資通安全管理法修法說明會（產業界場次）

逐字會議紀錄

時間：109 年 12 月 23 日（星期三）下午 2 時 30 分

地點：臺大醫院國際會議中心 301 會議室（台北市徐州路 2 號 3 樓）

【主席致詞】(略)

【資通安全管理法整體修法重點】(略)

【交流討論】

主席林春吟高級分析師：

大家好，我大概看一下與會的機關，有一些應該是對資安這一塊蠻熟悉的，可是也有一些公司，我們猜測可能是公司自己想要了解資安法的作業，所以我們剛剛的說明可能對有些公司來說有點太淺，可是又顧慮到有些出席者對資安法可能不是那麼熟悉，所以我們做剛才那樣的說明，如果大家對資安法有什麼樣的疑問或看法，歡迎給我們建議。

待會我們的發言規則先講一下，如果有問題提問先舉手，讓我們把麥克風遞到您那邊，先說明您是什麼公司或哪個機關構，我們再做相關後續的交流。今天進行的方式，原則上還是就今天談的 1 個母法跟 6 個子法做討論。

首先先就母法的部分，我們這次修的主要有一些名詞定義，再來是財團法人的納管範圍可能會做調整，我們把上級政府的概念納進去，那一塊的影響是縣市政府那邊，中央部會比較不會有影響，針對母法的部分，有沒有哪一位有一些問題想要提出來的？（無）

再進到施行細則的部分，施行細則的部分主要把實施情形提報...(臺下舉手)。

數聯資安：

有 1 個問題提問，母法提到上級機關對所屬機關稽核，因為主管機關分一級機關、二級機關、三級機關，假如底下有所屬機關都要去稽核嗎？還是這個就是由他的主管機關來執行這項業務？

主席林春吟高級分析師：

原則上我們會分公務機關跟特定非公務機關，我們現在先以公務機關

舉例，公務機關如果有三層式的架構，最上面是「法」的主管機關也就是行政院，中間這層就是上級機關，原則上就是各部會還有縣市政府都會在這邊，其他的都屬於公務機關。在法裡面我們賦與上級機關稽核他的所屬，在實務上有些上級機關會先盤它的所屬機關有多少個，它的所屬機關因為資安等級不一樣，所以要區分出每一個稽核頻率也不一樣。

因為上級機關下面還有二級、三級、四級，也有實務上會分層授權請他的下一級先稽核它下面的機關，在縣市政府比較常看到的，可能是教育局先稽核國中小學，整個縣市政府那一塊，可能是資訊單位去稽核他的民政局、財政局，原則上我們希望大家先盤出來你的所屬機關有多少個，你怎麼去分類或規劃你的稽核頻率。

以行政院來說，目前我們規劃 2 年會稽完我們所屬二級跟直屬三級，這個就是我們的稽核規劃，我們也希望上級機關用這種方式去規劃出來，然後照表操課就可以了。

(繼續修法說明)細則的部分，原則上我們就是把實施情形提報標準化起來，之前我們的法裡面規定的就是所屬機關要跟他的上級機關提報他的實施情形，在實務上我們自己做過，提報實施情形沒有標準化的話，後面要處理其實是比較不容易的，目前我們也做一套管考系統，提供給大家到這個系統裡面填報。

你的上級機關可以看到你所屬機關的提報情況，就可以把這個作為你去稽核的參考資料，目前我們就是明訂進去法裡面，針對施行細則大家有沒有問題？（無）

分級辦法的部分，主要條文裡面我們要調整 C 級機關的定義，如果機關自己架 Mail、有建 AD 就把你歸到 C 級去，因為近期 Mail 跟 AD 的攻擊比較頻繁，我們會希望你的上級機關去統籌建 Mail 服務，你的 AD 併到上級機關的 AD 網域裡面，原則上我們不希望 C 級變多，以這樣的方式，希望大家可以趕快把一些資訊，還有資安的資源向上集中，不要那麼多機關都有系統，或者有架 Mail，那是資安上的破口，主要我們要調整是 C 級的定義讓它更明確。

另外在應辦事項裡面，我們有把 VANS 跟 EDR 導入納到應辦事項裡，其他是比較細節的部分。針對分級辦法大家有沒有問題？

數聯資安：

VANS 系統的部分，資安處這邊會不會提供 VANS 相關的格式給業者，因為很多機關可能會委託這些公司來發展他的資產管理系統，甚至做資安健診，後面一定會要求，這些資料要上到 VANS 系統，這就是會有資料轉換的問題，所以有關這些技術規格的部分，是不是會有管道提供給業者？

