資通安全管理法修法說明會（北區第 3 場次）

逐字會議紀錄

時間：109 年 12 月 2 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（臺北市徐州路 2 號 3 樓）

【主席致詞】(略)

【資通安全管理法施行情形及整體修法重點】(略)

【交流討論】

主席林春吟高級分析師：

待會我們先就剛才簡報跟大家詢問一下，還有沒有需要我們做說明的地方？剛才可能講的有點快或者意思不太清楚的地方可以先提問，如果簡報沒有問題的話，接下來我們會就母法、6 個子法逐一再跟大家徵詢意見，因為之後會做逐字稿，大家發言先舉手，要麻煩各位先報你的機關再開始說相關的問題，或用紙本反映意見也可以。

柯旻圻助理設計師：

剛剛我報告的簡報有沒有什麼疑問或問題？（無）我們進入修法這邊，我們先看母法主要有改的是名詞解釋，改比較大的是財團法人這邊，政府捐助 50%以下又沒被主管機關指定為加強監督的全國性財團法人就不是我們納管範圍，再來是公所和代表會部分，他們責任等級提報，還有地方制度法的作業都是對到上級政府，所以在公所、代表會的實施情形提報，統一提報到他們所在區域的上級政府。母法部分有沒有修法上的問題？（無）

細則這邊主要就是 1 個，公所、代表會的部分加上級政府，實施情形的提報方式用法條明訂，全國統一實施情形提報方式，是細則主要改的部分，細則這邊有沒有什麼問題想要發問？

主席林春吟高級分析師：

補充一下，實施情形提報，是法明訂每個機關都要提報，如果機關不太會填，上級機關願意幫忙你填的話，我們的系統也會提供這樣的功能，讓上級機關幫你填相關實施內容，我們用系統來做，會讓大家填的東西比

較標準化、一致性，這個資料原則上會作為上級機關稽核實施情形的參考資料，如果大家對填寫的功能或內容部分有一些建議也可以提供給我們，我們從系統統一調整，就不用每個機關自己重新設計一套，有關這個，大家有沒有想要再提出詢問或要給我們建議的？（無）

柯旻圻助理設計師：

學校的部分，人員的更動比較頻繁一點，想要申請管考系統帳號，可以發 email 到我們處這邊，就可以幫忙開立管考系統的帳號。

資安責任等級分級辦法，我們有修蠻多的，一個是 C 級的定義，把它明確，Mail Server、AD 這種不是開發的套裝系統，明訂就是 C 級，文字我們會再改，上面寫「使用」好像不太對，只是精神是機關有在維運、維護的 Mail Server 就是 C 級，再來就是應辦事項要增加一些項目，一個是 VANS，還有一個是 EDR，VANS 就是 A、B、C 級公務機關加上 A、B 級 CI 提供者，EDR 是 A、B 級的公務機關。分級辦法有機關有問題嗎？

財政部國有財產署：

依照剛剛的說法，有 AD、Mail Server 都會升級為 C 級機關，可能是 D 級或 E 級的機關，明年度的資安維護計畫要依照原本的等級填寫，還是新的 C 級填寫？

柯旻圻助理設計師：

我剛剛有講到責任等級的提報，現在還沒有修法，所以還是依照現行標準，之後修法就會調整，維護計畫的填寫也是一樣。

主席林春吟高級分析師：

我說明一下，我們不希望 C 級變多，可是最近因為 email 跟 AD 這部分的資安事件越來越高，所以我們不希望每個機關去架 AD、mail server，目前有這樣的情況。儘量找上級機關，儘量向上集中，趁這段時間調整好，在你的等級沒有被核定修改前，就是依現行等級去做相關維護計畫，實施情形相關作業都是依照現行等級，等於說我們現在在處理修法，也同步在調查責任等級提報，我們把修法的調查因素放進去，所以原則上你們還是依目前的等級定義去評估你們的等級，可是有一些屬性幫我們填上去，因為你們提報過來我們還有核定的動作，我們正式核定下去，那時候看等級有沒有變更，在沒有生效前就是依現在的等級去做相關的作業。

