資通安全管理法修法說明會（中區第 1 場次）

逐字會議紀錄

時間：109 年 11 月 9 日(星期一) 下午 2 時 30 分

地點：國立台中科技大學 2 樓國際會議廳(台中市北區三民路三段 129 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：

我們這次修法幅度原則上不大，是在既有的基礎之下，做一些微調部份。比較重點的部份，剛才同仁已經有做說明，其他就是文字的修正。期間我們接到一些問題反應，也會滾動修正相關內容，修正內容會同步更新到會報網站資料那邊。說明會結束後，還是可以去再下載一次，我們會綜整大家的意見。如果這樣沒問題的話，我們就是照母法還有 6 個子法，逐個跟大家做一下確認。

首先是母法的部份，除了目前上面的檔案，剛才有報告會修 7 條，主要就會再增加第 13 條：公務機關應稽核其所屬或「所」監督機關，主要就是把一個「所」加上去，去釐清你要去稽核所監督的機關，這是我們目前修法跟各位手上版本不太一致的地方。有關母法的部份，有沒有哪個機關要給我們意見或發言的？如果您要發言請先舉個手讓我們看一下，如果沒有，那我們要進行下一個了。

好，那接下來就是施行細則的部份，施行細則部份我們目前修法是 4 條，這邊比較會有影響可能就是縣市政府那一塊，就是依地方制度法精神把上級政府的概念納進去。因為目前提資安責任等級或者事件通報審核，在縣市裡面的公所跟代表會，往上都是送給縣市政府的。所以實施情形的部份，我們一樣就是讓這個觀念是一貫的，把上級政府的文字納進去。

另外就是實施情形提報的部份，因為之前法沒有那麼明確，所以大家今年在提去年實施情形的時候有一些聲音，在整個執行過程中，當所屬機關數量很

多的時候，你用一個一個的檔案提報，其實真的是很難蒐集跟管理，所以目前我們也委託技服中心做一套實施情形的提報系統，所以就明定大家都到這邊來提報，上級機關也可以在這邊看到所屬機關提報的實施情形，在做稽核的時候，這都是一個重要參考資料，等於說不要大家再去做系統。其實我們在推資安法，一直一個概念就是向上集中，有關大家會共用的東西，原則上就是統一提供一套，讓大家去做處理。

今年還有一段是比較混亂的就是學校、國中小那一塊，原則上教育部目前跟我們溝通的結果是，應該明年還是會請縣市國中小，一樣到我們這個系統來做填報，他們就不要再去維運一套系統，目前情況是這樣。那有關那個施行細則部份，有沒有要再給我們一些建議或意見的？

好，沒有。那我們進到下一個，分級辦法目前修的項目數是 42 項，在條文裡面就只有 2 條，其它的 40 項都是附表應辦事項，就是比較技術面那一塊。那我看一下分級辦法的部分，對大家可能比較會有關聯就是 C 級機關的部份，在執行的過程中，本來 C 級機關的定義是各機關維運自行或委託開發資通系統，因為現在有一些資通系統是比較套裝式的，在套用上就會比較有一些疑慮，會覺得是不是 C 級？可是現行會有一些用套裝系統在管理機關裡面的資訊業務，或是業務管理，之前我們有聽到 1 個機關，可能是屬於家庭暴力防治的機關，他們用的就是一些公司開發了 1 個套裝的系統，他就拿來用，嚴格說起來，這不算他自己去開發，可是他用的那套系統，他存放的資料是有一些機敏性的，其實機關還是要去要求那個系統，針對相關一些弱點下去做處理。基於這樣的情況，C 級的定義我們就定得更明確一點，如果機關用的是比較像套裝系統的，可能會有一些權限區分或管理功能須納入，目前的定義大概是這樣。沒有權限區分大概就會回到我們的 CIA，其實就是那個機敏性那一塊，他就會有不該看到的人不可以看這個議題，所以我們目前是這樣的一個用詞，如果說大家有更好的用詞建議，也歡迎提供給我們。那有關分級辦法的部份，有沒有哪個機關代表想要給我們意見？或有一些疑問也可以。沒有嗎？這邊有一些應辦事項喔，好，發言前請說一下您們是那個機關，謝謝。

教育部國民及學前教育署：

長官好，我這邊是國教署第 1 次發言。有關於分級辦法，關於人力的部份，

因為B級機關,是要具備2位資安人力,但是因為我覺得光只看資安等級的話,好像沒有那麼的完整。我這邊建議應該要考量，譬如說在資安維護計畫有提到機關自己的系統數量，還有所屬的機關數量，來做綜合性的考量。另外1個建議，因為今年第1次的資安巡迴研討會是放e等公務員作數位學習，但是限時到9月底，建議像這種資安相關的說明會，實體課程也很重要，因為有1個互動的機制，那如果有時候剛好在自己所在區域有說明會，剛好有事沒有辦法參加的話，譬如說像今天的說明會，希望也可以放在e等公務員作數位學習，這樣如果說明會實體無法參加的話，那事後也可以用線上學習的方式，我們也建議不要用限時的，因為這種資訊是真的對我們現在資訊人員還有資安人員，其實都很重要，謝謝。