主席林春吟高級分析師：

有關 VANS 的部分，我們技服中心的網站有一個 VANS 專區，從去年開始就辦相關的說明會跟教育訓練，讓機關的同仁了解。另外我們也有邀請共同供應契約上面，有關資產系統的廠商，跟我們做介接測試，目前至少有 4、5 家有測試、連通 OK 了，如果各位有相關提供資產的服務，或者可以協助機關盤資產的軟體工具要跟我們介接，也可以跟我們聯絡，在那個網站上有一些聯絡資訊，原則上跟我們對測的，我們是希望國內的廠商，你們的產品是國外的產品也沒關係，可是不能是大陸廠牌的，我們的基本要求是這樣，如果你們要介接我們都歡迎。除了資產盤點的廠商，還有一些 GCB 的廠商或者是比較相關的，他們自己的軟體工具有資產蒐集的功能，都會找我們做一個聯繫，細節的部分就是那邊做處理，原則上就是這樣去做技術介接，如果機關那邊還有什麼需要，再反應給我們。

分級辦法的部分還有沒有？

台灣大哥大：

想請教關於資安弱點通報機制，導入行政院 VANS 這部分，針對特定非公務機關，其實我們依照主管機關的要求，以及國際一些標準的要求，我們已經自己導入一套弱點通報跟修補追蹤的機制，是不是可以讓非特定公務機關採用等同這樣的機制，而不侷限於一定要導入行政院的 VANS 系統？

主席林春吟高級分析師：

原則上我們會希望你們公司有這樣的議題，可以先跟我們的技服中心就技術面先確認。首先我們要先確認好你們做到什麼情況，因為之前修法說明會中，有些機關誤以為他們有，後來做細部了解的時候，發現大家的認知不太一樣。如果說你們有，我們再做細部的確認你們的機制，不過就整體弱點那一塊，我們還是希望可以做掌握，因為弱點未修補是近期比較大的破口，至少你們轉 CPE 格式上來那一段可能還是要做。還有沒有問

題？

中華電信：

針對這個法條上面看起來，弱點通報的機制好像沒有提到要提交資料，反而是端點的偵測有提到，法條上是不是會再做修訂？

再回去一下，問資通安全維護計畫，剛剛有提到，會在系統上面去提報，這個是指公務機關嗎？不包括特定非公務機關嗎？

主席林春吟高級分析師：

有關是不是要在 VANS 做一些資料提交的規定？因為目前 VANS 機制是必須要把你盤的彙整性資產資料上傳上來，才叫做介接，所以原則上那個上來後，一比對就大概知道弱點數量，那樣的資訊，原則上對我們來說就足夠了。至於機關的資產假設有 50 台，個弱點分布在哪邊？原則上只有機關自己才會知道，對我們來說我們只會知道這個弱點可能有 50 個設備有，至於在哪 50 個設備，就是機關自己才會知道，機關就要去做相關的防護或修補，那個責任在機關。

之前在講 VANS 的時候，機關還有 1 個疑慮，我們是不是就會開始追他們都要修復，原則上我們只會針對重大的弱點才會去追，像 10 月初的時候，我們就去針對 1 個微軟的漏洞去追大家的修補情況。平常的一些弱點資訊，因為原則上風險還是在各機關，所以各機關還是要自己注意，至於上傳資料這一段要不要做文字的調修，這個我們回去可以再評估一下，因為 EDR 是很明確，後續有資料提交的議題。

管考系統的提報方面，目前是讓公務機關上來填實施情形(不是維護計畫)，也有一些中央目的事業主管機關說他的特定非公務機關要上來填，原則上我們跟我們講，我們也是會開放使用，並沒有限制，可是我們沒有說一定要來這邊填，就是特定非公務機關那邊，原則上還是尊重中央目的事業主管機關。

中華資安國際：

想要請教一下 VANS 機制，剛剛有提到弱點資訊掌握，不管是 A、B、C 級或關鍵基礎設施提供者上傳的資訊，然後比對它的版本來判斷它的弱點，如果說某些系統上面，這個弱點有可能是無法修補，一般機關可能會採取一些補償性的防護措施，例如前端可能會架 WAF 設備或 UTM 設備來防護，在 CPE 資料上版本還是存在有一個弱點的版本資訊，有關於像