經濟部加工出口區管理處中港分處：

請問修正條文第 7 條，紅字的部分「未維運或使用」，我們有使用上級機關的系統，可是我們並沒有維運，這樣我們到底要算哪一個？

柯旻圻助理設計師：

「未維運或使用」，沒有維運就是 D 級，原則上有維運才是 C 級。

經濟部加工出口區管理處中港分處：

可是你的字是用「或」，是不是把它改成「及」，對我們 D 級會比較明確一點？

主席林春吟高級分析師：

我們其實是要先確認好 C 級，D 級的部分是扣掉 C 級的部分就會落在 D 級，目前修法會用一個使用，不是使用你上級機關的系統，因為有一些機關用的是雲端服務那段，是他自己採購，那個系統架在廠商那邊，像這樣情況，我們那時候評估在 D 級適不適合，還是要在 C 級，那一段我們會再做一些細部的調整，可是如果各位現在使用的是中央或上級機關給的系統，你就是 1 個使用者，這種不會被納 C 級，這是明確的。因為 C 級的定義，我們這邊也在做一些研議，我們的精神定義會朝這個方向，你不用擔心只是使用上級機關的系統就會變成 C 級，這個不會。這個系統如果架在你的機關，必須要有相關的防護，如果你是 D 級機關，你的防護可能沒有辦法達到那個水準，所以只要有主機、系統架在你的機關上面，你是 C 的機會非常高；如果不是，原則上我們不會框在 C，我們現在討論，你那個系統是在哪邊？

經濟部加工出口區管理處中港分處：

1 個在業者那邊，1 個在上級機關。

主席林春吟高級分析師：

因為你的上級機關原則上也都是納管機關，他的資安等級也落在上級機關那邊，這邊請大家先抓到這個精神。C 跟 D 的定義這邊一定會修，只不過目前還沒有找到比較好的措辭，所以我們先用這樣，大家激盪一下，有一些建議先提供給我們。

財團法人聯合信用卡中心：

我們屬於特定非公務機關，有關附表 2 修正對照表那邊有提到，關鍵基礎設施提供者要建置資安弱點通報機制，這邊是限定在關鍵基礎提供者嗎？如果我們是特定非公務機關不是關鍵提供者，是不是就不用建置這個

機制？

柯旻圻助理設計師：

對，應辦事項這邊，附表 2 是 A 級的特定非公務機關，資安弱點通報機制是針對關鍵基礎設施提供(CIP)者，這是只針對 CIP 的部分，公營事業、財團法人 CIP，有些被指定 CIP 納管，資安法會以規範強度比較高，同時 CIP 或財團法人，如果是以關鍵基礎設施提供者的納管特定非公務機關，就會需要導入資安弱點通報機制。

財團法人聯合信用卡中心：

不是的，就不用？

主席林春吟高級分析師：

不是，為什麼我們會把弱點通報納入應辦事項，若弱點已經被揭露，比較正規的做法是，有人發現弱點會跟產品原廠反應，產品原廠出修補程式，修補程式出來之後，就會公布弱點，修補程式也出來了，如果你不修補，另外一邊，他想要攻擊的，網路上工具很多，只要你的 IP 是曝露在外面，哪邊有弱點他是容易知道的，所以這件事情其實是重要的，只是考量每一個機關大家運作能量不太一樣，所以我們這邊會針對 A、B、C，還有特定非公務機關的 CI 提供者，納進應辦事項，如果你們機關不是 CI 提供者，可是你們有能量，還是建議把這個機制建立起來，因為這個風險是很高的，應該是這樣講比較好，不是就不用做，我們把風險高的納進去，講求防護，A、B 級原則上一定是持有一些重要、機敏業務或資料，所以相對的資安防護要求就會比較多一點。

