資通安全管理法修法說明會（南區第 2 場次）

逐字會議紀錄

時間：109 年 12 月 21 日（星期一）下午 2 時 30 分

地點：高雄國際會議中心 303A 會議室（高雄市中正四路 274 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：

首先就剛才簡報，機關提問的人力問題做回應，資安法開始實施的時候，就訂了 4、2、1 位的專職人力，那時候考量到過渡期，大家要爭取員額或是配置人力需要時間，所以本來的 QA 裡面原則上列了 2 年的過渡期，那個 2 年到今(109)年年底就結束了，代表的意思是明(110)年開始，你的資安專職人力就要以正式人員去配，他本來代表的意思是這樣。剛剛在簡報裡面不，知道大家有沒有注意到，我們會去調查大家的實施情形，目前 A 到 C 級各機關被要求資安專職人力，它達成的情況沒很理想，大約在 50％到 60％，那個是普遍現象，這個我們有注意到，當然法規還是訂在那邊，組織內人員的部分，我國法律不是只有資安法，也還有組織法，在組織內的員額權責，原則在機關首長，要怎麼去溝通協調，跟人事總處也要做相關的協調，我們也希望幫大家爭取用外加的方式去弄，可是整個國家還是有總員額法。

剛剛這位同仁提到是不是可能一條鞭，那個也有在討論的過程中提出過。就是說我們也有在努力，可是整個國家體制，大家還是得照著程序走，這點造成大家壓力，我們很抱歉。目前就是處理數位專責部會的時候，他們也有把資安的事情納入考量，我們就是等那個方案出來，看他們在那個方案內，如何把資安人力做一個統整的討論，目前可能有一些新聞有一些露出，可是還在做朝野協商，在方案還沒出來前，原則上我們不能跟各位確認，目前因為要互相搭配，所以我們會把過渡時間再往後延 2 年，當然因為整個時間沒辦法在今年年初就處理，因為那時候也還在處理其他方案，就是請大家互相體諒，我先回答剛剛那位同仁的問題。

國立虎尾科技大學電算中心：

我們主管叫我們來問這個問題，因為根據資安法 QA 1091124 內容中3.3回應也是根據這個，資安專職人力必須編制正式人力，但是可以先以約聘雇或委外人員擔任至本法實施後 4 年（110 年底）再以正式人員編制，現在我們的問題在於，我們是學校單位，學校單位本來就不只有公務人員還有約用人員、計畫人員，約用人員我們是以學校校務基金去聘用的，我想請問，目前我們學校已經向學校申請經費，希望用校務基金聘用約用人力來擔任資安專責人力，我想請問的是，正式人力是不是一定要是公務人員？這是我們的問題。

主席林春吟高級分析師：

對，我們目前在規劃資安的專職人員，是以正式人員，人事單位稱他們為職員，就是正式人員，我們過程中也曾經討論，如果是那種比較穩定的約聘僱人員是不是可以納入？可是在一陣討論後，目前還是暫緩，所以目前還是以正式職員為主，您剛剛講的校務基金聘用，聽起來比較像是契約關係，可能 1 年 1 聘還是？

國立虎尾科技大學電算中心：

是不定期的。

主席林春吟高級分析師：

不定期的，那原則上，在過渡期間是可以的，可是還是要朝向以正式人員擔任，目前政策方向是這樣，謝謝。

福建金門地方法院資訊室：

我大概就是 2 點，第 1 點就是我們在稽核上絕對不能自己稽核自己，所以我一直覺得修法應該是走，既然是資通安全處就應該下轄所有各機關的所有資通安全單位，如果真的做不到這點，像我們很多內稽是政風室在稽核我們，就在政風室底下設立人員，說實在我們資訊人員在資安這個部分，不是我們不學，問題是我們沒有時間去做這個東西，你說考了 1 張證照就可以保證網站不會被駭、資料不會被偷？這個是有點說夢話。以現在來講，資訊人員再努力要成為合格的資安人員，這實在是...所以我當初在 3 月份編的時候，就知道這個一定會延，因為你根本找不到合格的人力進來，所以基本上就是不要讓資訊室人員去擔責任，就由資通安全處下轄各機關一條鞭下來，我們只要負責做規劃執行，出問題由專職人員去負責。

