可能來源(如資料庫、網路磁碟機分享、備份磁帶及承包商等)

SP800-122摘要說明(3/7)

Ÿ 個資運用

- 當進行個資蒐集、使用及保留時，應限制以完成工作所需的個資項目為主，並儘可能減至所需之最小程度
- 組織應定期檢視以往蒐集的個資以決定是否仍為組織業務所需，如組織可以制訂每年固定一天為個資清除認知日(Purging Awareness Day)
- 美國管理預算局(Office of Management and Budget,OMB)於M-07-16備忘錄中具體提出聯邦政府機關需遵守事項
  - Ø 檢視持有之個資，確保其內容是否正確、即時、適當及完整
  - Ø 機關運作過程中，於對個資最小需求的原則下，降低持有之個資數量
  - Ø 定期檢視所持有之個資
  - Ø 針對社會安全號碼不必要的蒐集，建立一個刪除計畫

SP800-122摘要說明(4/7)

- 個資分類
  - 個資應以衝擊等級(Impact Level)結果去評估其機密性，如此才可以套用適當的保護措施
  - 個資機密衝擊等級可分為低、中、高三種等級，分別表示當個資遭到不當的存取、使用及揭露時，對組織或個人的潛在損害程度
  - 本文件將列出組織於考量機密衝擊等級時之因素，以利組織擬定適當的政策(Policy)、程序(Procedure)及控制措施(Control)
    - 可識別能力(Identifiability)：組織應評估個資是否容易識別出特定的個人
    - 個資數量：組織應評估有多少個資數量，25筆與2千5百萬筆個資破壞的衝擊是不一樣的
    - 資料欄位的敏感程度(Data Field Sensitivity)：組織應評估個資欄位的敏感程度，例如，社會安全號碼或金融帳號的敏感程度通常勝於個人電話或郵遞區號

SP800-122摘要說明(5/7)

- 使用情境(Context to Use)：組織應評估個資的使用目的－個資被蒐集、儲存、使用、處理、揭露及散播的目的。相同的個資元素(Element)可能會因其使用目的而有不同的機密衝擊等級。例如，假設組織擁有兩組相同個資欄位(包括姓名、地址、電話)的清單，第1組清單為訂閱由組織發行一般利益(General-Interest)電子報的訂閱者，第2組清單為在執法機關的秘密工作人員，很顯然地，第2組清單若遭到侵害，對個人或組織的潛在衝擊，將明顯不同於第1組清單
- 保護機密性的義務：組織因法律、規範及其他命令的要求(如隱私法、美國管理預算局發行的指引等)，而有義務去保護個資。例如，美國人口統計局(Census Bureau)與美國內地稅務局（Internal Revenue Service , IRS）因受到法規要求而有義務去保護特定型態的個資
- 個資存取與存放位置：組織可考量授權存取的性質(Nature)與個資存放位置，例如，個資頻繁地由人員與系統存取，或是定期地被傳送到異地(Offsite)，那麼個資的機密性就有較多的機會外洩

SP800-122摘要說明(6/7)

- 個資保護
  - 並非所有個資都使用同一種方式保護，組織應依個資機密衝擊等級，實施適當的保護措施
  - 美國國家標準與技術局建議使用操作性(Operational)、隱私相關的保護與安全控制措施。
    - 建立政策與程序：組織應發展全面性的政策與程序
    - 實施訓練：人員被授權存取包括個資的系統之前，需接受適當訓練
    - 個資去識別化(De-Identifying)：當有關個人的全部紀錄(Record)不再需要時，組織得以透過移除足以識別個人的相關資訊，加以去識別化，使留下來的資訊無法識別出特定之個人
    - 使用存取實施(Access Enforcement)：組織可透過存取控制政策與存取實施機制(Access Enforcement Mechanisms)，如存取控制清單，以控制對個資之存取
    - 實施行動裝置存取控制：組織應禁止或嚴格限制使用可攜式或行動裝置存取個資
    - 提供傳輸的機密性：組織應保護個資傳輸的機密性，通常可透過通訊協定加密或傳輸前資料加密完成
    - 事件稽核：組織應監看影響個資機密性的事件

SP800-122摘要說明(7/7)

- 個資事故回應計畫
  - 個資破壞將對個人與組織造成傷害，透過有效的個資事故回應計畫發展，可將對個人與組織的傷害降到最低。此個資事故回應計畫內容應包括當發生個資事故時，該於何時與如何通知到個人、該如何進行通報、是否有改善方案等
- 密切協調
  - 保護個資機密性需有資訊系統、資訊安全、隱私及法律需求等相關知識
  - 由於相關的法律、規範及命令，通常較為複雜且會隨時間變化，因此，需就教於組織內的法務或隱私部門，以決定相關規定之適用性
  - 此外，一些新的政策通常需要技術安全控制措施來達成，故密切地協調組織內的個資相關專家(如隱私長、資訊長、資安長及法律顧問)，確保個資安全要求被妥適地施行，以預防個資外洩事故發生

SP800-122技術控制措施簡介(1/5)

- 存取控制實施(AC-3)
  - 組織能透過存取控制政策與存取實施機制(如存取控制清單)控制對PII(Personally Identifiable Information)的存取
  - 實施的方式有很多種，其中之一為執行以角色為基礎(Role-Based)的存取控制並進行設定，如此，每位使用者僅能存取該使用者角色所需的片段資料。另一種作法為僅允許使用者透過應用程式限制使用者對PII的存取，而非允許使用者直接存取包括PII的資料庫或檔案
  - 對儲存的資訊進行加密也是實施存取控制的選項之一
  - OMB M-07-16明確指出聯邦機構必須"使用NIST驗證過的加密模組，所有帶有聯邦機構資料的可攜式電腦／設備，除非該資料經由副首長或資深人員以書面形式確認為非敏感級"

