資通安全管理法修法說明會（南區第 1 場次）

逐字會議紀錄

時間：109 年 11 月 11 日(星期三) 下午 2 時 30 分

地點：臺南文創園區 4 樓富貴文創講堂(臺南市東區北門路二段 16 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】

主席主席林春吟高級分析師：

謝謝大家來參加會議，就剛才同仁的簡報，有沒哪邊不是太清楚或需要再加強說明的地方？我們先就剛才的簡報做一些釐清，然後再就每個法去做確認。首先就簡報的部分。

法務部矯正署：

我是法務部矯正署第 1 次發言。剛剛我看簡報就是對那個資安人員，它是說專職括號什麼的，我印象中這個專職專責，你現在用這個括弧好像感覺不太一樣，你專職的話是說工作就是專門負責資安業務，如果是專責的話意思說，我可能有其它工作，本來是負責庶務業務，你要給我那個責任專門負責資安業務，所以這 2 個概念不大一樣，那修法之後專職專責，意思說機關的人以後負責資安業務的，可能可以兼其它的工作，我又來兼資安業務是不是這個意思，還是說還是應該是專職才對？

柯旻圻助理設計師：

好，謝謝機關的提問。那專職這一塊，如果看資安法大家有發現的話，公務機關附表 1、3、5，資安專責人員這一項，它辦理的內容有寫說，就是專責人員要以專職人員配置，就是說只要是公務機關，它的專責人員就一定要是專職人員；為什麼會有專責人員，主要是特定非公務機關，有一些公營事業、財團法人，不會要求一定要有一個專職的資安人員。專職專責的部分，修法這邊我們沒有動，因為公務機關它要專責人員就一定要是專職人員這樣，謝謝！

主席林春吟高級分析師：

我們這個簡報只是摘要說明，所以我們是考量篇幅，沒有說把它整個謄過來，因為我們專職、專責的定義，還是依現在目前法的定義，沒有調動這一塊。我們這邊主要釐清的，就是證照之前的寫法是總計應該持有，在執行上會有說是不是某一個人去把所有的證照考完就可以了，其實主要是每個資安專職人員都要有基本的概念，不然你在執行上會有一些落差在。所以我們現在只是把證照的持有是每個人都持有這件事，把它再更釐清而已，這議題主要是這樣。那對簡報還有沒有其它的問題？

高雄市政府資訊中心：

高分、設計師，各位先進大家好！高雄市政府資訊中心第 1 次詢問，問幾個問題，1 個是防護基準普級的話，現在就要監控遠端連線，那請問監控遠端連線是指用什麼方法監控？

那第 2 個問題就是說 B 級 1 年要導入、C 級 2 年要導入 VANS，那導入的範圍是資通系統？還是所有的電腦？

分級辦法定義 C 級機關有提到說 AD、資料庫這些之外，還有 1 個叫做帳務處理的系統，請各位舉例什麼是帳務處理的系統？

那最後 1 個是建議，就是管考系統改版的時候，可以幫我們做匯出的功能。譬如說我們要統計所屬機關的專職人力的時候，有一個匯出報表的方式，我們會比較好算這樣，謝謝！

柯旻圻助理設計師：

我先回答管考系統的問題。管考系統現在有匯出功能，可是它的功能只有單一的實施情形全部匯出，針對附表一、二、三統計功能，我們有請技服中心協助調修，所以統計功能可以給機關可以拿來匯出。

主席林春吟高級分析師：

遠端監控你指的就是遠端連線的監控嗎？其實在實務作業上有很多機制，就我知道的案例，有一些機關讓人家遠端連線，是透過 1 台固定的主機，要先到這個主機來，才能進到內部網路。那它到這個主機時，就開始啟動相關的連線側錄或相關的 log 去把它留下紀錄來。因為其實也是因應很多委外廠商，機關有時候難免因應緊急事件，讓委外廠商連線進來做維運，我們是不建議這麼

做，可是在實務上有一些機關的確還是開放了讓一些維護的人從外面連進來。本來是我們是訂在中高級，可是這樣的一個脆弱點越來越強，所以我們現在把這樣的規範拉到普級去做處理。

有關 VANS 的部分，我們目前扣的是 PC 跟 Sever，所以在 PC 跟 Sever 那一邊的資產盤點，盤點把它彙整起來，轉成 CPE 格式，跟 VANS 這邊做交換比對的動作。相關的一些作業，我們在技服網站有一個 VANS 專區，之前也有辦說明會，所以如果大家在執行上有問題的話，可以再跟我們做聯繫，確認後面那邊怎麼做。

帳務處理那個只是 1 個舉例，我們在去年資安法施行之後，有一些機關就打電話來說 C 級是自行開發或者是委外，可是我們用那一套系統是市面上的套裝，可能就是財管人員在用的那種系統，也曾經有遇過是社會體系的機關使用一些案例管理，比較套裝的系統，那套系統也賣給很多機關使用，那他會說這不是他們委託開發的，他只是買來用，可是那個系統也是需要去做維護的，它可能還是會有弱點，所以如果是像這樣的 1 個服務，我們會把它歸在 C 級，那就是為了讓定義更明確，所以我們現在把它納入法裡面。可是相關的文字如果大家有建議可以提供給我們，因為那個不好去擬定。有一些套裝軟體，像那種 office 編輯還是繪圖的那種，就不是要管的範圍。所以我們才去下一個定義可能是具有權限，有管理者跟一般使用者去區分，或者是你在裡面有管理功能，就像 AD 或者是 mail 這些，才是我們會把它希望納到 C 級去的。可是如果是那種繪圖軟體、office 文書編輯，其實只是用那個工具來產製自己的內容，那不是在要管理的範圍，用講的可能大家可以理解，我們要落到法裡面的文字，就很難這樣寫，所以我們盡量想辦法讓他明確，在這一邊也是要麻煩大家，如果真的有比較好的一個明確定義的話，務必要提供給我們，讓我們可以把它修得比較好一點。或者是我們在它的修正理由那邊，可以再加強什麼樣的一個說明，讓大家在適用上可以更明確。好，還有沒有？如果沒有，我們就先進到法這邊。