第 2 點是有關於 A、B、C 級的單位認定，當然講 A 級要 4 個、C 級要 1 個，可是，不是說我機關是幾個 A 級還是 B 級，你現在 1 個人都不給我，我憑什麼當 C 級，我覺得機關的認定不是系統什麼的，你沒有人力你就是降級，這個才是對的，你沒有人力憑什麼要求我做？這樣才能解決大家問題，你現在這個資安專職人力補充，絕對不是幾個人可以做到。

主席林春吟高級分析師：

當你有資通系統在那邊，不是降等級，駭客就不會去打你，他打的是資通系統。

福建金門地方法院資訊室：

但你們人沒有給，你又要求我做。

主席林春吟高級分析師：

我要講的是，剛剛我也講過了，機關的員額不在我們手上，那我們也只能透過我們接觸到的高層那邊去反應，然後往人事總處那邊去反應，各位在機關裡面，我知道大家有努力爭取，有些也成功了，有些機關還在努力，因為有些機關首長，當沒有發生資安事件的時候，他可能覺得資安沒有很重要，我知道 1 個案例是，之前去爭取資源爭取不到，可是在某次資安事件上報後，他就有個員額出來了。

你們要這麼解讀，我沒辦法控制，可是我要講的是，你要讓你們上面的主管、首長認知到資安的重要，給資源這件事情是重要的，我們也只能透過我們的方法儘量去宣導，希望讓這個觀念盡量落實，不會是一次到位的，資安會報從民國 90 年推動到現在，推 ISMS 制度也是從民國 90 年到現在，我們之前去稽核的時候，也發現過有單位沒有導入 ISMS。我只能說要逐步地去做，資安這件事情要逐步去做，我們以前的進程比較緩，議題不大，可是現在所有東西都連網、行動化了，每個人手 1 台手機，連民眾都是這樣。

再來，另外一邊是我們，簡稱駭客，他們也在資安事件裡面，算嚐到甜頭，最近連民間業者都發生資安事件，以前我聽到另外 1 個部會在講，以前他們推民間的資安很難推，去講的時候要從跟他講什麼是資安開始，講很久人家根本聽不下去，現在不太需要了，因為過去跟他們談的時候，他們立刻知道，因為他們中過勒索病毒，曾經受駭就會比較能了解資安跟它的重要性，我要講的是這件事情，我希望大家還沒受駭前就能先防好，

駭客打的是最弱的，沒有要大家做到最強，可是至少大家不要成為最弱的那一個，因為在網路上一堆工具很好找，最近也有一個新聞，連勒索軟體都有開源程式，可以拿來用，就可以知道有多猖獗。

我知道大家的資源，以往都是配置在提供機關、單位內的服務，或是便民服務，光是資通服務大家就花很多精力，以前我也在其他機關單位待過，原則上資安就是不出事，我可以理解大家的想法、心態和做法，但是因為現在整個時空環境跟之前不太一樣，很多東西變成以往這樣做可能沒事，但現在這樣做，就要多一些考量，爭取資源這件事情我們會持續去做，可是也要麻煩各位在機關內去呈現，不管是用法遵議題也好，原則上我們去稽核會寫缺失，例如專責人力未符法遵，我們重點就是在幫忙跟機關主管爭取資源，所以大家用這樣的角度去看這件事情會比較好，可是人家來稽核寫資安專責人力不夠，覺得是傷害的話，其實就比較不會達到那個效果，我嘗試用這樣的方式跟大家說明，我知道一些機關的主管其實沒太認知到資安這件事情，我們有發現這個現象，我們會持續看用什麼方式來處理。

福建金門地方法院資訊室：

補充一下，事實上我們去年司法院有預算要增員，我們資訊室已經得到院長同意第一時間先補資訊室，可是後來被砍掉了，可是不是我們不努力，是上面長官太遙遠他根本體會不到。現在我們弱勢團體都有補助，像我們這種 C 級單位要有 1 個人，我們資訊室只有 1 個人，你要我做資訊業務又要做資安的部分，是不是能有補助辦法，救濟一下我們這種三級貧戶，你可以審核，如果我人很多就不要給我錢，如果有些資訊單位真的沒有人或只有 1 個人的，你要他們資安專職真的沒辦法，拜託施捨一點錢讓我們可以先撐一下，我要去考證照也需要時間。