財團法人聯合信用卡中心：

這部分寫到經主管機關發布後 1 年內要完成這個導入，這個經主管機關發布後 1 年，這個發布後是指這個法律發布後嗎？如果以相對的部分來看，有一個認知與教育訓練，有關資通安全專業證照的部分，有更改持有的數量，這個地方也是一種變更，可是沒有相對的這種規定，像我們已經核定超過 1 年，會不會造成我們可能沒有辦法立刻滿足這個條件。

主席林春吟高級分析師：

原則上，我們這邊只是調它的寫法，因為之前就是 A、B、C 有 4、2、1 張，我們本來寫法是機關總計，是 1 個人去考 4 張就好了？還是 4 個人各考 1 張，之前我們在 FAQ 就有揭露，原則上 1 個人至少 1 張，不是找

一個比較會考的人，他就專門負責這項工作，我們怕這樣，現在只是把用詞更精準列出來，並沒有改變它的規則。

土地銀行：

一樣是證照的問題，依照金管會內控稽核實施辦法第 38-1 條，會設置 1 個資安專責單位，其所屬的人員都算是資安專責人員，像我們部門來說有 10 多個人，依照修正後的應辦事項，這 10 多個人每個都要有 1 張證照，還是像我們是 B 級機關，只要有 2 個人有各 1 張就符合應辦事項？

柯旻圻助理設計師：

如果是 B 級特定非公務機關，要求要有 2 位專責人員，這 2 位專責人員每人應持有各 1 張，不用 10 幾個人都要各 1 張，那 2 位要求要有，這個是低標，就是 2 位以上也沒關係，專業證照也是，那 2 位就是各 1 張。

主席林春吟高級分析師：

原則上你們被規範的應辦事項是 2 位專責人員，至少這 2 位各有 1 張就符合目前資安法要求，不會因為你們配了 10 位，所以 10 位每個人都要 1 張才符合，沒有那麼嚴格，這樣大家會不敢配置這麼多人。在資安法上，因為適用在所有機關，我們現在只是用分級方式，原則上它是低標，看你們機關要保護的資產，可以去做優於資安法的規定。

土地銀行：

如果我在填報資料，在填我有多少資安專責人員的時候，譬如我有 19 位，還是要填 2 位？

主席林春吟高級分析師：

可以填 10 多位，都列出來，每 1 位是否有證照也是會列，我拿我們去稽核的情況，我們會去看，你有沒有符合資安法，如果規範 2 位，你們有 10 位，這邊是符合，優於規範，再來規範證章，因為你們有 2 位所以至少有 2 張，也有的話，原則上在稽核標準就是符合，只要有超出，稽核的時候就會寫優點，這個是一般的處理方式。

經濟部資訊中心：

有 3 個問題請教：第 1 個問題，第 6 條的部分，在業者提供的雲端服務，我們看到比較多是比較小的財團法人，可能只有用 Gmail 或雲端儲存空間，或是我們現在 mail2000，這部分未來還會再評估 C 或者 D 嗎？

第 2 個問題，公務機關都要導入 EDR，怎麼樣子符合導入的定義，是

全部導入還是重點導入就好。

第 3 個問題，關鍵基礎設施提供者要導 VANS 的話，關鍵基礎設施提供者是法人，有部分的關鍵基礎設施提供者是有框定範圍的，也就是它框定的範圍不是全公司，在導入 VANS 是不是就框定的範圍去導入就符合法規的要求，以上 3 個問題請教。

主席林春吟高級分析師：

雲端的部分我們也還在評估，如果有建議的話，也提供給我們，我們再參考進去。有關 EDR 的部分會涉及機關資源的籌措，還有每個機關要保護的資產重點，如果要全機關做的話，是不是有辦法爭取到相關的資源，或者可能爭取到一部分的資源，就要去評估從哪個重點開始做，目前我們這邊是有一些彈性，有點比照資安健診那部分的規定。