我們今天主要的那個修法範圍就是資安管理法，1 個母法跟 6 個子法。首先我們就資通管理法的部分來看，這邊我們會修 8 個條文，我們的修法細節都在說明會網站資料的 word 檔上面，那邊是比較細的，簡報只是抓重點，簡要跟大家說明而已。在資安管理法母法的部分，我們動得比較多，當然就是財團法

人的定義，如果各位跟財團法人比較沒關係，那這一點原則上跟你們的關聯性就沒那麼高。另外就是納入上級政府的概念，這邊比較會有關的就是縣市政府，因為縣市政府撇開直轄市好了，其它縣市政府裡面，它的轄管範圍裡面會有公所跟代表會。一般來講我們主要是以地方自治法的精神，就是縣市政府其實算是他們的上級政府，我們的相關作業就是讓他們先提報給上級政府去做處理。針對母法的部分大家有沒有什麼問題？如果沒有，我們進入第 2 個施行細則的部分。

施行細則的部分我們主要是修 5 條，比較主要的就是那個實施情形提報，我們就讓它明確，因為今年我們 2 月其實也是有發文跟大家講，上管考系統提報，大家可能剛開始不曉得要填什麼，所以我們嘗試用 1 個系統，讓大家用系統填，也給一些範例，也有看說大家填的方式可能有一些執行上的困難，我們現在也研議把它修得讓大家比較好填。它只是一個初步的資料，因為在法上面，上級機關要對所屬機關的實施情形進行稽核，像我們出去稽核的時候，都會請機關先做一些自評，實施情形提報內容也是一個參考資料，這一段主要是這樣。就是說由我們統一弄 1 個系統讓大家上來填，那上級機關也可以在上面看到所屬機關填寫的情況，一來是大家會比較標準化，二來也不用大家個別去做系統，我們用意主要是這個樣子。如果說針對提報的內容，或是功能上的建議，歡迎就像剛才高雄市一樣，就是提供給我們，讓我們這邊做一個綜合的考量，很快去做處理就好了。那針對施行細則大家有沒有問題？好，沒有。那我們就進到第 3 個，分級辦法的部分。

分級辦法它修最多的主要是在附表，這邊有 40 項，然後在條文的部分，就是我剛才講的 C 級的定義，針對分級辦法，可能對大家衝擊比較大的就是 VANS 跟端點防護的導入，這邊我們主要推動的對象就是 A、B、C 級機關，VANS 是 A、B、C 級，如果是端點的話是 A、B 級，有分不同的責任等級還有對應要去加強的防護作業。那這邊大家有沒有問題？好，那邊。

臺南市政府交通局：

各位大家早安，大家好！這邊是臺南市政府交通局第 1 次發言。我想要請教一下有關端點監控這個部分，我們想要納管的範圍很多種，是找 1 個核心系統導入就好了還是怎麼樣？我們要做到多少範圍？

主席林春吟高級分析師：

好。這項在台中場那邊也有提問，端點防護跟經費是有關係的，大家執行的方式，就是比照目前在(分級辦法)附表裡面資安健診規定，處理彈性是回歸到機關這邊來做處理，就有限資源跟最重要的部分去做處理，執行彈性目前是保留在機關這邊，我們沒有去把它訂死。有關端點防護的部分跟 VANS 的部分，原則上我們目前評估範圍都是在 PC 跟主機，然後就是看你們可以取得的資源，去做一些對應的執行，大概執行的方式會是這樣子。

高雄市政府資訊中心：

建議剛剛那個 C 級機關分級那邊，因為不管多小的機關，多多少少會有財產、薪資系統、E-mail 系統這種類似套裝系統，如果這樣訂下去之後，C 級機關一下子會變很多，這個要考慮一下，那 C 級機關說要做 VANS、端點偵測，看起來越來越嚴格，每 1 個工作項目越來越多越來越嚴格，那實際上可行性如何，請再評估。

那另外有 1 個建議是，因為技服中心在辦理資安職能訓練，其實已經發展了許多好課程，相較於其它的專業國際證照，其實資安職能訓練的課程內容比較貼近機關實務的需求，建議不要再要求國際的專業證照，這個機關的經費負擔比較大，錢比較貴，而且人員流動就沒有了。所以我們建議 1 個人要 2 張資安證照，或者說讓機關可以選，要職能或者是國際專業證照。以上，謝謝！

主席林春吟高級分析師：

好。原則上 A、B、C 級的應辦事項很多，所以我們不希望 A、B、C 級的機關太多，在我們執行的過程中也有四十幾個機關，把它的網站或者是一些系統往上去集中，它自己就從 C 級降為 D 級，這是我們的目標。因為一個網站或者是一個系統就變成 C 級，那是不符合成本效益的，像這種情況就變成說它的上級機關要協助，因為在所謂上級機關這一層，它可能已經是個 B 級，我們希望資源是往上集中的。我們一直以來，不管是資安處還是國發會，我們推動的就是向上集中，可是我們也在宣導不要事情向上集中，錢沒有向上集中，所以我們講的是資訊或是資安資源向上集中，大家去集中防護、集中去培養相關的能量或者是相關的設備採購防護。那剛才你提到說他們有一些什麼財產系統、薪資系統 E-mail 這個，原則上我們就是不樂見各個機關都去建一套。有一些機

關，其實就像公文系統好了，應該是有縣政府集中做一套給他所屬去用，但如果不是這樣的話，就變成每 1 個機關都建 1 套公文系統，那不是個辦法，一個是在建置維護成本上是很高的，然後第二個就是資安的防護破口。所以像剛剛那個情況，財產、薪資我們還是建議向上集中，由它的上級機關提供一套，讓它的所屬機關能夠使用就好，大家的防護就會扣合在上級機關這邊，因為資安要做的事情非常多，可是就算做了這麼多事情，還是沒有人可以保證說不發生資安事件，這個觀念要有，我們也會在高階主管會出現的場合，去跟他們宣導這個觀念。我們相信有一些主管其實對資安不是那麼清楚，資安回到一般的情況就跟身體健康是一樣的，你早睡早起吃得健康，有誰可以保證你不生病嗎？不會有人跟你保證這一件事。其實資安就有點類似這樣的事情，這件事我們會去宣導。那可是回到執行面這邊，就是要麻煩上級機關，儘可能協助所屬機關，共用的部分盡量就向上集中。反正你有建置一套了，你就讓你的所屬機關來用。所以我們期待的是不要太多 C 級，真的。A、B、C 不要太多，大部分是到 D 跟 E 去，那 D 跟 E 就是做好他各自的防護，主要就是使用者觀念意識那一段。