主席林春吟高級分析師：

司法院原則上又跨出行政院，我們會跟它溝通了解一下，因為院與院之間是平行的。

福建金門地方法院資訊室：

因為我們長官跟我們講不要再講這個東西了，所以我只能向外求救。我有想說乾脆我自己出錢，但是廠商說不能這樣做。

主席林春吟高級分析師：

我們今天的議程先做修法的討論。

經濟部加工出口區管理處：

我們長官在這個地方想確認，所謂專職人員當然是專門負責資安，但這個專職人員可以兼職做其他事情嗎？因為我們人力實在很有限，他如果不兼職做其他事情，根本沒有人，所以我們長官想確認這件事情。

再來上次簡報說要正式人員，我們有去問人事室，何謂正式人員？因為我們有先問部裡面的資訊中心，所謂正式人員是什麼？他說所謂正式人員要人事室來認定，我們的確也是那種計畫起用人，可是我們人事說那個也是正式人員，這樣就跟你們認定的不一樣，這個部分是不是要跟人事總處溝通？我們長官還是聽人事室的，如果還有其他正式人員，他不會給你員額，他會說你們自行更動就好，也就是把正式做資安，把做資安的調去做其他事情，可是問題是專長不一樣，但他認為那個不是他的問題，要我們自己解決。

主席林春吟高級分析師：

我再講一遍，中肯的解釋一下法條，資安專職人員，從事資安相關作業，原則上就是不兼做其他事情，在實務上，除非你們編制比較充裕，不然在實務上可以達成的機關，有一定比例，當然我們會建議你們在填實施情形的時候如實填出來，因為人事總處也會來跟我們調各機關的專職人力到位情形，之前就我們跟他們的協調，他們第 1 個說法也是從機關裡面的員額先去做調撥，真的機關內的員額沒辦法了，再找他們協調，他們的說法大概是這樣，所以一定要先從機關內部先處理一遍。我知道有些機關會說他有一些壓力，所以實施情形都會填符合，可是你們要想一下，你們填符合，我們也這樣報給人總，當所有機關都符合的情況下，自然就不會是問題，我還是要強調大家要如實填寫，我們去稽核也遇過填符合，我們透過稽核來確認，你可以看到他們就 4 個資訊人員，又說 2 個是專職，也就是這樣可能性不太高，我們還是會去寫改善建議，我們還是希望去把這件事情凸顯出來，有時候是資訊科長說他是資安專職人力，因為他是資訊科不是資安科，所以資訊科長就不可能是資安專職，我們就會去把它點出來，有些是內部作業的原因，就必須透過外部稽核力量把這個事情凸顯出來，現在我們可以做的是至少忠實呈現，在數據上有 1 個比較明確的資料去呈現，這樣我們會有一些可以處理的作法，這邊要麻煩，我們知道大家

其實可以很順利達成這個目標的是很幸運，可能他的主管很支持，可是如果沒有也先不要灰心，至少我們先把它呈現出來我再做後續努力。

你剛剛講的計畫型，應該是不算，如果你們人事單位有疑義，是不是要問一下人總，「職員」這個詞也是人事總處給我的，以前我們也都以為叫「正式人員」，他們說正式的名詞叫「職員」，大概就先這樣，謝謝。

財政部高雄國稅局：

有 2 個問題請教，因為修法後必須在 1 年內導入 VANS、2 年內導入資安防護系統，假設說現在預算編列方式，當然財政部會要求我們以前一年度的 80%去編列今年度的預算，所以等於我們的預算是限縮在 1 個範圍內，又要做這2項系統的話，這種軟體的導入，如果以我們國稅局2,000部PC的規模來看，預算應該是數以百萬計，所以這個對我們導入來講是有點困難，是不是行政院資通安全處這邊可以為大家爭取預算，例如前瞻預算這種特別的預算來因應，以上報告。

主席林春吟高級分析師：

有關前瞻預算的部分，目前對到中央部會，我們是有幾件計畫在協助他們做推動，不過比較不是推機關的內部作業，至於經費他們怎麼處理還要再看。

有關EDR的部分，如果你們看共契上的價格一套一套買，如果你套數不多或許可以，如果規模大的話，目前我們有問到有一些機關是統籌，有點像是用區域型的共契去採購，這樣價錢跟共契比是有落差的，大家可以考慮一下。再來是，EDR 是需要經費的，所以我們建議大家先拿這條去編列相關經費，然後在採購策略上做一些處理，再來評估一下機關內部需要部署 EDR 的範圍，看你可以爭取到多少資源，優先要佈置的是哪幾塊。