主席林春吟高級分析師：

我們剛才會有一些發言規則，主要是希望兼顧到大家發言的公平性，不過目前看起來，應該提問不會太多，那我就先就他的問題去做處理。有關專職人力的部分，原則在法規定的是一個低標。剛才國教署的同仁的意思應該是，有一些機關雖然他是B級，可是他要管所屬，還有他自己的本身的資通系統可能又是共用的，那個範圍可能不是2個資安專職人力可以去處理的，那機關其實可以自己再往上去做一個處理，因為法上面，我們目前放的算是低標，因為有一些機關要達到低標已經要很努力了，那有些機關當然是在這低標又往上去，那我們在法只能要求一個至少一定要達到的水準，當你的資通系統數目多的時候，第1個可能先考量一下有沒有整併的空間，因為資通系統一多，其實代表了資安風險、破口可能就越多，你要花的心力也越多，所以我們不希望大家各自去建系統，大家就好好的共用，然後把資源集中起來去做一些防護，把一些該注意的事情，再多注意一點。那有關綜整考量去提升的部份，國教署這邊是可以再把它往上再提高一點，如果涉及一些溝通上議題，我們可以幫上忙的我們也可以幫忙。

第2個就是有關第1次巡迴說明會，當時主要是上半年疫情的考量，所以用視訊，那時候有考量說為什麼設定時間把它下架，因為它裡面有一些議題是比較有時效性，就是過那個時間點，裡面的一些內容可能就不是那麼適用，所以我們就是設一個時間點把它下架，那我們之後可能可以再看看說，是不是有

一些比較沒有時效性的持續放在那邊，讓大家去做檢視。有關那個巡迴說明會，我們下半年是實體場次是 12 月會辦，並已經公告出來了，所以大家如果要報名其實可以趕快去，因為那個也是蠻搶手的。有關這一次說明會的部份是不是放上數位學習，因為我們的時數可能也不是那麼多，這個我們綜整考量一下，謝謝。那還有沒有其它機關？

國立臺中科技大學：

主席，各位與會的同事大家好。我現在要提的是修正草案裡面，有關資通安全等級 ABCD 級公務單位應辦事項裡，現行規定是有分管理面、技術面跟認知與教育訓練，其中認知與教育訓練的部份，原先法條所規定是說資通安全職能評量證書的部份，我們臺中科技大學是屬於 B 級機關，那 B 級機關原來的應辦事項應該要有 2 張證照，當然這次修法裡面我看到 ABCD 各級的那個資通安全評量證書都已經做了 1 個修訂，但是我現在要提的就是說，這個是一個執行面的問題，因為資通安全處現在委託技服中心，現在我們去上教育訓練，每一個學科大概會有 2 天跟 3 天的，那現在在執行力方面，我知道在第 1 年執行的時候上完課後會立刻進行測驗，當時好像通過率不高。當然到了今年好像已經改成上完課之後有一段時間，然後到技服中心的網站報名，大概每年會考 4 到 6 次，根據我們去考的情形，我在中部當然是到中興大學去考，中興大學考試是用電腦測驗，那電腦測驗它在宣布的過程當中，是說依據考選部的什麼規定這樣去做。但是現在問題是，第 1 個考完試之後，沒有公布考題，譬如說現在考試及格成績是 70 分，那當然考試的情形就是在現場考試的時候，會有 1 個現場的說明，說對試題有疑問的話可以提出來，不過那個考試時間不是很長，好像 50 題，大概要考 70 分鐘左右，而且規定的成績是 70 分及格。

那我們這邊要提的是執行面，就是考完試之後他成績就出來了。那如果未達 70 分，譬如說 68 分，那當然技服中心有 1 個申訴的機制，據我所知，如果考題有問題的話，他們會回覆給我們。那我遇到 1 個情形，他今天考題有問題，但是複審的部份，他現在就還停留在複審部份，經過考試兩三個月，他還在審核，但是他們給我們的回答就是，這個題目是有問題，那考生反應是希望考題有問題的話，應該要不予計分，那回答的出題老師給考生的意見就是，技服中心給考生的意見說這 1 題應該要維持計分，那這個那個畫面就一直停在那邊，

就是考了 68 分，但結果 70 分是過不了的。那我們在詢問的過程就是說，技服中心他有回答給我們的考生說，他們的難易程度就是 1：2：1，就是最難的部份大概是占 25%，中間的部份是占 50%，最容易的部份是占 25%。如果這樣的話，他就說應該是屬於容易跟中等應該是 75%，但是他的成績一定要 70 分才過。我們班上大概有 30 個人去上，那第 1 次過大概才 10 個左右。我這邊的意見主要在執行面方面，既然在這次修法有修成每人持有 1 張以上，那這次是不是應該考慮考完試把題目公布給考生看。那我不曉得他們答覆是什麼？技服中心答覆好像是不行。我主要是針對執行面來做一個提出，看能不能做一個改善，大概就是這個問題。