有關職能訓練的部分，目前我們還是希望至少 1 張職能跟 1 張專業，我們現在看大家去取證照情況，專業的那一張，大部分都會去拿 ISO 27001LA，那一個課其實是有它的必要性在，我自己去上過，我自己覺得整個資安的觀念跟體系會在，所以我們會覺得至少你讓你的同仁去接受那樣的訓練，取得證照只要同仁不要太不用心，應該都可以取得，這個(不易取得)議題應該是不存在。然後職能訓練的部分也一樣，剛才有講其實比較扣合我們實務作業面上的，在台中場反應的就是說有一些職能訓練太難了，其實它有一個學習地圖，因為職能訓練會扣合一些實務操作面，如果說有一些機關因為資安法上路之後，一直以來也沒有資安人員，可能大部分都是現有人員去做資安，那人不會一夕之間那些職能都會有，所以當你要去處理職能訓練這一塊，可能就是 follow 職能學習地圖，從比較基礎開始，去取得一個相關的職能證書，人才是要時間培養的，所以這一部分我們應該還是會維持在職能證書跟專業證照都要有這樣的一個規定。好，大家還有沒有問題？

內政部消防署高雄港務消防隊：

主席，高雄港務消防隊做第 1 次發言，剛剛呼應一下那個高雄市政府資訊局的，C 級機關不要太多這個很好。以我來講的話也算是被歸屬 C 級。但是坦白講，我算是一個勤務的消防隊被歸類 C 級，這好像有一點太重了。那我要講的另外一點，就是剛才主席有講到說會在高層場合跟他們溝通，其實還有一點我會建議，尤其是主計單位，就是我們的上級它同意要幫我們做，但是就是卡在主計人員他有不同的觀點，他認為說你那個預算是要由地方來支出，不是我上級要來幫你支出這一塊，那你主計卡關，那主管人員他再有心要幫我們做也沒辦法，譬如說公文管理系統，你非得一定要其它 4 個機關各自去建這一塊，當然他有心要做，但是卡在主計那邊，他不放款就沒辦法。

那另外一點就是，C 級機關的認定，建議在核定審查時能夠放寬一點，就像主席講的，當上級機關已經是 B 級，在審核上面就是盡量放寬，要不然在我們這種小單位沒錢沒人，卡到 1、2 個系統變成 C 級，哪有可能有那種專職人員，外面搶人人都沒了，不太可能為了某 1 個資管派 1 個專職人員去處理資安的問題。那個部分可能要上面多考量一點，謝謝！

主席林春吟高級分析師：

好，有關於剛才講主計那一塊，我們跟主計總處那邊了解看看是不是循他們主計體系進行溝通，因為主計是一條鞭從內溝通，每一個人對於法的執行定義可能不太一樣，可是向上集中是我們明確的政策。那至經費那邊怎麼處理，絕對不是說上級不能幫你處理系統的錢，所以你得自己建一套，如果這樣的話，其實很多機關都沒辦法運作。然後再來一個就是 C 級審核部分，原則上我們就是依法條在處理，反而是說你們還有多少的系統，怎麼向上集中，我們建議朝這個方向去做處理。

交通部民用航空局臺南航空站：

主席您好，我這邊是台南航空站，剛剛那個消防同仁他們單位提出的那個我就覺得很奇怪，因為我們也有公文系統，當初它也是要求我們各站自己做 1 套，就跟它講說怎麼會這樣子？我們才幾個人，要我們自己做 1 套系統？所以那它才自己做 1 套，做 1 套之後，現在就是會計的問題，它就是說把這 1 套系統的預算分配給各個航空站，航空站每年因為有建置費跟維護費，它就是編在

我們這邊，我們只是出錢而已，實際上我們根本沒有在做，這是 1 個解決問題的方法。

另外一點就是說那個資訊人員，他們應該有擔當，因為我們不是資訊人員，我相信在場很多也都不是資訊人員，都被抓來當資訊，我覺得這個是錯誤的，因為我們自己也有我們的本業，雖然資訊很重要，但是我們的本業也非常重要，我們本業像我是做工程的，我還要發包還要帶廠商去看現場，還有一大堆事情要做，像我今天來我還擔心有 2 個案場廠商要來找我，那這個都不重要嗎？就是說資訊人員一定要自己要擔起責任來，我們是沒有資訊人員的機關。你是上級機關你有資訊人員你有資訊室，你要擔起責任來。我們雖然不懂資訊，但是我們稍微知道資訊是可以向上集中的，而不是拿資訊來當成你去打壓下屬機關的工具，我覺得是不對的，行政院是不是應該要體察實情？下面很多做不對的事情，那上面通通都不知道，這個是不對的，我們希望這個國家好，真的，請他們要擔起責任來，我們也不是不願意做，這麼多機關對不對？我們下面的系統幾乎都一模一樣，我們為什麼要自己做一套，然後自生自滅，這不對的事情啊，我們也願意做，我們資訊室做一套資安的管理系統要我們配合，我們都沒問題，但是你要逼著我們去考試去弄這樣太過分。那我是機電的，那我強迫你去考機電執照，感想如何，對不對？

主席林春吟高級分析師：

像剛才那樣是比較好的，就是說帳務部分做法不太一樣，有一些機關錢就統一編，統一幫大家做，有一些的確就是我統一幫大家做，那大家來分攤那個錢，實務面上做法，就是看那個機關比較想要什麼樣的方式去處理。可是不會是說因為錢各自編所以就各自做，因為這樣永遠錢都編不夠的，需要上級機關來統籌協調一下，這邊我們也跟交通部了解一下。好，大家還有沒有什麼...那邊。

屏東縣政府：

屏東縣政府第 1 次發問，就是我們現在 C 級單位以前是自建或者是委外的資訊系統，現在多了 1 個權限及管理功能，剛才高分有講說那個就是針對套裝的 mail server 或是 AD 這些，我們之前在看會誤以為說公文系統或者是網站，我們現在的所屬是用縣府的公文系統跟網站，可是他們是具有權限劃分具有帳