是這樣的部分，不曉得 VANS 系統有沒有 verify 的機制，來確定這個弱點是確切受到保護。

第 2 個問題，想請教，剛剛有提到，對於比較重大的弱點會要求機關進行修補，如果這個機關一直沒有修補的話，或者一直沒有回報修補的情況，不曉得資安處會不會有其他的措施來協助，或者催促這個機關進行修補？謝謝。

主席林春吟高級分析師：

首先在 VANS 系統上，原則上機關把它彙整性的資產資料上傳上來，我們比對完回饋下去，在資產弱點後面也可以備註它做什麼樣的處理，我們的弱點通知，原則上也只會通知 1 次。的確在實務上如果做修補以後，系統是沒有辦法運作的，所以它會用其他的方式做防護，只是你必須要有去做處理，在系統上是提供讓你註記，系統沒有辦法幫忙你確認是不是確實受到保護，原則上，至少你有處理這件事，你留下相關的處理紀錄，機關要確實監控這個風險的狀況有沒有做調整。

我們以 10 月那個例子，那 1 次我們公文下去，先調查回來，後面其實就是確認好哪個機關還有多少弱點還沒修補，後續不管是 Mail 還是電話，目前是先用這種方式去確認它的修補情況，或者是他會提報他什麼時候可以修補完成，像那 1 件事情我們就是追到底，如果它的時間押太久，原則上我們關切的力道就會強一點。一般來說就整個推動情況，還沒有遇到有不修補、不處理的情況。我們目前的做法就是一步一步，原則上還是讓機關處理，如果它真的有困難需要協助，我們就進去看需要什麼樣的協助，找他的上級機關一起，目前還沒有遇到都沒有合理的理由不處理的情況，原則上先用行政措施，在法上面也有相關的罰則、懲處，這些措施在真的必要時也是會動用的。

數聯資安：

有關 VANS 資料更新的頻率，有沒有律定要多久？還是說只要我電腦上面的版本系統變更，我就隨時要更新？

主席林春吟高級分析師：

目前我們還沒有特別的律定，我們有找幾個機關試行，主要就是看機關內部資產系統的機制，因為有幾家產品是已經可以作成設定，以設定的方式讓它自動把資料定期上傳，至於上傳的頻率，他們要每天都拋、每個

禮拜拋、還是每個月拋，我們現在也還在試。原則上我們就是定期的拋，看是不是 1 個禮拜拋 1 次，再來是可能有些弱點被揭露的時候，就即時拋上來比對一下，那個是機動的，目前比較明確的頻率還沒有明定下來，我們會看整個運作的狀況去處理。

VANS 介接，我們還是建議機關是採系統化的方式去介接，不要以人工作業的方式去處理會比較好。

金融業：

因為我們是業者，我們對於資安法有一些疑惑，想請主管機關幫我們解說。第 1 個問題，提到特定非公務機關，裡面名詞定義有講到只要實體資產、系統、網路，只要效能對國民生活或經濟有重大影響，所以我們想要了解，我們金融業未來會被納入納管範圍嗎？

第 2 個問題，因為我們現在是受到中央目的事業主管機關金管會的管理，他們在今年 8 月訂了金融資安行動方案，其實是跟資安法看齊，所以裡面很多措施幾乎是一模一樣，如果記憶有錯的話，再請先進幫忙指正，裡面有看到限制危害國家資通安全產品，在我們業者來說，我們要如何認定是危害國家產品。

第 3 個問題，在通報機制的部分，目前我們金融業，我是證券業，是依照證券通報應變辦法，這個通報應變辦法是跟以前的國家通報應變綱要看齊，所以是分為三級制，可是現在在資安法裡面是四級制，我想請教未來這兩邊會同步嗎？

第 4 個問題，有關於資安人力的部分，因為在金融行動方案中也提到資安證照這個議題，在目前的證照清單公布，只要使用的是 ISMS 證照或者是 DCM 的證照應該有參與 1 年有 2 次稽核的經驗，我想請問這 2 次稽核的經驗是怎麼認定，以上 4 個問題，謝謝。