財政部高雄國稅局：

這個 EDR 的佈建是沒限制範圍嗎？

主席林春吟高級分析師：

原則上 PC 與主機是你整個考量的範圍，我們目前是考量到大家可能沒辦法一下子取得這麼多資源，或者你們機關內的環境是單純的，有些機關內部用戶端是制式的，或是有隔離措施。

財政部高雄國稅局：

這個導入的話，我認為沒有全機關導入，70%就會有破口，所以 EDR

要導入應該是全機關導入才會有效果，但是全機關導入如果以千台 PC 與伺服器的規模來講的話，我們有跟廠商詢問過，再怎麼便宜也要數百萬，所以我們每年的資訊預算已經被限縮了，這個對我們來講其實是非常困難的，所以行政院資通安全處是否可以去爭取特別預算，或者是說行文各部會，如果要做這項業務的預算是否可以先行預支，不然其實大家都違法了。

主席林春吟高級分析師：

原則上，每一個領域都會說他的業務非常重要，大家都會想要去爭取資源，雖然我們是資安處，但是不是妥適跟大家講你錢一定要優先撥到這邊，那個妥適性有待斟酌，我現在只能跟您大概分享一下其他機關作法，您的看法是全部，也有機關曾經公開跟大家講，他覺得他機關只要佈建 PC，他覺得他們主機環境都很單純，那個會落到每個機關內部評估不太一樣，沒有標準答案，再來是可以爭取到完整的資源也很好，但是如果沒有，就要為有多少資源如何花在刀口上。

財政部高雄國稅局：

意思是我爭取到有限的資源，再加上我內部評估我要佈建的範圍，這樣我就有符合法律規定了嗎？

主席林春吟高級分析師：

先佈建，目前並沒有把它框死說一定要做到什麼程度，目前我們有個資安健診那樣的規範，目前先這樣，這個規定下去真的跟經費有關係，初期至少大家先走，因為有些機關已經先佈建了，近期發現防毒軟體那邊可以做到一些防護，其實比例下降了，反而 EDR 這邊可能可以比較早期或主動一點先抓到一些可疑的東西，所以才會把 A、B 級框列進去，而且我們也先框列在公務機關。

高等法院高雄分院：

長官好，我在這邊建議，有關資安專責人員，我認為沒有安全，其他的資訊都是白費，我的重點是，像我今年在辦駐點合約的時候，就把廠商要有資安專責人員的證照納入，為的是我怕我們的人沒考過，還好我們 2 個人都過了。總而言之，我們是否可以把資安專責人員不要限定，因為受限行政院總員額法，這個要突破，可能這十年來也很難，但是我認為我們不要把他限定一定要正式人員來擔任資安專責人員，我們如果把它開放像

我這樣，我為什麼會怕我今年沒考過，我明年沒資安專責人員可以用，我就要廠商要有資安專業證照，雖然我會被納入缺點，但對我機關一定有安全，所以我建議可以把那條改成可以用約聘雇或是委外人員擔任資安專責人員，這樣未來也不用考慮到總員額法，由各機關的經費自行處理，報告完畢。

主席林春吟高級分析師：

謝謝，為什麼我們資安專職人員希望扣在機關的正式人員，主要是資安人員原則上會碰到一些機敏的東西，忠誠也是一個議題，他其實要考量的事情比較多，像我們資安處每個進來的人都要被查核，甚至是被限制出境，在資安那邊的議題比較機敏一點，所以我們會把它框在正式人員這邊，希望能朝這方向，讓整個國家基本的資安能量慢慢累積建立起來。因為資安人力到處都缺，全世界、公部門、私部門都缺，像我們技服中心每個月都會被挖走幾個人，所以我們還是希望大家在正式人員那邊，儘量運用一些機關資源培養正式人員，有些機關會說我培養他後他就跑了，可是如果他如果持續在公部門，我們就把心放大一點，他還是我們整個國家的資安基礎能量。