至於 CI 提供者框定的範圍不是全公司，這一塊可能要跟關鍵基礎設施提供者指定程序的單位再確認一下，因為就目前來說，資安法納管是全機關納管，我們沒有分機關裡面哪一個單位才納管，我們在公務機關或特定非公務機關全納管，CI 提供者被指定以後，您說有框列範圍的部分，細部的部分還要做釐清跟確認。原則上弱點修補、確認這件事情，如果各個機關不是列在應辦事項，可能還是要找時間處理它，在 10 月初針對微軟的漏洞有發文下去調查大家的處理情況，就表示那一個漏洞其實是很嚴重的，在國際上很多事件已經在發生，要避免我們這邊也發生類似的情況，所以像重大就會發文去追，相信有些機關不管收到簡訊還是公文，如果你們自己的資產沒有一個好的盤點方式的話，你們的作法就是會撒出去讓所有同仁再盤一遍，變成整個盤點作業，還有掌握作業要很花力氣；如果沒有被納為應辦事項，建議你們找機會趕快把這一塊處理起來，如果是應辦事項的話，還是要麻煩就個人電腦端、主機端，儘量把資產盤進來，通常不會因為可能做了 5 臺、10 臺有很大的差別，當你要做的時候，你的機制是一致的，有時候不用這麼在意只要做這部分，那部分不要做，可能是這樣的議題。

宜蘭縣政府財政稅務局：

有關 VANS 的部分，現在修法要 1 年內，我們在 1、2 個月前去上課，知道有教複製貼上的方法，因為現在各機關的狀況應該都會有人力的問題，所以基本上用人工幾乎是不可能的事情，所以要有 1 個自動化的軟體

或系統的機制導入，這個就是資源籌措的部分。以我們來說，預算編列的期程已經過了，所以，以我們來說明年底以前都沒有辦法採購相關的系統或軟體來做 VANS，可不可以把期程延長為 2 年或 1 年半，因為現在還沒有公布，如果公布之後，又錯過明年編列預算的時間點，根本沒有辦法達到法遵的規定。

主席林春吟高級分析師：

原則上各機關資訊資產，拿個人電腦跟主機來看，數量多的話，建議要有比較好的系統工具，也有一些是下指令，可能做批次檔，也是一種系統化的方式，把資產資料收整回來的做法，這些做法一樣就是看機關裡面哪一個是比較符合你們現況可以去執行的，要邊做。

有關 VANS 的部分，這個已經推動好幾年了，去年我們有辦相關說明會，今年年度中間的時候，我們辦的說明會，也持續跟大家講這個會納入法遵事項，所以如果你們今年沒有編進去，我會建議現在修法的草案已經出來了，有一些機關應該就會拿這個去做經費的編列跟爭取，這是比較好的做法，我們建議的做法是這樣，而不是等真的法定以後再做處理，我們再次跟大家強調，因為這件事是可以降低大家風險的一個工作，所以我們才會提出來，所以經費籌措的部分就要麻煩一下，如果今年已經來不及編進去，至少明年編後年的時候一定要編進去，尤其 EDR 那個也是要編經費的。

財團法人長庚醫院：

關於弱點通報機制的部分，第 1 個因為修補有分幾個，系統端的，像剛剛提到微軟的弱點，再來軟體端的部分，就我所知，譬如像醫院端，我們有很多 OT 的儀器或作業是不能被修補的，因為可能牽扯到 FDA 的驗證，有些醫療儀器，甚至有些是國外不幫忙補，我們在實務上碰到一個困難點，其實我們碰到這個法規的時候，訂的非常嚴謹，實務上我們在執行面有一定的困難度，我不知道這一段政府單位有沒有辦法協助，或者是衛福部怎麼樣協助這部分。

主席林春吟高級分析師：

因為醫院那邊會有一些 OT，醫療儀器那一塊是比較特殊的，目前資安法裡面附表 10 主要是針對 IT，OT 我們有請中央目的事業主管機關嘗試去定 OT 的資安防護，因為他的確沒有辦法馬上修補，或類似密碼登出在