號開設管理功能的，如果說我們現在界定這個責任等級的劃分只是 Mail 或者是 AD 的話，可能我們在法條那邊寫說使用權限區分及管理功能非自行或者委外的系統，可能就會有一些問題了。

還有另外一個就是 C 級單位，我們常常面對一些 C 級單位說它跟別的公所是 D 級的差別，只是因為它多了 1 個差勤系統，差勤系統也沒有對外，就是它自己內部在用，它就變成 C 了，然後要它導 ISMS，這個差勤系統基本就不是核心業務，就算差勤業務掛掉了，他頂多就是回去原本的方式用紙本，那這樣子它還要導 ISMS 嗎？

還有另外 1 個就是稽核所屬機關，是不是一定要到現場去做審定還是書面的稽核就可以。以上。

主席林春吟高級分析師：

你的第 1 個問題其實我沒有聽得很清楚，就是因為像你剛才講得，如果公文系統是縣府做一套提供給所屬用，那你的所屬就是 1 個使用者而已。

屏東縣政府：

他們也有自己的權限管理。

主席林春吟高級分析師：

那沒關係，因為那整個系統維運是縣府在做，那它就是只是我有這個權限，可以進這個系統處理，重點是系統是誰在維運，它不會是因為我有它高一點的使用權限，然後我們機關等級就拉高，不是這樣。因為它沒辦法去改那個系統。那個系統有弱點、有漏洞或者是功能要調修什麼的，那些作業應該都是縣府在主導。那個系統原則上就是在縣府這邊，你的使用者、你的所屬機關不會因為使用這一個系統，然後可能設一個機關管理者權限，就會影響使用機關的責任等級。除非它自己在內部，就像你剛才講另外 1 個，就是公所它建了 1 個差勤系統在他們機關裡面，我們看的是資通系統，不是看它有沒有對外或者是只是內部用，如果那個公所它自己建了一個差勤系統，那的確會因為這個差勤系統變成 C 級。

屏東縣政府：

對，它會變成 C，它也認為它是 C，可是它斟酌的是要不要導 ISMS，因為他認為說那個根本不是核心系統。

主席林春吟高級分析師：

那就回到剛才核心資通系統的衡量基準，它怎麼去研判它的核心資通系統，如果說差勤不是它的資核心業務，核心資通系統在資安法裡面有 2 個定義，一個就是支援你的核心業務，你的核心業務就是看一下各個機關成立的責任任務是什麼，主要是那一塊；另外一個就是資通系統的防護需求等級是高的話，這 2 個就會是它的核心系統，如果它的差勤系統不是這 2 個之一，那原則上它是可以不把它畫在核心資通系統上的，它不是核心資通系統的話，它在法上面就沒有說一定要導入 ISMS，當然它也可以導入，可是不會落到法的要求上。至於是不是核心資通系統，還是一樣回到機關自己去研判，一樣就是剛才那 2 個標準，1 個就是你的核心業務，假設好了，假設說我是消防的機關，那我可能為了要支援我這個消防業務做的資通系統，那就是我的核心資通系統。可是如果我現在這個資通系統不是在支援我核心業務，可能就是其它讓我比較方便去做的資通系統的話，那它就有可能不是你的核心資通系統，但是還要再看它的防護需求等級，除非你覺得這個很重要，因為它裡面有個資，所以我把防護需求等級拉高，拉成高的話，那它也是你的核心資通系統，就回到那邊去做處理。

稽核的部分，原則上我們目前還是走實地稽核要去現場看，比較不會是紙本。因為紙本作業，拿我自己的稽核經驗好了，你去稽核之前你會有一些檢核表請機關先自評，有一些是符合或者是說就是有做到，可是到現場要去調實際上的一些執行紀錄，它是一個比較互動式的，所以在稽核我們目前是沒有把它放寬說你只做書面稽核就好了，大家在做稽核的時候，我們也是強調說可以藉由稽核去培養我們機關的同仁的稽核能量。所以行政院在對所屬做稽核的時候，我們每場稽核，除了稽核委員之外，我們還會配 2 個觀察員，那 2 個觀察員就是從中央跟地方政府那邊招募過來的人員，會跟著我們稽核委員一塊做稽核的動作，再把這整個稽核作業帶回機關去規劃執行。上級機關要做稽核的時候就可以聯合你的所屬機關，你的 A 所屬去稽 B 所屬，B 所屬稽 C 所屬，就是大家互相稽核，你可以用這種方法去做處理，因為稽核在去年的實施情形裡面，是大家達成情況是比較沒那麼理想的部分，以往資安從 90 年開始推到現在，其實比較沒有強調說機關要做稽核這一件事情，所以這一段也是大家可以再一塊努力的。這邊。

法務部矯正署：

主持人，好，回到那個比較宏觀的觀點，我相信在座的很多機關應該都沒有資訊單位。現在是說我們系統向上集中，當然是一個很好的做法。但是我是想說未來是一個資訊的社會，資訊時代的社會，不只是那個系統，可能很多機關的設施，譬如說發電機或是監視系統都是連網在監控，所以資安這一塊我相信是很重要，不只說因為資安處站在本位立場說資安很重要，其實私底下我們各個機關也覺得很重要，但是那個資安，我是贊成說有一個資安專責人力，那這個資安專責人力就是希望上面撥人力下來，但是這個又回歸到人事總處那個法給你框住。但是我想說法是人訂的，這個法也是人家去立的，我是說透過這個去 push 立法委員做一個修法的動作，因為資安這一塊可以把它認為是一個新興的業務，因為未來講比較廣一點就可能是資訊戰，這是上面很重視資安的這一塊，我覺得可能這一塊應該要放寬，我覺得法是人立的，應該是可以去修法，謝謝！

主席林春吟高級分析師：

好，有關人力那一塊，我們是有在做一個整體的研議，目前就是如剛才簡報其實最後一頁提到，為什麼我們會把過渡期延長？就是相關的一些人力研議規劃會併數位發展機關去做統籌的處理跟思考。那一段比較明確的話，可能就要等那個行政院這邊把那個數位發展機關的規劃公布出來之後，再看那一塊的方案，類似外加人力這一件事情，從資安法在溝通的時候其實大家都有提到這個議題，這一段我們也有注意到。可能後面我們就是先看一下那個數位發展機關，因為近期也有一些新聞出來，就是等那邊比較明確的結果公布以後，應該是有一些對應的處理方式會出來，好不好？就是大家再稍候一下。好，那還有沒有？