主席林春吟高級分析師：

如果你們目前不是公營事業，也不是政府捐助財團法人，也沒有被金管會指定為關鍵基礎設施提供者，你們就不是資安法納管對象。目前看起來金管會針對金融那邊的管理，應該是另外以業務那一面向切入，做加強跟推動，可是目前你們並沒有被規範在資安法的範圍裡面。

金融業：

所以未來也不會規範在資安法裡面？

主席林春吟高級分析師：

就目前我們的規劃沒有要把你們納進來。

金融業：

因為我們業者很擔心，想要目前提前先因應。

主席林春吟高級分析師：

如果有那樣的議題，我們會先通知金管會，那他會再通知你們，不過目前可見的規劃範圍，並沒有那一塊。

危害國家資通安全產品，原則上有 1 個處理程序在，因為那一塊要考量因素比較多，所以廠商清單還沒有出來，目前最明確的政策方向是不要採購大陸品牌，再強調一次，大陸品牌的軟、硬體產品或服務，重點是大陸品牌，不是其他的品牌在大陸製造，是大陸品牌，這是目前的既定政策，如果你們金融業想要避掉這塊，原則上就是大陸品牌。

金融業：

包括陸資廠商嗎？

主席林春吟高級分析師：

對，再來要提醒，因為現在有一些產品裡面是大陸做的，只是拿台灣的品牌貼在外頭，那個也是要注意，有些機關的做法會讓提交產品的廠商去切結，它的產品裡面是不是有大陸的軟、硬體元件，那個俗稱叫「貼牌」，大家在拆或處理的時候，會發現裡面的東西就是大陸的，所以大家採購、使用的時候，要特別注意這一點，這個是已經發生的案例。

您剛剛講的證券通報應變辦法，我們再找金管會研究一下，這個也是資安事件通報嗎？

金融業：

對，目前是採三級制，是 follow 以前的國家通報應變綱要，可是問題是國家通報應變綱要都廢止了。

主席林春吟高級分析師：

好，這個我們跟金管會研究一下，儘量讓它一致，大家使用上會比較方便一點。

再來是稽核、證照，主要是 ISO 27001 LA，在資安法上規定每年要 2 次參與稽核作業相關經驗。在實務上，你們機關辦的內部稽核，這位資安專職人力要去稽核，不是被稽核，被稽核不叫參與稽核，是他去稽核其他

單位，或是擔任觀察員，主要是以稽核的角度來參與稽核活動的話，原則上我們就會做一個認定。

至於金管會怎麼認定，可能你們要跟他確認一下，他們是不是更嚴格。在資安法上，我們會確認這個資安專職人力參與的稽核是什麼，在實務上，上級機關要對所屬機關稽核，所以上級機關也會聯合他所屬機關的資安人力一塊組成稽核團隊，A 稽 B、B 稽 A，如果有辦法就跨機關，如果沒辦法就去稽核機關內部的其他單位，這個也是可以的。

金融業：

實務上稽核有可能 3 到 5 天，我可能擔任觀察員，在工作實務上可能沒有辦法 5 天全程參與觀察，可能只會參與 1 到 2 天，這樣就有符合主管機關資安法這邊的認定嗎？

中央目的事業主管機關未來看金管會怎麼講，可是想先了解主管機關的看法。

主席林春吟高級分析師：

原則上初期我們不會那麼嚴格的去判定，在公務機關我們去稽核的時候，不會像你們稽核那麼多天，你們可能連業務稽核是一塊辦理的，可是一般公務機關去稽核，可能一天或半天為單位，可能就是幾個單位去做稽核，所以在實務作業上我們不會採那麼嚴格，原則上他有參與我們就會認定。大家還有沒有問題？

中華電信：

附表十的部分，不過不在簡報裡面，營運持續計畫的部分，系統備份在高的等級裡面，有提到要跟運作系統不同地點的獨立設施，不同地點的部分有沒有距離的要求？譬如同一個區域，但是不同建築物，不同地點這個部分。

另外一個，也是在附表十的部分，原本的條款在系統開發階段要做滲透測試，系統開發階段，原則上是指到什麼樣的程度？因為系統開發階段，整個開發階段可能很長，這個可不可以稍微釐清一下？

主席林春吟高級分析師：

目前有關異地的部分，距離我們目前沒有明確的規範進去，因為我們這個法要適用的機關比較多，規定以後有些機關事實上可不可以達成，不太確定，之前大家在推 ISMS 的時候，異地備援有公里數，還要考量是不