OT 環境可能有執行上困難，就那邊去做一些防範標準，衛福部有在處理這一段，不過之後可能要再找醫療體系的一些機構給他一些參考意見。有關弱點修補這一塊，我們目前的處理方式，只要弱點被揭露，至少大家知道這個弱點在機關裡面到底有多少數量、在那邊，不管是 OT，就算在 IT 系統，修補前還是會先測試，一上上去整個系統不能 run，連在 IT 也會發生，會取決於你測了以後，是修補程式就放上去，還是沒有辦法上去，可能要 AP 調整，修補時間就往後，這時候大家就要去看弱點特徵、機制是什麼，我們可能可以用其他的防護去擋掉，那是另外的防護措施，所以在弱點這邊的處理，我們的大概步驟是先掌握你的弱點，再來評估是做修補還是做其他的防護，如果沒辦法修補要做防護的話，就會有短、中、長期的做法，原則上，所有的作業都是降低這個弱點被不當利用所產生的資安事件，剛才 OT 那一段的作業也嘗試著用這樣的處理步驟去處理，至於 OT 防護的部分，可以在法上面另外再規範一套適用的作法，醫療領域可能有好幾個，醫療也還有其他法規適用的問題，那個要統整做考量，這個衛福部有處理。

國家表演藝術中心：

提出 3 項建議：第 1 個，在行政法人並沒有公務人員，所以在評量證書的取得是非常不方便，像今年國家表演藝術中心送了人去上課，準備要考證書的時候人又走了，我(機關)的證書就沒有辦法取得，是不是建議行政法人在評量證書的部分就不納入？

第 2 個，專業證照目前條列的項目數量有點太少，具備專業證照的人對行政法人整體薪資的支出是太高了，甚至已經超過管理階層的薪資，我舉例來說，我們主要資通系統是交換器為主，我們並不是使用思科交換器，也沒有把其他廠牌納入，其他廠牌也不見得會有資安的相關證照。專業證照列第 1 條要求 2 項實地稽核，對於 1 個單位有很難就 2 次外點實地稽核的機會，是不是已經有要求機關需要導入 ISMS 的控制點為要項就好了？

第 3 個，行政法人內部有些人員可能是長期在外面，不會接觸到內部的系統，強制導入GCB的困難度太高，多數系統都是租用系統，租用系統範圍不是我們能控制，要導入GCB的困難度也很高。

主席林春吟高級分析師：

有關人員流動這件事情，不只在行政法人會發生，公務機關也會發生，所以這一段儘量讓你們的處理資安的人可以有多一點，讓你的資訊人員也去受相關資安的訓練，用這種方式處理，可能會比不要求來得好，因為不管人怎麼流動，有資訊系統一定要處理資安，不會因為你人走就不用處理這一塊。另外，有關人才的養成訓練是需要時間，這是可以理解，所以我們專職人力的過渡時間有再做處理。

有關專業證照的部分，大家如果有建議要納進去的專業證照，可以依程序跟我們提出來，我們這邊也會做審查的動作，如果是偏資安不是產品介紹跟資安概念有關的，我們也會新增進去，有其他建議的證書或證照也可以照那個程序提報給我們。項目太少，我們建議 ISO 27001 LA，因為它等於算是基本概念，取得門檻沒那麼高，至少有那樣的證書在，有關稽核實務，我們沒有要求一定要參與外部稽核，如果機關自己內部單位做稽核，他是去稽核人家，不是被稽核，之前有機關問我們，被稽核算不算，我們拿到 LA 的證照，就是去稽核內部的單位，這個參與經驗是會被納進去的，你們可能就是規劃一下，因為我們強調你拿到證書之後，要去做實務作業，讓兩邊是可以搭配起來的。