剛才那樣去做，就非常有風險管控概念，先讓你的廠商取得證照，至少在符合證照那邊比較沒議題，很好的是機關同仁也拿到證照了，機關同仁如果你配置了，他就是 1 個資安專職人力，至於他有沒有拿到證照也不會有損資安專職人力的身分，你剛剛給的建議可能可以提供給其他機關，萬一同仁不管是還沒到位或是證書還沒拿到，那也是 1 個作法。我們可以先讓你的委外廠商處理這件事情，可是要讓他把相關技能傳承到機關內部，讓機關這邊是可以自己處理的，因為有很多攻擊、威脅、入侵從我們供應商那邊來也蠻多的，之前有案例是供應商，他可能有一些研發團隊在對岸，後來被發現了，那其實都會有一些議題，他們畢竟有他們的考量，變成我們現在在選擇委任商也要特別小心注意。

我們先繼續進行下去，謝謝。

柯旻圻助理設計師：

好，我們現在來討論修法部分，首先看母法，我們這次修法比較大的重點改的是幾個名詞定義，公法人還有財團法人那塊，還有公所、代表會實施情形提報給上級政府，主要就是這幾點，有關母法，資通安全管理法

修法的部分，有機關想要提供建議或是發問的嗎？（無）

沒有的話，我們進入下一個，再來第 2 個，資通安全管理法的施行細則，這邊主要改的是剛剛公所、代表會那邊，是對到上級政府，另 1 個是實施情形提報方式，這邊具體寫實施情形提報方式由主管機關統一訂定，也就是用行政院資通安全會報管考系統來做提報作業，有關施行細則的部分，有人有建議或問題的嗎？（無）

再來就是可能會有比較多機關有問題的責任等級分級辦法，這邊改了比較多的是，第 1 個，C 級機關的定義，原本是維運或自行或委外開發的資通系統是 C 級，可是有些不是自行開發或委外開發的就不會被算成 C 級，這個是有問題的，所以我們把它明確寫清楚，針對有一些高防護需求的套裝型資通訊系統列為 C 級，這個是 1 個。再來是應辦事項的部分，主要增加 2 大項，1 個是 VANS，這個 A、B、C 級公務機關與關鍵基礎設施提供者，第 2 個是 EDR 端點防護偵測機制，這個是要 A、B 級公務機關導入，再來是附表 10 讓大家明確知道要做哪些應辦事項，有一些文字的調修，這邊我就不一一介紹，有關分級辦法修法的部分，有機關有問題或建議嗎？

中油煉製事業部：

分級中 A 級的部分提到的是提供全國性服務，以中油來講，好幾個事業部都是全國性服務，比如說潤滑油、汽車用機油、工業用機油也都是全國性的，印象中潤滑油現在是在 C 級，跟 A 級有很大的差異。再舉例如液化石油氣，就是家裡用的瓦斯也是全國性的，甚至柏油、去漬油的業務也是全國性的，看起來就會符合全國性服務，因為我們組織架構就是事業部本身就會有各個加油站就是真的營業單位，但是營業單位上也會有業務管理單位就是事業部本身，可能是直接或間接，條文中沒有講到直接或間接怎麼區分或是有這塊相關的問題，大概有這 2 個部分比較需要去釐清。