是地震帶，有一些參考因素，如果機關可以的話，就以那個方式去做，在法規上，目前我們沒有明確的規定，至少要做不同地點的存放或儲存。

開發期間的滲透測試，提供其他機關的做法給你們參考，因為那個在實務上不盡然大家都是一樣的做法，有些機關是以上線做一個切分點，如果 1 個系統分階段上線，要上線前，在開發廠商那邊，等於要交出來前自己就要做過1次，或者在測試環境就要做，後面才可以上你的production，原則上，這邊在意的是你上 production 之前，一定要做過滲透測試，至於開發的過程中要不要做、要做幾次，那個就要去看，有些步驟比較嚴謹，可能開發一個階段就要去做，去確認相關程式碼的議題，各種可能性都有，至少在測試環境要上正式環境前一定要做過 1 次，確保你上線的東西是被檢視過的。因為實務上沒有什麼特定的標準答案在。

分級辦法的部分還有沒有？（無）我們再進行下去。通報應變辦法的部分，我們是將關聯性的事件，將上級機關可以另行通報，做一個統籌處理的機制明列進去，因為這個在實務的案例上也有看到，我們大概就是做這樣的規定，大家有沒有問題？（無）

稽核辦法的部分，剛剛同仁有講到，主要是本來規劃好的稽核規劃，可能因為一些不可抗力因素需要調整，這邊只是提供 1 個調整的彈性，在稽核的部分，原則上我們還是建議，主管機關稽核特定非公務機關還是會採實地稽核的方式辦理。有一些機關有提出來，是不是可以用視訊的方式處理，目前主管機關稽特定非公務機關的部分，還是以實體、現場的方式，只是辦理的方式或是時間上可以做一些調整，或者他們有一些建議、作法，可以提出來做彈性調整，法規只是提供那樣的處理彈性，大家有沒有問題？（無）

情資分享辦法，這邊也是有中央目的事業主管機關反映，他們在推動跟特定非公務機關之間的資安聯防，有一些情資分享，如果特定非公務機關分享比較重要、有價值的情資，希望可以給他鼓勵，可以有一個法源依據，所以我們在這邊列出來，讓中央目的事業主管機關可以做處理。有沒有問題？（無）

獎懲辦法，這邊跟公務機關比較有關係，原則上我們傾向是採獎勵，其實資安作業非常辛苦，做得好原則上是天下太平，所以常常就會被忽略掉，所以我們比較希望用獎勵的方式鼓勵大家，可是可能在有一些應辦未

辦，而且經提醒無正當理由又不處理的情況下，不得不的話，相關的懲處，我們檢討的範圍就不只是相關的人，我們會把相關作業的主管，跟它的上級機關納進去做一個檢討，看上級機關有沒有做到督導、協助的責任，機關為什麼會沒有辦法，讓這個應辦未辦的事情會發生，大概主要是這一點，大家有沒有問題？（無）。

還有沒有其他想要提問的？

中華電信：

在附表十的部分，系統與通訊保護那個段落，加密金鑰或憑證應定期更換，有加上「定期」兩個字，這邊想要了解的是，我們有一些已經加密儲存的檔案，也要定期解密再採用新的加密金鑰再做加密嗎？

主席林春吟高級分析師：

在適用上有這個疑義？這個部分我可能要回去詢問一下技術人員的建議，我跟他們確認一下，金鑰更換是確定的，但是不是那些東西要解開再加密 1 次，這個我們再確認一下，謝謝。

ACFD：

我要幫業者發聲，剛剛有談到我們業者因應國家政策，不要採購大陸的用品，這個是確定的。話又講回來，這一次美國連愛因斯坦花幾百億都沒有辦法做到這樣，我們國家有沒有 1 個機制，因為我們很多台商在那邊有幫大陸做產品，他也會在第三地做，可是業者的能量有限，所以我們對於故意、非故意或是應盡而未盡的責任，我們國家應該是把認為大陸的哪些產品都公告讓百姓遵守，國家力量有限，安全不是百分之百，國家都沒辦法做到的話，還要加諸我們業者一定要遵守，因為我們沒有能力，所以這個部分能不能採寬鬆？因為我認為很難讓業者沒有辦法 100％遵守，所以國家是不是有 1 個機制還有配套措施？這個配套措施怎麼做，就像剛才 VANS 一樣，你公告 1 個弱點，讓業者參考，讓業者不要不自覺陷入陷阱，政策我們都願意遵守，這是第 1 個。