至於人員長期在外，這個可能要看一下你們的執行細節，會後討論一下，如果你們的人員長期在外，他應該不是桌上型電腦，可能是筆電，總是會跟人事差勤、email 去做串連，為什麼我們做社交工程演練，其實就是從郵件進到機關裡面，如果他人員在外，可是他用的設備，原則上跟你們的內部系統有做一些連結的話，還是要做一些處理。GCB 在運用上，是有一些可以放寬、例外設定的部分，我們要跟大家強調，例外不要太寬鬆，不然會失去它的效果，的確要做一個折衷，實務上要可以運作，可是會有一些限制，那些限制是提高你的資安，太方便代表你的資安風險比較高，也不能不方便到你沒辦法做，要取得平衡。

租用系統部分，這個我有興趣，會後可以交流一下，你們會租用的系統，因為那個可能會涉及 C、D 及研判的規格參考。

臺灣銀行：

想就剛剛土地銀行提到的應辦事項專業證照的要求再提問，專業證照那段，銀行有時候金管會要求，要成立專責單位，我們專責單位裡面的人員也都是列資安專責人員，在提報維護計畫實施情形，也都列資安專責人

員，剛剛提到還是會只要求 2 張以上，因為每一個稽核單位對法條的認知會不一樣，建議這邊資安專責人員每人應持有 1 張以上的證照，這邊加上「至少 2 位」，加入張數的說明，才不會好像整個資安專責單位都需要。

主席林春吟高級分析師：

土銀的先進跟臺銀的問題一樣，這一題有另外一個民間企業也有提出來，如果我們現在的寫法，如果你配 10 個人，可能 10 個人都要有，可能會造成這樣的狀況，這個我們回去會做調整。

勞動部職業安全衛生署：

有關 VANS 的部分，之前我們有測試過，就我們的了解是把機關的資產送到技服，跟弱點去做比對，因為我們機關本身就有弱點整個管理，是不是規定一定全部都要導到 VANS 上，如果可以的話，是不是不一定走 VANS？

主席林春吟高級分析師：

我們還是要了解所謂你們已經有弱點管理的機制是怎麼跑，會後也給我們資訊，後續要做細部的了解，可是在目前我們沒有其他的調整之前，還是一律要接到 VANS，你們如果已經有資產，不管是系統盤點，或者在單機批次檔把資料收回來，要做的作業就是把資產的格式轉成 CPE 格式，也是一個國際標準格式，上傳到技服這邊，這個目前還是要這麼做。

勞動部職業安全衛生署：

之前跟技服那邊的主辦人員討論過，我們跟他講我們的做法後，他說我們的做法不會比那個差，我們就不要額外花那個時間，因為貼上去只是比對那個結果，等於只是為了比對那個結果，事實上自己機關裡面整個從蒐集、資產跟弱點都會自行比對，修了之後我們只要做分析，就會把那個弱點變不見，人家有比較好解決方法，就不一定要導到那裡去。

主席林春吟高級分析師：

技術面我們先評估確認以後再說，原則上我們不做重複的事情，有一些資訊是需要回報過來，我們才有辦法做比較整體的掌握，看到時候做細部了解，我們再去看後面怎麼處理比較好。

經濟部：

前面先進有提到，關鍵基礎設施在適用應辦事項這個問題，就資通安全責任等級分級辦法第 11 條的部分，只授權中央目的事業主管機關就附表

10 可以另定，附表 1 到附表 8 我們是無能為力的，附表 10 該條法只授權我們去另訂 1 個防護基準，讓特定非公務機關可以適用，但是目前有 1 種狀況，公務機關兼具關鍵基礎設施提供者的這個身分，我們如何讓它適用，這個部分後續請資安處指導我們，我們目前有討論，可是我們還沒有找到一個方法，能夠讓公務機關兼具關鍵基礎設施提供者去適用我們另訂的防護基準。