臺南市政府交通局：

主席好，臺南市政府交通局第 2 次發言，我這邊有 1 個小建議，就是我們現在都要去綁定我們的資安時數，那我們的資安時數可不可以跟人事行政總處那個公務人員發展的那些綁在一起，少去我們每次都再去統計，做這樣的建議，覺得這是有可能。同事也不會誤會說他上了公務人員的課之後又上資安的課，謝謝！

主席林春吟高級分析師：

這個由我們跟人總那邊去協調，原則上會在那個時數那邊畫 2 個代碼，就是資安的通識訓練跟資安的專業訓練，到時候大家把時數登上去的時候，記得代碼把它選對，那至少從人事那一邊出來的學習時數就會很快統計出來。

臺南市政府交通局：

其實他們都會去統計我們整個機關人員的學習時數，我們有一些公務人員必修的一些課程，那現在既然資安法有這樣的規定，那資安其實也是必修的課程，想說是不是可以合在一起。

主席林春吟高級分析師：

好。那一段因為我們現在至少是先讓大家的學習時數在人事的時數系統裡面是分得開來，所以要讓它統計出來其實是簡單的。至於說是不是把它納在人事單位一定會幫忙統計的那一塊，那我們再跟人總確認一下，它們對那一塊有沒有什麼規定，因為目前它大概就是有處理 10 個小時的幾個類別那一塊，因為他們不希望管控的類別越來越多，至少大家可以從人事那邊直接統計出來，大家不用個別統計，這樣會輕鬆一點。好，還有沒有問題？這邊。

高雄市政府資訊中心：

高雄市政府資訊中心第 3 次發言，我是想要針對 C 級機關定義那邊再提一下，因為以目前的情況 C 級機關因為 1 個系統，然後它要跟著做很多的應辦事項，其實很多機關沒有資訊人員，他們叫苦連天。現在要把這個定義又再擴大解釋，要再考量一下。我覺得它上面說明的話寫說電子郵件系統、目錄系統、資料庫這個合理，這個是比較風險比較高的系統，那其它譬如說防毒軟體的系統，監視器系統、薪資系統，小機關也會有的小系統，是不是把它排除掉就好了？如果一定要擴大解釋 C 級機關的話，那就電子郵件、目錄系統跟資料庫這樣就好了，不要再擴大了。不然的話可能要先盤點一下這樣會多出多少個 C 級機關，因為現在綁的事項越來越多、越來越嚴格，那資安專責人力的的數量可能 B 級 2 個，C 級 1 個，也漸漸不夠了。以上，謝謝！

主席林春吟高級分析師：

好。原則上我們不是擴大 C 級，比較明確來講應該是 Mail 那一塊，因為 D 級應辦事項裡有 Mail，表示之前你如果只有 Mail 可能是在 D 級，可是近期一

些已經上報的資安事件，都是因為 mail 管理引發的議題，所以有 Mail 這一件事，原則上我們就往 C 級去做處理。那像您提的防毒系統，還是會落在 D 級，因為 D 級也有一些資通業務要處理，防毒會落在那邊。其實監視系統也是一個入侵的重點，因為常常在機關盤點系統時，都漏盤了監視系統，就會有另外的議題。我們看一下近期有一些攻防，其實就是透由監視系統進到機關內部，所以我們會著重一些有管理權限議題的資通系統，請各機關盡量不要再各自建系統，我們的議題點會在那邊，重點不是在擴大 C 級範圍，但是如果說大家盤點的過程中有哪些執行上是不是可以落到 D 去，可以再跟我們反應，我們一塊再做考量，如果說在文字的用詞上有一些建議，或者是在修正上有一些建議可以給我們。如果有一些主機端需要管理設定的，是在機關裡面布建的，機關的防護能量不足就會是你們體系的一個資安破口，我們針對點其實是在那邊，所以希望如果有這樣的情況，是不是提一個向上集中的規劃，像我們跟教育部就有類似這樣的合作，他們在國中小那邊會去推向上集中到教網那邊，過渡期間會協議一個做法，先把等級列 D 級，然後在向上集中完成後，它就是 D 級，中間過程中因為在做移轉，仍要加強防護，這是我們比較希望朝向的一個做法。

世新有線電視股份有限公司：

大家好！我是嘉義世新有線電視第 1 次發言。像 B 級、C 級要考證照的人員是強制還是建議？像有一些單位他們是沒有資訊人員的，那如果強制的話，他們如果好不容易真的逼自己去考了一張證照，但是公司總會有流動的問題，他們可能退休之後或者是換了公司，是不是公司又必須去隨便拉一個人出來又強制讓那個人去考證照？以上，謝謝！

主席林春吟高級分析師：

您是有線電視那一邊？

世新有線電視股份有限公司：

是。

主席林春吟高級分析師：

所以你們是以什麼等級被納管進來？

世新有線電視股份有限公司：

我們嘉義有 2 間，一間是 B 級，一間是 C 級。

主席林春吟高級分析師：

特定非公務機關跟公務機關的要求不一樣，那原則上我們還是回到規定的部分，如果是 C 級特定非公務機關，專業證照就是需要 1 張。

世新有線電視股份有限公司：

強制的嗎？

主席林春吟高級分析師：

這是法規上的要求。原則上，因為你們是 CI 提供者，它在法令的要求上是僅次於公務機關的，所以你們的規範是資安專責，公務機關是專職，所以必須要有人來負責這些資安的事情，我們強調在意的是資安這個作業怎麼做會比較好，所以我們不希望隨便找個人來頂這個位置，因為我們重點不是在有人去占那個位置，而是要做相關的事情。然後它證照的要求在法規上是必須要有的，所以如果你們被指定為 C 級特定非公務機關納管對象的話，那就要照相關的應辦事項去做。