第 2 個，107 年資安變成國安，所以有資安法，可是資安沒有 100％，能不能政府先發起資安保險，政府中央跟地方預算沒有編資安保險，ISO 27102 去年通過，為了減少業者的損失，政府是不是可以先編中央預算，因為我們國家到在現在都沒有編資安保險的預算，如果有編的話，產值就會出來，這個是我提以上的建議。

主席林春吟高級分析師：

您第 1 個議題點是大陸產品的？

ACFD：

剛才你解釋這個，業者願意配合，但是這個我們怎麼知道是不是 100％？

主席林春吟高級分析師：

可以做的我們盡量做，降低風險，我們從剛才就一直講是在降低風險。

ACFD：

所以政府要規範出來明文確定，指定那些可以買、哪些不能買，這樣對業者恐懼感才能降低。

主席林春吟高級分析師：

如果它是單純的議題，可能可以那樣處理。

ACFD：

政府都做不到了，讓業者怎麼做？

主席林春吟高級分析師：

我們也是要求政府部門這麼做。

ACFD：

那政府部門這麼做，能不能先公告那些產品不應該買，很難，做不到。

主席林春吟高級分析師：

它的議題如果比較單純，重點是它的議題不是那麼單純。

ACFD：

所以我建議配套就是 A、B、C，先公告 A 就是哪些產品不應該買的，B 部分，我的意思是說，讓業者恐懼感減少，風險降低，這個不是資安法的本質嗎？

主席林春吟高級分析師：

資安法是在規範納管對象的資安防護作業。

ACFD：

這個是建議，當然做不做得到，我是替業者講話。

主席林春吟高級分析師：

可以做的，我們會儘量做，有一些議題比較複雜一點，我們就是用比較能夠穩健往前走的方式去處理。

資安保險的部分之前有研議過，不過相關有一些環境條件還沒有辦法搭配，這個議題曾經被提出來過。

ACFD：

我推動 5 年了，我們這個協會，而且標準 ISO 27102 已經出來了，國際標準也有了，我是認為這樣做，今天可以達到修法整體的概念，對我們政府應該有幫助，謝謝。

主席林春吟高級分析師：

謝謝您。大家還有沒有？

台灣醫院協會：

我想問的是應辦事項中的資安弱點通報機制，如果我們這邊，我方是代表 CI 關鍵基礎設施提供者的話，我們要跟行政院做通報嗎？還是跟中央目的事業主管機關通報？還是以各領域所建置的平台做通報？

主席林春吟高級分析師：

有關 VANS 的部分，原則上全國目前就是這一套，介接就是介接到我們這邊，技服中心幫忙建的那一套，現在法上的 VANS 導入，原則上就是要跟這一套做介接。你剛剛講的通報如果是資安事件通報的話，是跟中央目的事業主管機關通報。

台亞衛星：

關於大陸設備採購的部分，這個部分可能不是單純文件切結，可能會衍生另外 1 個問題，很多政府採購案的部分，政府採購案有時候會規定不可以使用一些限制的設備，限制設備裡面任何的軟硬體或韌體，很難完全辨別它到底是不是大陸的產製，如果又涉及到標案，最後如果出了問題的話，廠商就會有責任。所以這部分還是請資安處稍微再研議一下。

主席林春吟高級分析師：

大概跟大家講一下有些機關的做法，因為產品除非很明確就是掛大陸品牌，不然產品有陸資，大家非常不容易判斷，曾經上新聞的，有關上層股權資金組成，那個很複雜，有時候會難以釐清。我們先就我們可以做的去處理，目前機關可以做的做法，如果大家有更好的做法也可以提出來，首先大陸品牌一定不能進來，投審會那邊有一個在台陸資廠商，原則上走

採購法的時候，資安或敏感業務相關的採購可以排除在台陸資，最難處理的是第三地有陸資，那塊不好查。

目前我看到實務上的做法，先請廠商做切結，我看到供應契約上就有幾條，首先廠商自己確認供應的產品裡面沒有，至於他的產品裡面有沒有，他至少要做初步的查證，畢竟他要把產品拿來賣給你，就是相關的責任要釐清，這個是前面採購要注意。在過程中也有可能那家公司賣給大陸，有可能中間轉換成陸資，這個是複雜、滾動的議題，在契約上，工程會範本中也有相關的條文，當你變成陸資的時候要跟甲方講，大家去後續對應的處理。

