資通安全管理法修法說明會（北區第 1 場次）

逐字會議紀錄

時間：109 年 11 月 24 日(星期二) 下午 2 時 30 分

地點：科技服務大樓創新廳(臺北市松山區民生東路四段 133 號)

【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：

我們有 1 張意見調查表，大家寫完以後可以交給我們的委辦團隊，之後就大家提的意見做研議。首先針對剛才的簡報，有沒有需要我們再做進一步說明的地方？沒有的話，我們要進到母法了，首先母法的部分，這次修法到目前為止，我們研議要修的有 70 條，其中涉及母法計有 9 條，有關配合財團法人法的部分，因為資安法剛發布的時候，財團法人法還沒有通過，所以資安法跟財團法人法上面的一些定義會不太一致。這次有一些修法意見是希望資安法可以跟財團法人法一致，所以我們目前擬出來的是 50%以上的全國性財團法人，還有中央目的事業主管機關指定加強監督的財團法人；然後另外 1 個修法重點就是，在母法也把上級政府的概念明確放進去，那針對母法的部分，大家有沒有要再給我們建議的地方？

行政院農業委員會農糧署：

農糧署，敝姓張，母法有幾個名詞定義，有主管機關、上級機關還有監督機關，在母法的修正條文裡面有提到上級或者監督機關之類的。我建議本法第 3 條的用詞裡，是不是可以去定義上級機關或者是監督機關指的是哪一些？能有比較明確的定義，因為以我們所管的特定非公務機關，也就是農產品批發市場，跟我們農糧署的業務往來密切，所以我們就比較雞婆一點，找了一些批發市場，跟他們講資通安全法要做的事情。所以一開始大家都認為我們是他們的上級機關，提報給我們，後來我們花了很多心思跟他講，你們的上級機關是縣市政府，不要一下子就馬上來找我們，所以在這一次修法的時候，我們建議定義是不是可以比較明確？以上建議。

主席林春吟高級分析師：

我確認一下，剛才講的農產品批發市場是屬於特定非公務機關嗎？

行政院農業委員會農糧署：

對。

主席林春吟高級分析師：

特定非公務機關依資安法的精神，往上是對到中央目的事業主管機關。

行政院農業委員會農糧署：

沒有，因為還有1個農產品交易管理法。

主席林春吟高級分析師：

農產品交易管理法？

行政院農業委員會農糧署：

在農產品管理法裡面有關業務推動的部分，他們的上級主管機關又是縣市政府。

主席林春吟高級分析師：

喔！那是業務推動。

行政院農業委員會農糧署：

對。

主席林春吟高級分析師：

對，不過在資安法上面的一些等級提報、資安事件通報，在資安法上面的一些作業流程，特定非公務機關往上是對到中央目的事業主管機關，所以不是縣市政府。那您講的法條我們會研究一下。大家就母法的部分，還有沒有問題？

那接下來我們再往下進行，有關施行細則的部分，目前擬修的條文有5條，主要就是把上級政府的概念納進來，另外1個是統一實施情形之提報方式，因為各機關其實都有提報實施情形的作業要求，如果說所屬機關很多的話，沒有1個比較好的系統讓大家填報，後面的處理是很麻煩的，我們已經統一做了1套系統，為了避免大家再另外去做，所以我們在法條統一明定提報方式。我們也會針對今年大家提報的情況，就可以再改善或者調修的功能及問項作簡化。如果各機關有其他系統功能上的建議，也歡迎提供給我們。另外提醒大家，上級機關如果要去稽核所屬的話，記得要進這個系統裡面去看一下所屬機關填報的實施情形，作為稽核的參考資料。那有關施行細則的

部分，大家有沒有要建議的地方？

法務部：

主席，各位先進大家好，我是法務部資訊處。我想請教幾個問題，第 1 個問題就是我們如果在做稽核的時候，因為法務部的員工一向比較知法守法，然後非常尊重法律上的問題。所以他有跟我們討論過說，憑什麼來做稽核？因為我們會看個人電腦、個人保管的 PC，甚至是發下去的 Notebook，或者是平板電腦等各式各樣的東西，都可能會涉及到個人隱私。如果他正面的拒絕接受稽核，像查看電腦等事情的時候，有沒有比較好的說法？