世新有線電視股份有限公司：

人員流通之後還是必定得重考嗎？

主席林春吟高級分析師：

就是以擔任那個專責人力的部分有這樣的要求，現在 A 是資安專責人力，那我可能就要排時間讓他去上課取得證照，那取得證照以後，因為人會流動，所以是不是有 1 個代理人，有時間我也讓他去上課，去取得證照，是在過程中就做這樣的一個處理，而不是說等這個人退休我再去培養 1 個人，因為這個人還是會請假，所以還是會有一個代理制度。

內政部消防署高雄港務消防隊：

主持人，高雄港務消防隊做第 2 次發言，剛剛聽到還蠻多先進針對 C 級機關提出一些建議。我這裡再做一個針對 C 級機關認定的 1 個建議。因為只要沒有專責的資訊單位或是說沒有專責資訊人員，就是說單位內如果沒有資訊單位，或者是沒有專門技術，專技人員、資管人員、資訊人員考進來的這些單位，那是不是代表機關所屬的層級應該不是那麼高，那是不是可以建議列為 D 級。如果說你的機關真的有一些比較核心的資訊系統，那是不是由單位律定上級單位

向上集中，要不然現在的單位多多少少一定會有一些瑕疵，因為這個系統要寫也寫不完，就卡在C級D級的問題，以上建議。

主席林春吟高級分析師：

好，我們再回到我們扣合還是資安風險的議題，就像有一些講駭客好了，駭客原則上他找好打的打，他不是說你是A級我才打你，有些駭客會用工具在網路上會先做掃描的動作，看哪邊有漏洞就從那邊去打，他不會因為你是A級，A級比較挑戰性我就打你，E級其實沒有太多系統，所以我就不打你，他的觀念不是這樣。所以我們也不會因為它是不是有設資訊單位而去評斷它資安責任等級，我們還是看它對資通系統的使用、維運情形，如果它使用的都是中央機關給的系統，它就是1個使用者，它是有機會做到D跟E的，這是真的有。有一些機關像一些縣市政府，它大概只有幾個是B，如資訊單位、衛生局、稅捐等單位是B，有一些C，然後所屬大部分都是D或E，所以D跟E是有機會去達成的，可是的確是需要跟你的上級機關一塊去共同努力的。因為像金管會好了，它在管那一些銀行，其實他們會更嚴謹，它直接要求銀行都要設資安單位，你知道資訊單位本來就有，因為銀行有金融交易，金管會直接就是律定銀行要設立資安單位，它的考量點就是資安威脅跟風險，不會是它有沒有資訊單位來研判它的資安能力。再回到這邊，有一些C級機關也很大，可是有一些C級機關就是1、2個系統，我覺得大家的重心還是放在這1、2個系統可以把它向上集中，或者使用上級機關的系統，不要自己維運，就當1個單純的使用者就好，我覺得大家努力方向往那邊會比較好，大家還有沒有問題？OK，好。

屏東縣政府財稅局：

屏東縣政府財稅局第1次詢問。我想問一下剛剛講到端點偵測，有說要經費的部分，那它是機關明年度要編列這個經費，然後它會有共約的方式讓機關做採購嗎？這是第1個。

第2個部分就是說之前去年吧，那個巡迴研討會的時候有提到專職人力可以用約聘雇，但是經費的部分是以人事費去支付的，就算是正式人力。那你們剛剛簡報上投影片講得約聘雇人力，是指職稱上還是說我現在只要是約聘雇人力，我不管它的經費是哪1個項目流出來的，在延長兩年後都是不能用？

第 3 個問題，普的部分有加上遠端監控的連線加密，那因為 VANS 跟端點的部分，它有提到法公布之後，1 到 2 年完成就可以了，那我這個普的部分加上監控的部分是一生效，我明年就要適用了嗎？因為這個部分很多系統都是普，那目前也都沒有做這個部分，我們可能需要去採購相關的設備，才能符合這樣的規定，那這個時程上的話可不可以解答一下？謝謝！

主席林春吟高級分析師：

好，首先端點防護目前已經有了，那我們現在匡列就是要麻煩大家籌編相關的經費，那我們也會嘗試跟那些端點防護廠商談，就是怎麼可以讓大家經費可以省一點，這邊主要是這個樣子。

然後有關正式人員的部分，因為我們會希望說資安專職人員是正式的，就是人事規定那邊的正式人員去擔任。可是因為大家實務上可能會有一些比較穩定的約聘雇人力，目前在過渡期間是可以的，其他的原則上可能還是要等數位專責機關比較明確的方案出來，我大概先說明到這邊。

再來是遠端監控，資通系統附表十有很多辦理事項，有一些控制措施，初步我們就是請大家至少資通系統要盤清楚，然後把普、中、高級分好，再去檢視說每個系統的相關控制措施，目前的達成情況，或者是規劃處理，原則上就是依你們目前對它的一些風險評估，還有你們經費資源的情況去做對應處理。我們在意的是一定要把它盤全不要漏，就是每一個我都知道它大概的情況，我打算怎麼處理，然後就是照表操課去做相關的對應處理，目前大概是這樣。好，大家還有沒有？

臺灣嘉義地方檢察署：

大家好！我是法務部嘉義地檢署第 1 次發言。那個之前有講到說就是資安法的 FAQ 裡面有 1 個 3.15，有 1 個資訊安全專職專責人員需要 12 個小時的時數。那你們那個 FAQ 裡面解釋有幾個方式可以取得，那我覺得這幾個方式都不是很普遍。第 1 個像資安處所認證的資安訓練機構的資安職能訓練，其實早上也講過說它難度也是蠻高的，也不是說想上都可以上。然後第 2 個技服中心也是差不多。然後第 3 個資安專業證照清單所列的訓練課程，感覺上都不是很普遍。第 4 個更不要說什麼公私立大專院校職能，因為我們今年有被挑出來說是有這個缺點，想要去上，我到網路去查，其實它是很少，根本就它所上的課程

的頻率跟那個課程事實上是不多，所以說在這裡做 1 個建議說可不可以把這個定義放寬鬆一點，那大家如果想上的話可以就比較方便的去上。那另外的話就是說如果要讓大家更方便去上的話，就是可以加開一些數位學習的課程，不然的話，其實我在想很多機關它可能都達不到這個要求，以上，謝謝！