主席林春吟高級分析師：

好，沒關係，你麥克風先給他，我再請教一下。對這題我沒有特定公布或不公布的立場，我只是想要請問一下，就是你們希望公布的想法跟立論點是什麼？我帶回去反應。

國立臺中科技大學：

其實我們從小學、國中、高中、大學或者參加高普考，或任何 1 個公家機關或者公營機關考試，其實他們考完之後都會公布這些題目。那因為這邊職能的訓練，其實是從 108 年正式實施之後，今年是第 2 年，我個人的思考疑慮是說，既然所有的考試都應該公平、公開、公正，那為什麼你題目不願意公布給考生來做改善。譬如你今天規定 70 分，而且它的難易程度中等，就是容易的是占 75%，如果是這樣的話，你用這個去卡我們的公務機關專職人員，我是覺得有一點...因為只要是我們從事這個行業，其實本身都會有一些 ISO 27001 LA 的證書或是教版的，或者說在個資方面 BS 10012 的這些 LA 的證書，其實我們這些都考過，機關才會派我們去參加這些職能考試。

如果你們就是委託技服中心，他們不願意公告、公布，是因為這個是由國內外專家學者參考國際跟國內的考題，他這樣子形容的意思好像就是說，這個考題應該是比較少，在市面上比較少，而且我甚至是去 Google 搜尋這些考題，其實我是找不到的。那我只是希望說，既然要公平、公正跟公開，而且他在考試的期間所放出來的 1 個宣達事項是說，參考考選部的考試規定，那這個其實應該是要讓考生去拿到這些題目，而不是說用這個職能考試去卡那個我們這邊

要拿證書的人。

主席林春吟高級分析師：

好，原則上他們這樣的一個機制，應該也不是說卡大家，我相信有一些他們的考量，那沒關係，這題我們會帶回去然後再研究一下，看怎麼樣處理會比較好，您應該是希望考題公布，然後讓大家至少可以多研習或是練習之類的，好，那我知道了，謝謝，還有沒有其它機關？

臺中市政府衛生局：

長官你好，台中市政府衛生局陳元志第 1 次發言，關於那個資通安全專業證照的問題，一般大部份都取得那個 27001 的證照，那在個資安處的 Q&A 裡面有講說，取得證照的話需要 2 次的實際稽核紀錄，那想要問一下，說如果每年都達不到這個 2 次的稽核紀錄，那是否我的證照就失效了？另外，內部稽核也算是計次的數量，但是我們在做內部稽核的時候，資訊單位一般都是站在受稽的角色，那他勢必沒有稽核的經驗，因為他是受稽的嘛，那這個次數的計算、範圍是在哪邊？受稽也是在那個次數裡面嗎？

第 2 個問題就是說，C 級機關的那個認定修改條文裡面，現在講說使用具權限區分級及管理功能且非自行或委外開發的系統，那麼我們有一些系統都是屬於中央開發或者主導的一些系統，那我們使用單位也具有一部分的管理權限，那這個也算是 C 級機關界定的 1 個範圍嗎？謝謝。

主席林春吟高級分析師：

好，有關證照部份 LA 那張，在證照那邊，原則上就是走證照的有效性，所以不會因為你沒有參與稽核使證照失效。那我們回到資安法認定的證照，因為 LA 那張，它並沒有定期 review，它只有改版，可能上次有改過一次版，那大家會再去取得證照，可是後續他什麼時候改版不知道。我們會希望說拿到 LA 那一張後，你實際參與稽核，不是被稽，被稽不算，稽核這件事就是變成你把你學到的東西應用在實務上，然後以稽核的角度去看這個機關。剛才台中市衛生局也提到，我們的內稽，原則上不是只稽資訊單位，資安法原則上套用範圍是整個機關，所以資訊單位會被其它單位來稽，有可能是政風，有可能是會計，他們組合過來稽資訊單位，可是一樣你們其它單位，你們就可以過去稽核他們，然後在衛生局應該也有一些所屬，你們其實可以去稽你們的所屬，或者是往上

對到衛福部。

那衛福部也有對所屬稽核的議題，我們會鼓勵大家聯合稽核，讓機關裡的資安人員，大家一塊可能這個 A 機關的去稽 B 機關的，B 機關的去稽 A 機關的，大家其實是在把 LA 上學到的一些東西，運用在實務上。像行政院這邊每年都會辦稽核，那在稽核的時候，我們組成的稽核委員，除找外部專家學者，會再留 2 個觀察員的名額。觀察員的候選，就是跟中央機關還有地方機關去徵求，你們可以報名單過來，那我們會把他納進去，等於也讓他來實際參與相關稽核作業，我們的稽核委員會帶著觀察員一塊去做稽核，這樣就算你有參與。其實我們這樣的一個機制就是，希望大家不要只拿到證照，因為實際去稽核的角度真的是不一樣，跟念書是不一樣的。沒參予稽核，只是在資安法上，你的那一張證照，我們在稽核的時候會說，你這張不能算，可是在你的那張 LA 的證照有效性上，還是有效的。