第 2 個問題我想要請教一下，我們有看到 A、B、C 級機關要配置指定數量的資安人力，然後又說可以延到 111 年的 12 月 31 日。雖然是這樣子，但我們的人還是不夠。而且我們的感覺也是逐步的在退讓，到最後我們的人什麼時候才會有？或者是怎麼樣才能夠補實資安人力？因為去修正我們的組織表，也不是說一下就可以做到的事情，不是說等到 111 年 12 月 31 日的時候再來改好了，這個問題我們想要先知道。

那還有 1 項就是有關 VANS 和 EDR，會不會給我們一些預算？因為錢就是一樣的問題，你說法務部可不可以省出這些錢？絕對可以，但就是拆東牆，挖西牆，然後拆到最後，部會的同仁會有一點反彈。我要完成上級交代的任務，可是上級又不給我錢，又不給我人，然後就一直叫我在那邊挖來挖去。請問有沒有比較好一點的方法？謝謝。

主席林春吟高級分析師：

原則上，公務的電腦跟設備應該屬公務使用，如果你們機關有一些同仁將個人隱私存在公務電腦裡，可能要先討論在作業上適不適當？因為我們相關作業是在維護整個公務作業環境的資訊安全。然後再來就是有關人力的部分，因為機關員額權責還是在機關首長，我們也有持續跟人事總處協調，近期主要會在數位發展機關的籌設上，統籌考量這件事情，所以有關資安專職人力的部分，會建議等院裡把數位發展機關的整體方案提出來以後，可能會有一些相對應的處理辦法。再來就是有關經費的部分，大家的經費編列其實都有一定的限制在那邊。

至於 VANS 的部分，主要已經推很多年了，我們是請技服把 VANS 的機制建起來。各機關要做的就是把機關裡面的資產資訊轉成標準格式，並拋轉上來，比對完以後，讓機關方便掌握機關內的一些資訊資產弱點情況。就我

們資安處的執行情形，只會針對重大的弱點去追蹤改善情形，像 10 月初的時候，我們有發文調查，那時候有 1 個微軟的漏洞，它的影響其實就比較嚴重，就我知道有一些機關是通知給所有同仁，然後確認大家手上有沒有使用那樣軟體，然後再回報，至於後面的整個修正及相關作業，其實會很花力氣，時間又拉很長，所以在一些資安作業機制的引入，應該是要逐步去處理的，在資安法這邊把它明確定義出來，主要就是因為近期的資安威脅越來越嚴重，大家可能想籌措一些資源，然後來處理這一塊，至於端點防護那一塊，也是因應這樣的資安威脅，所以我們現在是把時間拉成 2 年，讓大家方便去編列一些預算，然後爭取相關的經費來做對應的處理，逐步去做這一些事情。有關端點防護，其實我們最近有找一些資料，有一些機關是採聯合採購，把價錢壓到一個相對低的情況，其實是有一些採購策略可以運用的。

行政院農業委員會農糧署：

各位先進大家好，我想請教一下有關管考系統的部分，特定非公務機關需不需要上管考系統進行填報作業？謝謝。

主席林春吟高級分析師：

原則上我們現在管考系統裡面，主要要求的是公務機關，至於特定非公務機關的執行，會以他的中央目的事業主管機關為主，如果說中央目的事業主管機關也希望他的特定非公務機關來這邊填的話，我們不會反對這件事。因為特定非公務機關可能會涉及比較多其他因素，和一些民營公司有關，那部分的處理機制會比較謹慎一點，這邊主要還是看中央目的事業主管機關決定。

臺灣基隆地方檢察署：

我想要延續一下剛才法務部科長的那個議題，這邊難做稽核的原因，並不是因為他不是公務資料，是檢察官說他們的偵查是不公開的，同樣的問題也有聽到像軍方說只要是軍事機密，我們後面都做不下去了。所以我們後續執行這一方面的確是有一點困擾，謝謝。

主席林春吟高級分析師：

法務部的情況，可能我們之後再看看要怎麼去執行這些實務上遇到的問題，然後再看可以怎麼樣來做一些折衷處理，盡量也達成他們想要做得機密保護，然後我們也可以達到資安的管控作為。