主席林春吟高級分析師：

好。主要剛才講的就是資安專責人員的專業課程或者是職能訓練。職能訓練目前就是技服每年都會遴選一些學校，北中南的學校，他們可以開職能訓練的課，只要你去上就會有時數，剛才說難得是拿到證書，時數跟證書我們分開來看，那些學校開的那些課，就會把它認列進去。剛才其實還有提到就是有一些大專院校，主要是說它是訓練機構辦的資安專業課程，原則上我們這邊才會認。目前我們沒有把數位課程納進去，主要就是因為數位課程有執行上的盲點，因為我們這邊扣的是資安的專業課程，不是資安的通識課程。如果是通識，就是意識訓練那一塊，數位課程是 OK 的，這邊就是專業這件事情，有些機關會跟這些訓練機構談，直接開一個專班給機關及所屬機關同仁，這也是另外 1 個做法；如就既有課程報名，目前有 2 種班，1 種就是我們這邊會負擔一半學費，另外一半就是由機關負擔，不是學員負擔，這種課程很快就滿了，另外有一些就是機關全額負擔費用的，那個課程其實沒有滿的，所以大家還是可以去報那個課，這是目前大概的情況，還有沒有問題？

雲林縣口湖鄉公所：

大家好！我這邊是口湖鄉公所第 1 次發言，我想請問一下有關那個專職人員的部分，我想請問一下你對專職人員的定義，因為像資訊人員的話，資訊範圍其實很廣，並不是只包含資安，那你們的資安專職人員是只能負責資安嗎？還是只要有資訊人員就可以？然後另外的話，就是我們其實還有負責其它的業務，然後我是兼職資安的話，那這樣子有符合法規的規定嗎？就是只能做資安的專職人員，那有負責其它的業務不行，這樣嗎？謝謝！

主席林春吟高級分析師：

資安專職人員，他的業務範圍就是要跟資安相關，那您剛才已經講了，如果是兼職，那一定不是專職，所以兼職一定不是法定意義上的所謂專職，資安專職人員他處理的業務範圍就是要跟資安是相關的，這才是我們的定義。

雲林縣口湖鄉公所：

所以他專職的內容不只是資安的話，就不符合法規嗎？

主席林春吟高級分析師：

就不是目前法定意義的專職。

雲林縣口湖鄉公所：

好，懂了，謝謝！

交通部民用航空局臺南航空站：

主席，您好，我是臺南航空站第 2 次發言，因為剛才討論了那麼久，我覺得這個法是不是要建 1 個自我評核機制，譬如說我們自己都認為我們台灣是科技島嘛，那科技島大概多少人來做資安的事情，然後美國、日本有多少人在做資安的事情，人口比例，這樣是不是適當，是不是合宜，不要說我們科技島，譬如說人家美國 1 個公司幾千人幾萬人，那負責資訊安全大概只有 4、5 個，那怎麼到我們台灣來就變成 40 個 50 個人在做，那我們就是有自我評核機制。我們如果是科技島的話，譬如說美國 4、5 萬個人要 4、5 個資安人員，我們是不是 1 個就夠了？我們才叫科技島嘛，是不是應該把這個自我評核機制納進去，不然法規進去，下面的機關就自我解釋，又開始曲解法令，下面又一大堆亂象出來了，是不是應該這樣子，這樣有 1 個自我評核機制存在的話，才不會這個法規立意是很好很美，但是執行面就會走鐘，謝謝。

主席林春吟高級分析師：

好，原則上我們資安有 1 個成熟度的自我評量，原則上就是讓大家在評量各機關的資安治理作業，目前成熟度大概是怎樣。那有關資安專責能力的部分，原則上它在法上面訂的是 1 個低標，因為資安的工作大家如果要做，非常多，就看你做到多深多細，剛才其實也有機關就講說他們是 B 級，可是他們 2 個資安專職人力是不夠的，那會再往上提，那這一塊就是法令規定，它只能給 1 個 baseline，大家還是得依自己的實務狀況去做一些調適，那我們也嘗試做資安成熟度的一個評量，可是目前在世界各地，還沒有特定的標準可以出來。所以很多其實都在問說資安做得怎樣，其實大家很難衡量，這是一些實務上的限制，那大家給的意見，我們會看看說有什麼方式，或者是有什麼機會可以再讓大家比較好執行下去。

台灣高鐵股份有限公司：

長官們好！我是台灣高鐵資訊部，我姓汪。那個我想請教一下，因為那個特定非公務機關針對那個專責人員有 12 小時的課程訓練。那剛才有講過它的取得方式有 3 種。這個的話其實我們有很努力去報名技服中心的課程，其實都有符合，那另外有 1 個是那個資訊人員每 2 年要完成 3 小時，因為資訊人員其實不是只有少數的 2、3 位，以公司來說的話，我們大概有三百多位資訊人員，可是他要取得 3 小時的方式也是那 3 種，所以對我們來說其實是一個很困難執行的項目。所以想請教一下是不是有放寬可以有其它的認證方式這樣。

主席林春吟高級分析師：

我覺得還好啊，高鐵你們就包專班，幾班開完。

台灣高鐵股份有限公司：

沒錯，這很辛苦很努力去達成它，可是它真的是有它的難度存在，因為我們包班要採購要預算，都很多。

主席林春吟高級分析師：

或者你們覺得有什麼樣的建議我們再列進去的，可以給我們相關的 wording，我們來評估看看，因為真的目前的這些項目，就是我們覺得這樣是比較可以確保的作法，如果說你們有覺得說是不是哪一種機構辦理的，在品質是比較可以的，需要客觀一點的規定。

台灣高鐵股份有限公司：

對，因為它是資安專業的課程，那如果說像我們公司自己內部其實有所謂的數位課程，那我們開課其實也是嚴謹，我們也會以專業的內容去開課，這樣子去符合它 3 小時是不是也是可以的。

主席林春吟高級分析師：

原則上我們會比較希望是大家一致性的，因為每個機關其實都會認為自己辦的是專業的，這樣會不好認定。

台灣高鐵股份有限公司：

所以如果說我們有比較長期合作的這些教育訓練機構，如果提報這樣做訓練也是可以的。

主席林春吟高級分析師：

對。

交通部民用航空局高雄國際航空站：

我這邊是高雄航空站第 1 次發言，剛才有提到那個資安職能教育的課程，我們觀察 2、3 年，可能南部地區都只有昆山科大可以報，可是相對於北部跟中部事實上可以報名的點比較多，所以我覺得說南部這邊就比較奇怪，只能選昆山科大那邊，所以這邊是看可不可以有多一點的點，讓我們可以比較方便一點。