然後還有 C 級共用，因為中央開發一些共用系統，它會有幾個模式，1 個是它就建在中央，各機關是連過去做使用，那這時候你就是 1 個單純的使用者。原則上會在 D 或 E 級，可是如果說那一套系統是在你們機關裡面有佈建一套，是架在你們機關裡面的，那一定至少是 C 級。雖然那一套是中央開發的，可是因為它架在機關裡面，它就會有一些資安防護的議題，不管是架你們的 Firewall、IPS 或者是定期去檢核，通常走這樣的架構，中央部會不會跑到你們機關做掃描還是什麼的，他可能有發布一些版本讓你去更版，相關的一些維護作業，還是要由機關這邊來做，所以如果是這個情況，你還是會落到 C 去，雖然那個系統是中央給的，可是取決於它架在你們的機關網域環境裡面。只要有資通系統或 1 個網站都會算成 C，所以我們才一直推向上集中。

現在等級調整上，C 往 D 降的情況是最多的，因為很多機關他常常只有 1 個網站，然後想辦法就讓上級機關幫他建到網站共用平台上，這個機關原則上就只是做那個內容的維護，這樣他整個系統維運就會由上級機關去處理，他就有機會往下降一級。那您剛才講的應該是中央一套系統，還是有一些佈在你們機關裡面，那就要看，因為如果他是佈在你們機關裡面，可能有 2 種，可是現在應該比較少走那個 client server 的架構，client server 的話，server 可能在中央，可是 client 就是你電腦那邊會裝一個小程式，這種 client server 可能有討論

空間。人事總處提供的共用系統，其實他有一套就會架在機關，像公文電子交換也一樣，如果縣市政府會架在那個縣市政府那邊，那縣市政府就要負那個維運的責任，雖然版次是中央統一給的，大概是以這樣來做區分。如果說在執行上有一些要釐清的也沒關係，就再跟我們聯絡，我們大家一塊討論。好，那還有沒有其它？

臺中高等行政法院：

主席，這邊是台中高等行政法院第 1 次發言，有關於資安專職人員就是全責辦理資安工作的人員，但目前人力不足，就是可以以委外的人力來開發，但是之前就是說講到今年年底，所以等於就是明年年度的經費現在立法院已經在審了，所以來不及再編明年的部份。那我這邊是建議說是不是在那個人力的問題上面，能夠在資通安全法，現在這次修法能夠一併來解套？就是在法規裡面，能夠去定義每個機關他一定要新增 1 個人力，因為現在有預算員額的問題，所以其實各機關，你說要去新增這個人力是很不簡單的，我們現在都變成要用原來的人力，然後去做這件事情，但是原來的工作誰來做？所以這個部份是不是能夠用資通安全法，用法規來解套，明定各機關一定要新增人力。

然後第 2 點就是說，那個資安職能的考試，我本身有去上過，然後我不斷的去考過。但是我聽同事在講，就是這個考題部分，好像是要考倒大家。我感覺是你應該是考基礎，就是說教材裡面，起碼我能夠把這個課本看了，我能夠及格，結果大家是把教材都看得很熟了，結果還考不及格，我不曉得這個是要考倒大家還是？因為我覺得應該就是考大家基礎觀念有沒有通嘛，有很多複選的項目，就是感覺很難去準備，那大家其實工作上平常已經很忙了，然後還是接這個工作，然後人力部份又沒辦法解決，我是覺得是資通安全法應該要幫大家考慮，儘量考慮到人力的問題，謝謝。

主席林春吟高級分析師：

好，有關職能證書的部份，剛才您反應的，我們請技服中心同仁這邊帶回去，然後再檢視一下。有關專職人力的部份，我們資安處在努力，不過就機關員額，還是有他另外的法規規定，所以我們法跟法中間也不能互打，那段我們有持續在努力。我們今天簡報最後一頁其實有提到，我們會配合那個數位發展機關，最近有一些新聞，如果大家有注意到的話，大概會看到，那有關那個資

安人力部份，會併同那個數位發展機關一塊去做考量，就是等那邊比較明確的時候，其實大家可能就會知道後面的一些做法跟方向，那在還沒有出來之前，我們會把整個過渡時間再往後延 2 年。因為有一些機關，我知道在機關裡面爭取員額真的不容易，那有一些機關很幸運，他們的首長支持，然後整個有去爭取到，那當然很多機關也持續在努力。過渡時間我們會往後再延 2 年，所以大家壓力不要那麼大，我們去調查 108 年大家的實施情形，裡面有關資安專職人力的部分，就是 ABC 級機關目前的達成情況，他們填回來的情況大概就是 53 到 63%，那表示大概還有 3、40%的機關其實還沒有辦法達到，還沒辦法順利爭取到相關的員額，等於說他們可能就要用過渡性的做法來處理。我們還是持續在關注這個議題，持續有在跟人事總處那邊做一些交流，目前大概就是看一下數位發展機關，那邊如果有定案的資訊出來，會併同這個議題一塊處理。