SP800-122技術控制措施簡介(2/5)

- 職責分工(AC-5)
  - 組織對於存取PII應強制實施職責分工。例如，去識別化PII的使用者不該也被允許存取完整的PII
- 最小權限(AC-6)
  - 組織應強制實施嚴格的權限/特權設定或由所需的使用者(與代表使用者的執行程序)進行存取，以完成指定之作業。關於PII，組織必須確保需存取PII的使用者僅能存取最小的PII數量，以及從事工作任務所需的特權(如讀、寫、執行)
- 遠端存取(AC-17)
  - 組織可選擇禁止或嚴格限制遠端存取PII。如果允計遠端存取，組織應確保傳輸過程是經過加密
- 使用者基礎的協同合作與資訊分享(AC-21)
  - 組織可提供自動化機制以協助使用者決定對PII的存取授權是否符合存取限制

SP800-122技術控制措施簡介(3/5)

- 行動裝置的存取控制(AC-19)
  - 組織必須選擇禁止或嚴格限制來自於可攜式或行動裝置對PII的存取，如膝上型電腦、行動電話及個人數位助理 (PDA)，這些設備通常比非可攜式設備(如桌上型電腦)具有較高的風險。有些組織可能選擇限制對含有高衝擊性的PII進行遠端存取，如此，資訊就不會離開實體範圍。如果行動裝置被允許存取，組織需確保裝置被適當的保護，並定期掃描這些裝置以驗證其安全狀態(如使用最新的防惡意程式並啟動、作業系統完整更新)
- 稽核事件(AU-2)
  - 組織能監控影響PII機密性的事件，如對PII的未授權存取
- 稽核紀錄的檢視、分析及報告(AU-6)
  - 組織可定期檢視與分析資訊系統稽核紀錄，以發現影響PII的不當或不尋常活動的跡象；調查可疑的活動或可疑的違規；將發現報告給適合的主管並採取適當措施
- 識別與驗證(鑑別/Authentication)(機關使用者)(IA-2)
  - 使用者於存取PII之前，可被唯一識別與驗證。而驗證機制的強度需求一般而言應視系統與PII的衝擊等級而定。OMB-07-16規定聯邦機關必須”只有在使用雙因子驗證的情況下，始可允許遠端存取。其中一項驗證因子為所使用的設備需從獲得存取的電腦中隔離”。而且”對於遠端存取必項使用暫停功能(Time-Out)；行動裝置使用者在三十分鐘內沒有動作時，應重新驗證”

SP800-122技術控制措施簡介(4/5)

- 媒體存取(MP-2)
  - 組織可限制對包含PII的資訊系統媒體之存取，例如數位媒體(如光碟片、USB隨身碟及磁帶等)與非數位媒體(如文件或縮微膠片)。這當中也包括具有儲存能力的可攜式或行動裝置
- 媒體標記(MP-3)
  - 組織可標記包含PII的資訊系統媒體與輸出，以指示該媒體與產出該如何被散佈與處理。只要該媒體或輸出被保存在安全的環境下，這些特定的媒體或輸出可免予標記。至於標記的範例包括標示於列印出來文件的封面或貼標籤於數位媒體上
- 媒體儲存(MP-4)
  - 組織必須安全地儲存PII，不論是文件與數位媒體，直到該媒體經由適當的設備、技術及程序破壞或加工處理。例如，將儲存於可移動式媒體上的PII進行加密
- 媒體傳輸(MP-5)
  - 組織對於包含PII的數位／非數位媒體與行動裝置，在組織控制區域之外進行傳輸時，必須加以保護。例如，加密儲存資訊與將媒體鎖定固定的容器內

SP800-122技術控制措施簡介(5/5)

- 媒體淨化(MP-6)
  - 組織對於包含PII的數位／非數位媒體於丟棄或釋出再使用之前，應先予以淨化處理。例如，硬碟的消磁處理－使用磁場方式讓硬碟無法使用
- 傳輸機密性(SC-9)
  - 組織必須保護PII傳輸的機密性。最常使用的方式為通訊加密或傳輸前將資訊加密
- 靜態資訊的保護(SC-28)
  - 組織必須保護靜態下的PII機密性，所謂靜態資訊意指存於於輔助儲存設備的資訊，如硬碟、磁帶。通常是藉由加密這些儲存資訊來完成
- 資訊系統監視(SI-4)
  - 組織必須使用自動化工具以監視內部或網路邊界對PII的不尋常／可疑傳輸或事件。例如，使用資料遺失預防技術(DLP)

結論

- 國際組織如經濟合作暨發展組織(OECD)、亞太經濟合作組織(APEC)等，均已訂定相關規範，提供其會員國對於涉及個人隱私資料保護問題之處理原則
- 我國亦於99年5月26日公布「個人資料保護法」，在保障個人隱私資料，並兼顧新聞自由平衡下邁向新的里程碑，個資法強化了個資揭露、查詢及更正等的自主控制，同時也將「亞太經濟合作論壇(APEC)隱私保護綱領」所揭示的預防損害、告知及蒐集限制等9項原則納入規範，以迎接個資保護全球化時代的來臨