交通部公路總局：

我是公路總局第 1 次發言，附表十有 1 個識別與鑑別，裡面有修正 1 個密碼使用，使用密碼進行驗證。所以有關鑑別與驗證的名詞，有些是鑑別，有些是用驗證，這其實還要再看一下，就是說原來驗證的意思，還是要留有驗證，還是到最後把它統一修，就是再確認鑑別跟驗證這 2 個名詞，謝謝。

主席林春吟高級分析師：

好。謝謝你，那個我們之後再確認一下。還有沒有問題？

那我們就再往下了，接下來就是分級辦法的部分，分級辦法主要在附表一到十，然後在條文調整細節的定義，因為執行過程中，有一些機關會反應他們使用的比較偏套裝軟體，像 AD 跟 mail，因為近期 AD 跟 mail 的資安事件其實還蠻多的，要請大家多注意。AD 跟 mail 那類不是自行開發，或者委外開發的套裝軟體，我們希望把它明確納到 C 級這邊來，有做相關的文字修正，不過因為目前這樣的文字修正，還是有一些不太理想的地方，如果大家有建議的修正文字，也歡迎提供給我們。然後另 1 個比較大的變動是 VANS 跟端點防護的部分，目前我們還是把它納進整個 ABC 級的應辦事項，端點防護主要是 AB 級。那針對這邊大家還有沒有意見？

中華電信股份有限公司：

有關這次分級辦法訂修，我們有 3 項建議，昨天有先透過 E-mail 的方式給鄭小姐，那在這邊說明一下，第 1 個是針對附表 2 的資安弱點通報機制，我們希望能夠加上一句，就是除了 VANS 以外，或者其他具有同等或者以上效用的措施。因為我們公司之前就已經有建立自動化的通報機制，假設是跟我們公司資產有關的漏洞，我們就會自己做 SOC 通報跟追蹤。所以這個部分我們已經跑了很長一段時間。那因為我們之前有派人去參加 VANS 的訓練，因為 VANS 現在是主要是適用在 Windows 平台，而且很多人工作業，對我們人工作業的部分介入很多，或者還要另外採購類似的工具，這部分可能沒有辦法符合公司的需求，所以我們希望能夠比照資安健診的方式，加上這樣一句話，就是說我們有具備同等或者是以上效果的措施。

那第 2 個是針對附表二的資通安全專業證照，我們是建議在條文裡面初次受核定等級 1 年內，是不是加上應按本表所定義配置的資通安全專責人員員額數，然後每人應持有 1 張證照並維持有效性。那這個部分只是對齊前面的法條，建議把它對齊。

那第 3 項是針對附表 10 稽核紀錄這個部分，這一次沒有進行修法，那

我們建議針對稽核紀錄的這個部分，有一段話是說針對事件發生，到最後一句話有說單一的這個格式。因為事實上我們現在資訊設備種類非常多，其實紀錄的這些格式都是依這個產品會有一些不同，所以我們是建議把後面這樣子的字眼移除，以上說明，謝謝。

主席林春吟高級分析師：

好，有關 VANS 那一塊，我們昨天收到資訊，其實嘗試要跟貴公司聯絡，不過一直沒有聯絡上，那一邊我們可能要先確認一下你們的作業方式，然後我們再看說後面可以怎麼做處理？可是在還沒有明確之前，原則上我們還是依目前的規範。