臺中高等行政法院：

因為好像有聽說要增加那個資安職能的職系，資安職系。

主席林春吟高級分析師：

都會併數位發展機關的正式公布，看後面會怎麼處理，所以可能就要請大家再稍候一下。

臺中高等行政法院：

是說最主要就是說多了執行，但是人力部分就是說要補充給各機關，我是覺得這個法真的多了不少事情，然後變成我們現在也沒有新增人力，都是原來的人也要去吸收這些工作。

主席林春吟高級分析師：

好，我知道，其實資安作業，行政院從民國 90 年就開始推了，大概是電子化政府開始起步的時候，那時候就注意到電子化政府可能帶來另外一個資安方面的議題，可是近期資安威脅跟以前比，真的是差太多了，現在威脅趨勢的成長應該是很快的，所以你也不得不在這邊多做一些著墨，這個可能也是辛苦大家，我知道大家一定是先從既有的資源去做一些運用，那法規上要做的事情，也非常謝謝大家，非常支持跟努力的在運作。那有關人力的部份，我們就先確認一下，併同數位發展機關議題一塊處理，好不好？謝謝。那還有沒有？

臺中市政府社會局：

不好意思，想要請教是說剛才提到的稽核(證照)這個部份，是不是每年都要去進行機關的稽核，那如果說用那個委外廠商的稽核，這個算不算？

主席林春吟高級分析師：

可以算的，因為我們重點是在稽核這件事情。你們在稽核廠商的時候，要先做好相關的稽核規劃，然後讓你們的同仁可以去培養。有一些機關以往不太自己做稽核，會讓他的委外團隊也會一塊，初期是一個過渡，有點是銜接、培養自己機關同仁的一個稽核能力，看看委外團隊是怎麼稽的，那我們可以怎麼稽。實務作業上我們看，其實同仁去稽出來的其實會比較深入，因為同仁對業務會比較熟，自己的同仁其實會比較清楚自己的需求，所以如果有委外團隊，可以借用他們的長處，可是不要只依賴委外團隊，我們還是要培養自己同仁一些資安跟稽核的能量，相關的參與作業你們就留好紀錄，主要是做稽核這件事情就可以。好，那邊。

彰化縣警察局：

長官好，這邊是彰化市警察局，想請教幾個問題，第 1 個就是我們 B 級機關，應辦事項在管理面有 1 個限制使用危害國家資通安全產品，上面的定義覺得有點模糊，下面科室還問說，我可以使用大陸產品嗎？這個我們不好跟他回答說，因為它上面沒有寫說不可使用大陸製產品，坦白講大部份都是，只是牌子不太一樣而已，那如果我們本身的能力可能沒辦法確認說，他使用這個大陸的產品，到底會不會對機關造成資通安全的危害，所以這塊在定義上有沒有更明確讓我們可以做判斷?因為看上面好像中央這邊會列一個清單，讓我們做選擇，從去年或者更早之前到現在，也都沒有(發布)，所以單位內部在簽是否是大陸產品，是否有資安疑慮，我們都很難寫有或沒有，這是第 1 點問題。

然後第 2 點就是現在應辦事項裡面有很多要做的工作，先講第 1 個問題好了，就是端點偵測及回應，想了解端點偵測的範圍，我們是只要有做就可以了嗎？還是說一定要全機關每台電腦?因為這牽扯到經費的問題，廠商給我們報價，因為我們電腦台數大概 2,000 台，光這一項可能要花 200 萬，我們在經費上不足以支應，想了解所謂端點偵測是做到每 1 台個人電腦，或者只要針對我們核心系統、機房端、重要核心主機有做至少可以符合要求?

第 3 點就是資安弱點通報機制，這個也是牽扯到經費的問題，我們就不再多說了，結論就是很多工作都牽涉經費的問題，因為有些工作項目想要納在未來 4 年的清單，後來好像也都沒有，關於明後年經費編列，這一塊中央能夠給地方經費上什麼協助?很多法規要求，但是實務上也不會給你錢或沒辦百分百滿足工作上要求的經費，以上 3 點建議。