主席林春吟高級分析師：

你們中油被納管的身分是關鍵基礎設施提供者？

中油煉製事業部：

有直接去定義哪些單位，譬如說天然氣、煉製這邊 2 個煉油廠，這個就有直接訂的，我剛剛講的不是關鍵基礎設施。

主席林春吟高級分析師：

那就是公營事業被納管。

中油煉製事業部：

對，因為中油是 1 個公營事業，特定非公務機關，A 級他的業務是符合的，就是我剛剛舉的例子。

主席林春吟高級分析師：

原則上我們就是 A 級納管你們中油。

中油煉製事業部：

就主管機關來講，中油這個事業單位當然是 A 級，他提供好幾樣民生、工業服務當然就是 A 級，但是在我們自己本身單位內定義裡面又會不同。

主席林春吟高級分析師：

原則上我們是以機關來納管，你現在講的應該是你們機關裡面每個單位負責的不一樣，一般我們是對到一般行政機關，當那個機關被納管成什麼等級之後，原則上法遵的要求對到是整個機關，當然機關裡面每個單位可能會因為重要性不同，你們內部怎麼要求是變成在機關裡面的；就是假設你們中油是 A 級，被要求的事情是整個機關來做提報，所以最少要有 4 個資安專職人力，但可能你們部門很多，兩三個部門都很重要，所以你們資安專職人力的配置會比法令要求 4 個人更高，可是在法上面來講，在法遵的符合性上，只要你們總數至少 4 個，原則上在法遵符合性上就沒議題。可是在實務上可能你們需要更多，就像你剛剛講的全國性那邊，因為我們看的是資通系統，我們在意的是那套系統是誰建的，如果通通統一由你們建、維運，那整個資安維護的責任就會在你們家，雖然他們是使用者，或者是說你們也有建你們重要的，他也有建他們重要的，那你在盤資通訊系統的時候就要把他那個盤進來，要看你們公司裡面誰來做統籌。

我現在舉一般機關例子，某個部會可能會去統籌資安的相關作業，他會去盤他們自己單位的資通系統，但人事單位自己做的系統要盤進來、秘書單位做的公文系統也要盤進來，就是盤系統的時候，統籌(資訊)單位會把它通通盤進來，大家來擬定哪些是核心系統，都是以機關為單位，釐清出哪些是核心資通系統後，法遵上就有要求，類似要導入 ISMS、取得驗證、滲透測試、掃描等等作業，再往下做下去。原則上管制單位是以機關來看，機關裡面會有幾個單位，那個就是在機關內部作業，法通常不會再

把單位從機關內抽出來，法上面是有這個彈性，可是一般來講不太會抽出來，如果有必要討論再抽出來定的話，那就再做細部討論，我有回答到你的問題嗎？

中油煉製事業部：

謝謝，請問一下第 3 條，剛剛講師講的核心業務與資通系統的關聯性有需要釐清嗎？

主席林春吟高級分析師：

原則上，我們會請大家先盤點你的資通系統，盤出來之後再去找出你的核心資通系統，目前法上的針對核心資通系統有 2 個定義，滿足 1 個就算，1 個是支援你的核心業務，他只要是你的核心業務必要用到的資通系統就是你的核心資通系統。另外你盤出來的這些資通系統，你要對這些系統的防護去衡量普、中、高，當它是屬於高防護的資通系統也會是你的核心資通系統；另有一些細節，像衡量普、中、高，在法的附表 9 有規則，可是因為要讓大家都適用，所以他是用比較模糊的字眼，可能就是嚴重、輕微，落到機關，你們要把它量化，有些機關是用它可以容忍停止服務 4 個小時或 8 個小時，用這個來衡量重要性，也有機關是用系統內含有個資的筆數，類似 10 萬筆以上或是以下的去衡量，落到機關的時候就要用客觀、量化的方式去衡量普、中、高。當他是高防護等級的話，就會是你的核心資通訊系統，另外看你們公司或機關的核心業務職掌是什麼，支援你核心業務職掌的資通訊系統就是核心資通系統，如果有些機關的業務好像也還好，那它就會把公文系統放進去，這個不一定，要看每個機關自己衡量標準，只要定義核心資通系統後，就會有對應的法遵應辦事項，看的範圍是以機關為單位，機關裡面的各個單位，由你們內部透過內部資安推動小組去統合起來做推動作業，謝謝。

台電核能營業處：

剛有提到事業機構的部分，因為台電在全國各地有好幾十個單位，剛剛提到的分級是針對台電定 1 個還是各個不同單位個別去定義？因為每個單位的風險等級都不相同，所以想請問這點。

柯旻圻助理設計師：

這個由我來回答，一開始資安法施行的時候，剛剛也有講到我們是對這個機關，就是台電 1 個，應該是 A 級以公營事業納管，可是後來我們資

安法裡面有 1 個關鍵基礎設施提供者，這個是今年 6 月中我們陸續去做核定，因為台電有很多電廠，個別的廠房被指定為關鍵基礎設施提供者，個別都有責任等級，只是他們不是以公營事業納管，是以關鍵基礎設施提供者的身分來納管，這個等級的分法主要是這樣去看，台電的公營事業是 1 個 A 級沒錯，只是其他電廠因為是關鍵基礎設施提供者的關係，這樣有回答到你的問題嗎？