在危害國家產品清單裡面，揭露處理原則首先是不要買，機關裡面目前有的，就先隔開趕快汰換，這是處理原則跟步驟，當然不管是不小心或者是後來變陸資，問題到了，我們就面對處理它。

資安原則上就是風險管理，我們就是在降低風險，我們不會去期待沒有資安事件發生，所以我們平常準備的是，萬一資安事件發生以後，我要的通報應處是什麼，有關大陸產品的採購也一樣，就算大家再小心，你會不會不小心買到？不知道，萬一真的買到，後面有資訊出來的時候，就看怎麼去處理，至少在前面我們可以阻擋就先阻擋，這個是比較實務面的做法。還有沒有問題？

大考中心：

關於資通安全證照這個問題，我們原本是要求 4 張，如果我們只有 4 位專責人員有 4 張沒問題，假設我們專責人員有 10 位，依照修正我們要有 10 張以上嗎？還是 4 張就夠了？

主席林春吟高級分析師：

好像我們目前修法內容不是很好，大家會誤解，原則上，精神是如果你是 A 級，至少要配 4 個人，所以我們會搭配 4 張，我們是希望這 4 張分布在這 4 個人身上，不要派 1 個人去考證照的意思，所以最少 4 個人各持有 1 張，你們配 10 個、20 人都是優於規定，那我們可以寫優點，至少要有 4 個人各持有 1 張，那個文字我們再看怎麼修才不會造成誤解。

ACFD：

剛才有一個人回應，可以上網看一下行政院在 4 月 1 日有危害國家資通安全產品清單，5 月 1 日這個清單，我的意思是這個就是用紙本，能不

能像 VANS 作成軟體，我們一輸入比對後就知道，沒有，我們就不用負責任了，因為這個清單很多，但是都是紙本，5 月 1 日、4 月 1 日，業者有時候進口比較快，我的意思是政府也要負一點責任，不要讓我們業者承擔，所以作成一個軟體，像 VANS 一樣，像 VANS 也是資訊資產來做比對，這樣清單應該也可以做主動比對，萬一比對沒有在裡面我們又進口，業者不應該把他馬上處分，我這樣提可不可以我不曉得。

主席林春吟高級分析師：

這些作法，我們討論清單的時候，其實都已經討論過。

ACFD：

這個業者真的不能生存，因為你打資安產品禁止清單，都有行政院一些報表，裡面內容真的不錯，但是是紙本的，能不能做成 VANS？

主席林春吟高級分析師：

裡面應該沒有清單，目前清單並沒有公布。前 2 天有發一個文，正式明白揭露不要採購大陸的產品，目前明確的政策就是不要採購大陸產品。有關產品清單的問題，我們之前有研議過，不管清單公布不公布，然後提供大家查詢比對，採購上如何處理，細節我們都有討論過，可是在實務上有其他相關的議題，我們可以做，我們真的都會去做。

ACFD：

我要列入紀錄，我的名字也可以寫，寫了對歷史負責，做不到是另外一件事，我們提出來，政府說我做不到。

聯合報：

針對 A、B、C 級應辦事項，有關資訊人員以及資安專職人員，資安教育訓練部分，有規定資安專責人員要上 12 小時資安專業課程，以及資安專責人員之外的資訊人員每 2 年要上 3 小時的資安專業訓練，這個資安專業訓練的認定，在 FAQ 的 3.15 與 3.16 也講，可不可以講清楚一點，像今天資通安全管理法修法說明會，算不算我們資安專業課程訓練？因為上面有說一定要有教育。

主席林春吟高級分析師：

原則上我們這個修法說明會是資安的通識時數，專業課程是技術面。

聯合報：

我遇到一些機關還在盤點資訊人員今年到底有沒有符合 12 小時跟 3 小

時的，他就把上課都列出來，這個是資安處辦的，算不算？這邊可不可以清楚講一下，FAQ 3.15 有沒有資料，到底怎麼樣才算數。

主席林春吟高級分析師：

原則上我們在 FAQ 上就有列，第 1 個資安職能訓練，我們有讓一些學校去開課，如果你去上那個課，就會認定是專業的資安時數。第 2 個是巡迴說明會，我們在 12 月也有辦，通常 1 年會辦 2 次，上半年跟下半年，應該都有 3 小時。第 3 個，證照的課程，我們列了 1 個證照清單，如果去上證照課程的時數也可以算。第 4 個，公、私營訓練機構開設的資安管理或技術課程，所謂的公、私營訓練機構就是 FAQ 裡列的 4 種，他們辦的資安管理或技術課程都可以認定。