主席林春吟高級分析師：

好，有關那個危害國家資通安全產品的部份，因為相關的清單，我們是持續在做一些技術檢測跟一些國際趨勢的一些關注，所以短時間內可能不太會出來。我們今年的資安長會議，有 1 個會議的結論，就是請大家不要採購或使用大陸產品，那是很明確的。所以你們的市府應該會有收到這份紀錄的公文，可以先拿那個，因為有關大陸的軟硬體還有服務，其實在近期的情資來說是風險極高，所以我們會建議你們就是不要去使用或採購，然後甚至是你們現在的資通系統，你都要跟你的委託團隊確認一下裡面有沒有用到一些大陸元件，或者是他在大陸有一些研發團隊或成員，那個都要確認。因為在一些資安的議題上，我們發現有這樣的情況，可能是台灣的廠商比較沒有議題，可是他裡面的服務元件有可能去用到，所以這個你們要再跟你們的廠商那邊再做確認。那大陸的軟硬體跟服務，原則上我們就是不使用、不採購。所以我們在調查去年的實施情形的時候，我們有一張附表 4，就是專門調查那個大陸的資通設備。那我們明年會調查的可能是一些軟體還有一些 APP，APP 真的不要亂裝，我們目前比較明確的就是，大陸那邊軟硬體產品跟服務，就是不要去做使用。那其它的資通服務或產品，那你們就可以就你們自己的一些評估去做一些處理，大概是這樣。那有關端點偵測的部份，因為它初期，你可以把它看成跟資安健診一樣，使用者電腦那邊就是要導入這樣的一個機制，看你們機關，資安要做這些作業一定是需要經費，經費是有限的，然後去評估說應該是先投注在哪邊去做處理，那是一個比較好的一個做法。

端點防護、VANS 的部份也是一樣，VANS 的部份原則上就是看看你們機關內部，如果已經有一些資產管理系統，尤其像你們可能一兩千台，會導那個資產管理系統，那你至少已經把資產資訊收回來，它有一個轉格式的議題，目前有一些市面廠商，他也有服務就是專門幫你轉 CPE 格式，讓你們可以評估相

關的 solution，然後去做一個介接，主要是比較可以快速掌握，因為近幾年多資安事件都是因為弱點已經被公布了，可是沒有修補到就進來了，後面要收拾就更不容易。大概是這樣。在經費跟人力上，我們就是盡量的看怎麼把它用在比較 critical 的部份，先優先去做處理，好不好？好，大家還有沒有？那邊。

國立臺灣體育運動大學：

好，這邊是台體大第 1 次發言，那我這邊想問的，就是目前有關委託辦理的部分，這邊是說委外寬限期一直到 111 年 12 月 30 日為止，那針對資通安全相關事務，因為人力關係，很多工作都委外，想問說，是不是 111 年 12 月 30 號之後,都不能委外?或者是說有部分可以委外?哪些不能的委外?希望有明確的 1 個範圍，第 2 個部份的話就是說，專職人員是以正職人員配置，正職人員的話是哪些人員？一般來講公務人員是正職人員，是這樣子，或者是說在法規應該針對正職人員明確定義，以上。

主席林春吟高級分析師：

好，我原則上我們規範的是資安專職、專責人力，不會說大家資安這一塊不能委外，它是 2 件不一樣的事情。正式人員的部份，之後我們還是併數位發展機關，到時候一併做一個處理。因為在我們的立場，我們希望盡量是在機關裡是穩定的人力，之前曾經有討論過，除了正式編制之外，因為有一些機關的約聘雇人員，如果他是屬於穩定的，我們其實也可以把他納進去做考量，可是因為有一些機關的約聘雇人員，他不是穩定的，所以那一塊你會很難說是或不是，我們考量點都是在說，屬於機關的 1 個正式的運作人力這一塊，我們是可以把資安的一些核心作業，還有核心資訊，掌握在自己手上的，以這個概念做切入，所以他的正式定義可能還是要併那個數位發展機關，到時候我們會一併有一個整體的規劃。

彰化縣政府：

彰化縣政府，有關分級基準從 D 級移到 C 級，那剛說這樣子到底會影響到多少機關？這樣整併是一個很大的缺口，譬如說像電子郵件系統在共契的話，到時候可能一年才幾萬塊授權，但是變成 C 級，他要有一段時間的努力，他要做 VANS 或其它的一些工作。可能要數十萬，所以這樣子的經費，就是說除了把它改成 C 級，有沒有其它的方式來增加他的屬性？

那另外一個問題就是資通安全維護計畫的提報，是可以把所屬納進來，上級機關可以幫他來函發。但是在維護計畫實施情形的時候，譬如說像公所他的維護計畫提報的時候，就包括清潔隊、圖書館，幼兒院這些機關。但是如果說是維護計畫實施情形提報的時候，幼兒園、清潔隊、圖書館他們自己去提報，那我們彰化縣有 26 個公所，但每個公所下面我們所屬機關就一下子就增加了 100 多個。所以是不是維護計畫實施情形提報也是可以比照安全維護計畫的訂定，上級機關一起幫他提報就好了，不用再個別機關提報？以上建議。

主席林春吟高級分析師：

有關 mail 的部份，他買這樣單套是便宜的，可是後面要做的資安作業，其實是不能被忽略的，我們會希望的是，也不要各個機關自己在那邊建 mail，我們還是希望 mail 的服務可以往上，因為近期有幾件 mail 管理不當，造成了一些資安事件。為什麼我們常常在練社交工程？常常外面入侵到機關裡面，都是透由社交工程進來的，mail 的管理，事實上如果說該補漏洞沒有補，更容易有風險，因為相關的一些掃描工具在網路上很常見，一掃就發現弱點，如果你們要架 mail，你又不去注意它的資安管理，那我們建議你是不是跟你的上級機關那邊，共用它的 mail 就好了，因為 mail 後面還有一些其它的議題要處理，你就不能單看說我買一套 mail，其實才一點點錢，就怕因為很便宜就買來用，可是其實你不曉得後面要做一些處理的事情，就會變很辛苦，尤其如果是 D 級機關的話，可能連資訊人力都不見得有的時候，你要讓他去處理資安，難度其實會更高。