主席林春吟高級分析師：

這個資訊之前有 pass 過來，主要我們是 OT，其實公務機關裡面也有 OT，OT 原則上附表 10 的適用會比較困難一點，如果公務機關有 OT，是不是也適用特定非公務機關針對 OT 的管制作業，這個我們也會納進去做研議。

財團法人聯合信用卡中心：

因為我們同仁有反應資通安全訓練課程，它有 1 個規定的時數，但我們可以報名的機構很少，有關於行政院資通安全處認證的資安教育機構舉辦的職能訓練，還有技服中心舉辦的教育訓練課程，是不是可以開放給我們特定非公務機關報名？

主席林春吟高級分析師：

都可以報名。

財團法人聯合信用卡中心：

好像要具備公務員資格才可以報名。

主席林春吟高級分析師：

你們報名的時候，看能不能加註一下，我們怕有一些不是納管機關，其實納管機關我們都會接受，在過渡時間有一些機關是以委外人力當專責人員，只要加註哪個機關的專責人力的話，報名還是會讓他報進來，在那邊你們加註一下。

柯旻圻助理設計師：

分級辦法還有問題嗎？（無）進到下一個子法，通報案件辦法，主要改 2 個，1 個是調查處理改善報告，上級機關可以請所屬機關提出一些修正跟說明之外，還有事中的處理、損害控制跟復原作業。

另外 1 個，多發型的通知發生，類似同樣的體系、同樣的攻擊形態，可以把這幾個事件當成 1 個資安事件通報，主要是這 2 個比較大，通報應

變辦法修法有什麼問題嗎？

經濟部：

有關修法第 6 條，後面提到上級監督機關或主管機關就第 1 項之損害控制或復原作業，可以請他們提出說明或調整，目前實務上的做法，不管是初報、續報或結報，都是在通報應變網站上去完成的，我們在實務的操作上，因為通報應變網站的設計，除了3、4級以外，並沒有審核或退回的機制，我們實務上要如何處理，我們認為不適當的話，可以提出讓他們調整的這個部分，實務上我們怎麼操作，這邊有沒有一些建議的想法？

在第11條後面，增加最後1項的部分也是同樣的問題，大家發現有同一類型資安事件的時候，得另行通報資安事件及統籌事件相關根因調查及處理，這個部分在實務上，如何就另行通報資安事件，應該如何操作，不知道資安處有什麼可以指導我們？

主席林春吟高級分析師：

我們現在從損害控制，上級機關還有主管機關就可以做一些關切的動作，主要因為在實務上針對比較重大的資安事件，其實在損害控制那一段，上級機關跟主管機關通常就會進去，等於在那個時間點做處理，目前在這一端實務上的處理，在系統面配合調整的地方，我們會再做內部研議，假設某個機關發生比較重大的資安事件，他自己做損害控制、復原，上級機關就會關心他目前情況是什麼、處理的進程是什麼、損害控制是什麼，實務面是這樣做，在目前法規上沒這段，比較像是損害控制報給你，後面 1 個月後給你結報就好，中間其實就沒有一些可以處理的規定，我們現在其實是把相關的實務面會做的作業放進去，因為有一些機關資安事件有可能就是因為設備故障，剛好故障在重要的系統上，所以資安責任等級其實會拉高，如果不涉及比較外在的，這個時候他的上級機關跟主管機關也不會去問你怎麼處理或做什麼，原則上就會照目前的程序 4 個階段，由機關自己去處理。可是針對比較複雜又比較嚴重的，在這邊賦予一個他在處理的過程中，上級機關跟主管機關一塊去協助他，處理及關切的一個機制，至於系統上是不是需要有一些機制，回去我們會再討論一下，我們也不希望大家一直在系統上做填報，因為當發生比較重大的事件，大家處理的能量會在實務上的處理。

至於統籌資安事件，之前聽到他們會在系統裡面有一個設計，讓上級

管發現所屬機關可能有好幾個，可能有 3、4 件類似，做通報的時候把這 3、4 件關聯起來，做相關的處理是讓它有連結，目前我聽到的規劃是這樣，後面就是看他們什麼時候把這個事情再做一個發布。