然後有關你剛才講的附表 2 的部分，我知道你的意思，就是把應配置那個人數把他對齊。

中華電信股份有限公司：

對，只是建議對齊。

主席林春吟高級分析師：

這個我們回去還會再研議一下，然後再來就是附表十的部分，稽核有一個單一格式的部分，那一塊採用單一紀錄機制，就是那一段文字，對不對？

中華電信股份有限公司：

對，因為他要確保輸出格式的一致性。

主席林春吟高級分析師：

對。

中華電信股份有限公司：

所以我們在實務上覺得比較困難，因為每個設備的格式都不同，大家在對這個條文的解讀，會有一些疑惑。

主席林春吟高級分析師：

所以你們建議是？

中華電信股份有限公司：

其實是後面這句話，覺得...。

主席林春吟高級分析師：

就是「並採用，還有確保輸出的一致性...」，這 2 段都把它拿掉嗎？

中華電信股份有限公司：

對，是建議可以移除。

主席林春吟高級分析師：

好，那這個我們一樣帶回去研議，謝謝你的意見。好，然後還有沒有問題？

再來是通報應變的部分，那通報應變目前我們研修的條文有 5 條，主要是針對那種多發性，在我們實際運作情況下，有時候會發現可能某一個領域裡面，短時間內有幾個機關，有類似的一些資安事件發生。那針對短時間裡面，事件間可能會有關聯的，我們是賦予他的上級機關，或中央目的事業主管機關，可以另行通報資安事件的處理彈性。那主管機關如果有發現這樣的情況，也可以提醒上級機關或者是中央目的事業主管機關去做通報。另外就目前法規上，大家提結案報告給我們的時候再給改善建議，其實很多處理的時效都不見了，所以我們也把相關的規定放上去。那針對通報應變，大家有沒有一些建議或者疑問？如果沒有，那我們就繼續往下了。

接下來就是特定非公務機關的稽核辦法，目前我們要研修的條文有 4 條，主要是提供萬一真的發生一些不可抗力因素的時候，有一些稽核計畫調整的彈性，那有沒有問題？好。

接下來是情資分享辦法，目前就是主要研修是 2 條，主要就是讓中央目的事業主管機關，可以針對特定非公務機關有一些獎懲的處理彈性。如果他有提供一些有貢獻的情資的話，其實中央目的事業主管機關是可以去獎勵。也希望用這個方式來推動特定非公務機關做相關的情資分享作業，好，大家有沒有問題？沒有，好。

接下來就是獎懲辦法的部分，原則上我們不會以懲處的角度在看這件事，可是當有一些資安作業應辦未辦，已經情節重大，在這樣的情況下，不得不有一些檢討的時候，除了相關作業的人員之外，我們會希望主管或者上級機關在督導或者協助上，是不是有可以改善的地方？就把這個範圍納進來做一個檢討，那大家有沒有問題？

法務部：

不好意思，那我還是想請教一下，就是說因為我看到端點防護，端點防護是有規定做到百分之百嗎？或者是說有一個容忍值？因為我們還是有人不願意，以我們部來講，還是有人不願意刷指紋，還是有人不願意領國旅卡。那我們也同樣認定應該會有人拒絕安裝這個東西，而且拒絕安裝的人，也許不是我們輕易能夠勸說的，那我想問一下遇到這種狀況的話，那獎懲辦法是

一個強制的規定，但是我們有沒有辦法解決？我們還是有，反正就是靠談判、靠人情壓力，靠什麼東西去解決，但是我是想問說有沒有一個比較實際一點的法律上的規定，或者是可以讓我們有上下調整的空間，也許不要百分之百，讓我們可以做稍微迴旋，謝謝。

主席林春吟高級分析師：

好，首先回答端點防護的範圍，原則上我們會希望盡量朝最理想的狀態去做。因為每個機關其實可以獲得資源不一定，那就目前的規範，我們的寫法是有點比照資安健診那一塊，原則上就是看各機關。我們希望可以就盡量做，可是還是會受限於我們的資源，所以需要去評估，就是哪邊是你們比較重要，需要保護的資產？因為資安本來就是一個風險管理的概念，那當你資源是有限的時候，你一定從最重要開始做，然後看可以做到什麼程度，開始做處理。所以目前我們的規範文字，就是以這樣的寫法。然後至於說你剛才講的那個，我們會看看你們有沒有比較建議的一些文字規定？可以提供給我們，讓我們來評估看看說這樣放進去適不適合？

法務部：

那關於正常的處理模式，我們還是會處理掉這些事情，可是我們希望有一個正常的處理模式。

主席林春吟高級分析師：

目前正常的處理模式，我們都已經寫在上面，沒關係，我們可能可以討論一下，或者是說我們看是不是可以反應給你們機關的資安長？我們為什麼會請機關的副首長來當資安長？其實資安有很多作業都要跨單位協調，所以我們希望說有一個比較高階的主管，來協助做推動，您的問題可能要個案去處理。

那大家還有沒有針對我們這次修法的問題，也歡迎你們透過書面資料給我們。如果大家針對這一次的修法說明會沒有其他問題的話，我們今天說明會到這邊，謝謝。