然後第 2 個就是有關維護計畫，計畫是 1 個規劃，所以大家可以一塊，就像每天我們可以規劃說我要吃午餐，要吃晚餐，這是一個規劃，大家可以一塊寫，所以一塊提維護計畫議題不大，可是實施情形，就要每個機關去呈現他吃了午餐以後的效果，那每個機關是不一樣的，所以你不能說我就是把我的情況寫成好像他跟我一樣，實施情形是要每個機關不同去呈現，那當然有一些可能像清潔隊，實施情形可能他不會寫，那沒關係，公所可以幫他寫，可是一樣，你就是要就清潔隊它的實施情形填進去，所以維護計畫跟實施情形，可以整個去處理，但還是要個別呈現它的資訊，它的概念其實不太一樣。好，大家好像都是比較執行面的問題，我們還是先回到我們修法這邊來。有關分級辦法的部

份，大家對修法的內容，看是不是還有其它的意見？

內政部國土測繪中心：

你好，這邊是內政部國土測繪中心。我想問一下分級辦法的第十一條第三款，其實資通安全法的所有資通系統，不見得會符合附件十的防護，那麼第三款規定中沒有符合的情況下，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得報請主管機關核備後，免執行該事項或控制措施；其為主管機關者，經其同意後，免予執行。那像我們內政部所屬的機關，我們會得到一個問題，我們次級機關其實沒有人力，沒有資安人員哪來的資安專責，什麼叫專責？我們現在都是兼任，那就是現場的苦力，這是第 1 個問題。

第 2 個部份就是，這些系統已經過了 2 年，一直都沒有達到這樣的保護等級，那我們到底應該要到什麼樣的程序來回報？我們可以說因為技術和人力的儲備不足，我們還可以暫緩實施嗎？還是說這個部份怎麼提報給主管機關？還是提報到行政院資通安全處去？我們今年下半年內政部要求，所有明年度的資通系統在寫採購案的時候，要先評估自己附件一到附件十的項目是不是有達成？如果沒有達成要寫在合約裡面。我們今年遭遇到最大的困難就是，如果要達成這些項目，到底要花多少經費？沒有的部份，明年度的資通安全這些系統要怎麼執行？這是我們現階段遭遇到最大的困難，以上。

主席林春吟高級分析師：

好，有關就是分級辦法第十一條第三項那一塊，因為大家執行上可能會遇到困難，主要應該是附表 10，附表 10 主要是就資通系統的各個階段，還有一些存取控制那邊做一些普中高級的規範。有一些系統可能因為它是很久以前建的，所以它在執行上或在技術上，有它實務上沒有辦法執行的困難，在我們法的一個精神，原則上你先報給內政部，在提報之前，我們建議就是先跟內政部那邊溝通，因為你們的等級提交機關就是內政部，你們是內政部所屬，所以會提給內政部，原則上是先跟內政部那邊確認那一塊是不是需要報？就是執行顯有困難還是希望去排除的，他的整個程序是這樣。那至於說顯有困難的議題點，原則上我們比較扣在技術，可能是新舊版本的資源或者是軟體硬體的限制，還是什麼的，那些情況下才去做排除的動作，有關比較執行的細節，我建議就是

先跟內政部那邊討論看看，萬一還是有一些議題的話，那沒關係，就看找內政部，還有我們，我們就是一塊可以做一個細部的討論。好，大家有沒有？那邊。

南投縣政府：

南投縣政府第 1 次發言，我們這邊聽起來就是施行細則第六條，有新增條文就是維護計畫相關內容，公務機關得由其上級、監督機關或上級政府辦理，並依主管機關指定之方式提出前項實施情形，所以目前是不是可以放權給地方政府，甚至鄉鎮市公所？因為我們很難想像就是實施情形，我們很難想像要怎麼去跟清潔隊的人員還是幼兒園，介紹說策略面怎麼寫、技術面怎麼寫，剛才高分說得好，維護計畫一起寫，但是個別執行還是要個別寫，是不是可以把權利放給公所，然後讓他們決定提報的樣式的，謝謝。

主席林春吟高級分析師：

好，有關實施情形提報，我們有注意到就是 D 級跟 E 級，因為它本身應辦事項，其實就比較少，然後理論上他們提的東西，應該會比較簡單，所以我們今年在實施情形填報那邊，有做一些簡化的調整，如果說南投縣這邊有一些提報的建議，看是不是可以提供給我們？我們統一做處理就好。因為我們現在很怕就是，如果你有 10 個公所就有 10 套標準，這後面會有點難處理。所以有關簡化的部份，看有什麼樣的明確建議，就提供給我們，我們就在整個填報系統，可以把它弄進去，然後讓全國有關 D 級、E 級的機關，都照比較一致性的標準做一些填報，好不好。好，大家還有沒有？沒有，我們要進到下一個？好，這邊。