國立臺灣博物館：

在知悉資安事件後，我們在 1 小時內通報，我們可以寫事件發生的狀態，可是損害通知的狀態，經常不是我們有能力去處理，是上級機關做一些檢測，為什麼會發生這樣的情形，到底通報是由使用單位去通報，還是系統開發的上級單位做通報，怎麼樣做 1 個好的結案，在這邊有一點困難，因為我沒有能力去做通知。

主席林春吟高級分析師：

那個系統是架在你們上級機關那邊還是你們那端？

國立臺灣博物館：

用共構的。

主席林春吟高級分析師：

都在那邊？所以系統那邊可以進主機維護都是你上級機關。

國立臺灣博物館：

我們沒有權限。

主席林春吟高級分析師：

理論上應該是上級機關通報。

國立臺灣博物館：

那意思是當我發現的時候，因為我們會告訴上級單位。

主席林春吟高級分析師：

你要確認那個系統狀況，是效能問題或什麼，那個是他才能處理，所以你們的責任應該是通報給他們，由他們去研判，是不是會達到資安事件的標準，如果是，是他那邊去通報。

國立臺灣博物館：

因為在法規裡面沒有明確，我也曾經問過這個問題，大家都不清楚。

主席林春吟高級分析師：

我們看 FAQ 有沒有需要再寫一下，因為大家對文字的解讀可能會有一些落差，主要是可以研判這到底是什麼狀況，原則上會在系統提供的單位，就像機關裡面提供你們公文系統、差勤系統，大家都是使用者不會是

由使用者去通報，你們可能發現系統有問題，反應給提供系統的單位，他進去看之後判斷狀況，會由那邊統一做處理，因為一般實務運作會是這樣，像你剛剛講的也是這樣，只是是跨機關，可是他的處理原則還是這樣子。

國立臺灣博物館：

因為我們資安長很在意有沒有按照 1 小時內通報，時間很短沒有辦法太多投入在這個上面，希望很明確。

主席林春吟高級分析師：

資安長層級比較高，可以跨單位協調，但很多資安長不是資通訊領域，可能不是太清楚，中間可能要多溝通一下，我們再看 FAQ 那邊有沒有什麼地方把這個也放進去，讓你們比較好跟他說明。

柯旻圻助理設計師：

通報應變這邊還有問題嗎？（無）特定非公務機關的資安維護計畫實施情形稽核辦法，這裡修 OT 稽核那一塊，以前比較多是 IT，現在多了共通系統稽核，所以需要一些 OT 領域的專家擔任稽核小組的成員，有關特定非公務機關稽核修改的部分有問題嗎？（無）接下來情資分享，這邊改 1 個，鼓勵特定非公務機關去做情資的分享，目的事業主管機關可以依子法適時予以獎勵，這邊有問題嗎？（無）最後是獎懲辦法，這裡修改的部分，如果有嚴重缺失的話要做懲處，檢視的範圍有關主管及上級機關，有關這 1 條的修正有問題嗎？（無）子法都跑完了。

主席林春吟高級分析師：

如果大家針對母法與 6 個子法相關的研擬還有其他建議，也可以用書面方式提供給我們，在這邊跟大家宣導一下大陸軟體的採購跟使用，在我們今年的資安長會議有 1 個決議，就是不要使用跟購買大陸品牌的軟硬體，你們的委託廠商，記得跟他們確認他們的軟硬體裡面有沒有大陸的元件，或者他們的服務人員或客服人員有沒有大陸的議題，每個人自己都有手機，那個是有點資安習慣的問題，儘量還是買比較沒有資安疑慮的手機，APP 儘量不要裝對岸，因為對岸的 APP 議題會比較多一點，建議大家平常在自己的作息上，掌握這樣的原則，如果大家沒有其他問題，我們今天說明會就到這邊，謝謝。