主席林春吟高級分析師：

每年技服都會公告，只要學校有興趣都可以來報名，所以這個也不是說技服自己去挑誰，我要你辦，不是。他們是公開徵求，也要看學校的意願，學校有意願，再經過相關一些遴選機制，通過的話，就會列進去。我們可能就是再看看南部那邊還是不是可以再多 push 一些其它學校來參與這部分。其實縣市政府如果有訓練中心也可以來申請，像台北市政府他們自己的訓練中心就來參與遴選，目前他們也有進遴選的機構，大概是這樣。好，那還有沒有？

嘉義縣衛生局：

嘉義縣衛生局第 1 次發言。我想請問一下，就是說主席剛才有提到這樣電子郵件，還有薪資系統這些部分，然後有這些部分的統統都會列為 C 級機關嗎？那這部分的話，是不是可以請行政院那邊，可能就各縣市政府或是薪資系統的一些主計單位，採取一個就是由您這邊來推動向上集中的一個方式，是不是更為有效。因為可能很多縣市政府可能有自己的資訊系統，那像主計單位也有它自己的資訊系統，那如果為了採取向上集中，由他們來統一，譬如說像轄下的這些 D 級、C 級機關推動的話，我認為這個可能會更加有效率一點。或者像電子郵件的部分，像可能縣市政府也有用電子郵件，那可能它所屬的一些 B 級、C 級、D 級也有用電子郵件，那他們也可以用統一的一個電子郵件，是不是也是由縣市政府來權管這樣子，那這個是建議。那另外再一個就是像差勤系統的部分，我想除了就是像一些比較小的單位，可能只有幾個人或者是十幾個人，差勤系統就是局裡面的一些人員他們相關資料而已，它可能只有少數幾個人，那他們建這個系統他們就變成 C 級單位，這個是不是也有一點矯枉過正啊，對，這個部分的話是不是可以再研議一下。謝謝！

主席林春吟高級分析師：

像差勤系統人事總處其實有建，我們真的建議不要讓大家自己去建。

嘉義縣衛生局：

執行面的問題，執行面下面就是曲解法律就是要我們自己弄啊，自生自滅。

主席林春吟高級分析師：

好，法令認知落差那個我們另外來處理，像人事總處就有在推共用差勤系統，它也是往縣政府那邊推，所以縣市政府所屬的，原則上我們是往縣市政府那邊集中，不會是刻意說你有這個系統，就把你列為 C 級，希望它不要自己再建那個系統。剛才薪資系統的部分，這邊我們再確認一下它是不是有 1 個中央機關來提供那個系統，目前有一些縣市其實有集中建置 1 套薪資系統給所屬機關用，這是我們的目標。然後 Mail 的部分由縣市政府權管，我們就是要推這樣的一個概念，那一段也是大家要努力，我們也會再關注這一件事，因為國發會推動向上集中，那也是國發會的一個政策目標，但是這一段我們後續會再做持續的處理跟推動，好，大家有沒有問題？

沒有的話，剛才是分級辦法，接下來是通報跟應變辦法，通報應變辦法的部分，我們主要就是針對那種多發型的，資安事件目前就是跟自己機關有關係，可是我們有發現有一些是可能是那種有策略性的攻擊，之前曾經像醫療機構，就是可能幾天內好幾件類似的資安事件，主要就是因應這樣的情況，賦予它的上級機關像衛福部，可以自己再起 1 個事件通報，然後來統籌這樣的一個專案處理。那針對通報跟應變辦法，大家還有沒有一些問題？沒有的話，好。

那我們再來就是特定非公務機關稽核辦法的部分，那這邊我們也是放寬，其實機關在提意見的時候，有提到說是不是可以不要實地稽核，不過我們考量了之後，我們還是在時間上做 1 個彈性，主要是今年本來上半年要做稽核的，因為 COVID-19 的事情，整個作業都擠到下半年，所以跟它本來的規劃會有一些差異，我們這邊就是保留了 1 個處理的彈性而已，那目前我們還是以實地稽核為主，那針對這個稽核辦法大家有沒有問題？沒有，那我們再往下。

情資分享辦法，這邊主要是中央目的事業主管機關提出來的，我們之前推資安大概都是公務機關，所以特定非公務機關的資安推動還在起步，我們有稽核過幾個，他們的資安作業，努力的空間還蠻大的。那他們如果願意做一些情資分享，不管事件通報或者是它的體系有一些情資，我們會鼓勵他分享，所以

在這邊，我們就是讓中央目的事業主管機關可以針對它的特定非公務機關有一些情資分享的話，它可以給它一些獎勵，就是鼓勵這樣的一個作為出來，大家有沒有問題？

沒有的話，最後一個就是獎懲辦法的部分，原則上這一個地方主要就是說沒有依法規，屬情節重大，這邊要跟大家講屬情節重大，可能就是應辦的一直被提醒還都不去辦理，沒有一個合理的理由，這種情況的話，那我們在做一些相關的檢討，範圍我們不希望只扣在承辦人，因為有時候可能也不是他的議題，所以在這邊，我們會把整個檢討的範圍就是往主管還有他的上級機關，一塊納進去做考量，在這邊去做一個揭示，它原則上是一個方向的指引。那就我們這樣執行一年多以來，我們看到大部分的機關都很努力的在做，我們不會因為說你一時沒有辦法去處理，因為處理有時候需要時間的，而去做什麼樣的處置。像那個專職人力的部分，剛才在簡報裡大家有看到，A、B、C 級機關在第 1 年，大家的達成情況大概也就是 53%到 63%。在這些 53%到 63%裡面，拿到證照的不到一半。其實這一段都是需要時間，就是大家一塊努力的事情，所以有關這個，反正我們大家就是盡力去做就好了。

那針對 1 個母法 6 個子法的部分，大家還有沒有什麼其它的問題？如果沒有的話，那我們今天的說明會就暫時到這邊。有關執行上如果還有一些想要跟我們做交流的，會後再跟大家做一下交流跟分享，好，謝謝大家，謝謝！