聯合報：

關於資安巡迴，據我所知資安巡迴不是人人都有辦法報名得上。這個我們可以確定，我們常常接到電話，常常聽到不好意思我們額滿了，好像有限定名額，因為我們想要幫所有的政府機關資訊資安專職人員 12 小時，以及資安專責人員之外的資訊人員每 2 年 3 小時的應辦事項，如果我們公司請了公、私營訓練機構的講師到那個機關去演講，講技術方面的課程，這樣可以認列嗎？

主席林春吟高級分析師：

原則上我們是訓練課程不是演講，像如果恆逸或某個大學到那個機關開專班，那個是可以的，1 個可能在學校，或者訓練機構開的班，有縣市政府通知所屬機關，找那些機構來開班，找所屬機關的資安人員、資訊人員來上，那個也會認。

聯合報：

訓練機構的講師，以私人的名義到機關來開班授課，這樣可不可以？

主席林春吟高級分析師：

原則上目前沒有開放這一條路。

聯合報：

所以一定要以訓練機構的名義到那邊開班授課。

主席林春吟高級分析師：

目前我們會扣著訓練機構去把關相關的教學品質。

聯合報：

謝謝。

ACFD：

行政法人有沒有包括社團法人？

主席林春吟高級分析師：

目前就是行政法人跟財團法人。大家還有沒有問題？

中華資安國際：

就剛剛教育訓練議題延伸一下，我們在承接政府的標案或企業的標案，在標案的內容裡面有些要求，我們對於業者提供教育訓練，如果按照這個辦法來看，資安業者所提供的教育訓練，就沒有納入課程的點數計算裡面，資安處可不可以考量一下，可不可以讓資安業者也可以納入時數的考量裡面？

主席林春吟高級分析師：

因為我們希望有一個比較客觀可以去確保、去認證教學品質，因為我知道有一些資安、資訊公司有一些上的課程，那個老師教的也很好，有些教的不是那麼好，它的品質比較難有衡量標準。所以我們目前沒有把那個開放出來，主要的點在這邊，當然專業性一定夠，但我們的重點會在它的教學品質，你自己很厲害，可是重點是你要讓你的學生聽懂，所以我們在意的比較是教學部分，看怎麼樣可以確保一定的教學品質成果，所以我們現在是扣著訓練機構來做這件事情。

您剛剛講的，除非你們有另外的，如果在業界也有類似衡量標準，也歡迎提供給我們，我們評估怎麼放進去，因為也有機關在反映，不管是資訊廠商或原廠，他們上的專業課程專業性也很夠，變成我們沒有辦法確保他們授課的老師是不是能夠有比較好的教學方式。

ACFD：

大學教授透過社團法人或法院登記可不可以算？

主席林春吟高級分析師：

目前我們沒有，如果是學術研究機構，可以用學術研究機構處理。

ACFD：

短期補習班會比一般國家社團法人強？我提議要採嚴格，我們政府要推動實驗室是 ISO 17025，有辦法訓練的機構，讓凡是有通過 17024 才可以，因為 17024 我喊了 5 年，國內現在沒有 1 個社團法人通過 17024 的教

材訓練，我再舉例一下 CEH 有、CISA 有，叫 17024。如果你踩這麼嚴格把國內很好的社團法人排除掉，我建議這個訓練課程應該以國際標準17024，不曉得林高分有沒有聽過，17025 是實驗室，17024 是針對人才訓練，符合國際標準。

以前我沒有注意這個規定，這樣對我們社團法人傷害很大，像我們數位鑑識協會推動好多年，在鑑識課程也是很出名的，這樣抹殺我們。

主席林春吟高級分析師：

有建議都可以提出來，若有缺漏，您可以提出來。

ACFD：

所以我說可不可以增加相關的社團法人？

主席林春吟高級分析師：

給我們一個建議的標準，不然社團法人很多。

ACFD：

標準你們訂就好，我不敢訂。

主席林春吟高級分析師：

大家還有沒有問題？（無）如果暫時沒有的話，大家可以用書面做交流，今天的修法說明會到這邊，謝謝大家。