臺中市政府社會局：

不好意思，我第 2 次發言，可以嗎？資通安全責任的分級辦法，我們意思就是說針對各機關自行或委外開發的資通系統，依附表 9，鎖定資通系統，防護系統，要完成資通系統分級，那我現在這邊的疑問就是說，應該寫自行或委外開發的資通系統做分級，那請教一下，如果是這個系統是上級統一委外開發完成，然後給所屬機關使用的這些資通系統，我們需不需要去做這些事情？做分級這件事情？因為如果說我們是所屬，那如果說所屬機關自己針對上級機關所開發系統，我們還要自己再去做分級的話，那所屬每個機關，他所定義的分級標準不一樣的時候，不曉得這個是屬於上級的事情還是我們的事情？

主席林春吟高級分析師：

好，原則上，我先講原則上，那個像共用系統的部份，它的資安維護作業，在那個開發的主政機關，責任是最重的，他可能會在你們機關裡面有做使用，那你們機關記得盤點，一定要把它盤出來，不要漏。那其實下一個點，原則上就是看那一套系統，在你們機關裡面的放置程度，它整套進來還是不是？因為他整套如果建在你們機關裡面，就是你們可以對他的管控程度，如果只是那個防護作業的話，那你們就是把防護作業做好，那他的普中高級，原則上就讓那個提供機關去做核定就好，因為你們可以做的是他的周邊防護，你比較沒有辦法對它的版本或者是它的一些存取控制，去做附表 10 的動作，所以那個會回到上級機關那邊的權責。可是你們在盤點的時候，一定要把它盤出來，千萬不要說這不是，這是上級機關給我的，我就沒有盤進去，這樣會漏。

臺中市政府社會局：

你的意思是說在資通系統的資產盤點？

主席林春吟高級分析師：

資產盤點，還是要盤出來，對。

臺中市政府社會局：

那針對 11 條這部分就不用主動去做分級對嗎？

主席林春吟高級分析師：

對。

臺中市政府社會局：

好，謝謝。

主席林春吟高級分析師：

好。我們往下一個，再來是那個通報應變辦法。這邊主要也是因為資安事件是沒有辦法避免的，可是大家平常又得做好相關準備，有點像把它想成地震演習之類的。所以在事件通報跟應變的部份，我們還是要跟大家宣導一下，你們機關裡面，一定要做好相關的一些作業，萬一資安事件發生的時候，你怎麼去組成整個應變團隊，尤其是三級以上的，只要有個資外洩部份，原則上就會到三級以上，那整個處理的組織，還有資安長的關切，那些都記得要去做處理。

近期我們處應該有給大家一個資安事件應變的作業程序，就是還要麻煩大家參考一下。那我們這一次修法主要是針對就是比較聯合性的，我們舉個例子好了，像應該是去年吧，醫療體系那邊有幾個醫院就發生資安事件，那時候衛福部其實算很積極，他就發現不對，不只一家，因為通常我們只會注意自己機關的資安事件。那如果說他的上一層有注意到不對，好像有好幾個機關都有發生，那他其實可能要提高警覺看看。

我們的這次修法，就是讓上級機關針對這樣的情況，另外再起一個像專案性質的資安事件，來做後面的統籌處理。那針對通報及應變辦法，大家有沒有要提出問題的？

好。如果沒有，那我們再就特定非公務機關的資安維護計畫實施情形的稽核辦法。這邊只修了 3 條。好。有沒有？如果沒有，那我們就再往下。

情資分享辦法這邊主要是針對特定非公務機關那一塊，主要有 1 個中央目的事業主管機關提供的修法建議，希望可以鼓勵情資分享，像各位資安事件就是一個重要情資，對我們來講它是 1 個重要情資，所以我們鼓勵大家通報，這可能跟以往的觀念會有點矛盾，這是我們一直在做一些強化說明跟宣導的部份。

好，情資分享，如果沒有的話，那就是獎懲辦法的部份，原則上我們修了 1 條。主要就是在如果說沒有依資安法執行，情節重大的情況，我們要去檢討的範圍，會把主管或者上級機關一塊納進來。目前我們對資安法的推動，原則上我們都是採鼓勵的方式，這個作業我們不會希望去動用到，在執行上其實我們也是會一再的提醒，不過還是要麻煩大家就是盡量配合，如果執行上的困難，可能大家就一塊看怎麼去執行，然後共同把這件事情做好。

好，那如果也沒有的話，那我們今天就是針對 1 個母法跟 6 個子法目前的修法概況在這邊跟大家做報告，那大家如果沒有問題的話，我們今天的會議可能就到這邊結束。如果大家在資安法執行上有什麼問題的話，我們可以再做一些討論跟了解。好，謝謝大家，謝謝。