主席林春吟高級分析師：

這表示如果你的電廠被拉出來，以關鍵基礎設施提供者納管的話，那就變成 1 個納管的等級在那邊，那就要去做應辦事項，因為關鍵基礎設施提供者要求要做的事情比公營事業多，所以又單獨被抽出來變成關鍵基礎設施提供者，那個被拉成 CI 提供者，就要用 CI 提供者那邊的等級去做相關法遵事項。如果整個台電公司是以公營事業納管，整個台電公司就是抽掉那幾個（CI 提供者）之後，整個台電公司以公營事業納管，整個台電公司就是處理公營事業那塊，這是比較不太一樣的，因為你們是有幾個特別重要的電廠，被提報出來變成 CI 提供者。

台電核能營業處：

那在各個單位的部分，等級都是一樣的嗎？

主席林春吟高級分析師：

就是跟著你那個機關，除非他特別被拉出來，不然你其他單位就是跟你的機關是一塊去看的。

台電核能營業處：

再來是證照數量的部分是以單位去分？還是？

主席林春吟高級分析師：

台電是以公營事業被納管，那你裡面可能 2 個單位又被拉出來當成 CI 提供者被納管，是這樣嗎？那你每一 1 個被納管的 CI 提供者，就要依據他的等級去做，應該是這樣子。

柯旻圻助理設計師：

簡單講，就是台電很大，他有很多廠房在台灣各地區，這些廠房有些可能是 A、有些可能是 B、有些可能是 C，那這些廠房他依法就是做 C 級特定非公務機關-關鍵基礎設施提供者的事情，如果他是 1 個 C 級的廠房被認定的話，那個廠房就要有 1 個資安專責人員。除了這些被獨立核定等級

的廠區、廠房、場館，這些之外都算是台電總公司，台電假設是 A 級的話，因為整個就 4 個，你們總公司就用 4 個去看，看你們總公司哪 4 個人去看，就看你們這 10 幾 20 個廠房，有哪一些是 CI 提供者，他們是哪一級，那些廠房就是需要對應的資安專責人員，除此之外，整個台電就算是一個大公司來看他的人數。

台電核能營業處：

你的意思是整個公司由 4 個人來負責資安業務嗎？

主席林春吟高級分析師：

不是，就法遵上來講，如果你們是 A 級，法的要求是至少配置 4 個資安專責人力，你們可以多配置沒有問題，因為有些機關管的範圍很大、系統很多，所以他們可以多配，可是就法遵上來講，台電公司至少 4 個，在稽核或檢視的時候，原則上那條法遵事項是符合，並不表示你們只能有 4 個，法是最低的要求，你們家要先把 CI 提供者抽出來，那些照他被核的等級去做，剩下的全部歸在「台電」這個機關去納管，我們就是以台電當單位來看各個法遵配合辦理事項，至於台電這些裡面內部單位，就是透過你們資安推動組織去推動大家的資安，不是只有資訊單位做，業務單位也要做。

台電核能營業處：

另外「專責」與「專職」的部分，在我們也是有一些困擾，因為資安的業務量還蠻多的，現在公司內部針對這塊，其實他不是「專職」是「兼任」，是由資訊人員兼任這塊業務，這個在法上面有沒有明確定義，就是在事業機構的部分，也是一定要專任不能兼任。

主席林春吟高級分析師：

因為法是具有強制力的規定，所以在公部門，我們要求比較嚴格是專職，在特定非公務機關我們放寬叫專責，他的確可以兼辦其他事情，可是你們要去看你們資安作業，當你們資安作業已經很多，當這些人做資安作業都做不完了，怎麼可能還去兼做其他的事情，應該要以這個角度看這個事情。

像金管會，他對到銀行體系，他規定銀行要有資安專責單位出來，也就是說不是只做到法的要求，因為法是最低要求，我們要去規範所有人，所以我們不能拉到高標，這樣大家沒辦法做，可是至少你要做到這個程

度，你可以往上，因為每個機關不一樣，所以法其實是在低標，你一定要符合這個門檻，但不表示你只能做這個門檻，要掌握這個精神，謝謝。

柯旻圻助理設計師：

有關資安責任等級辦法修法項目，還有機關有問題要詢問的嗎？（無）

進到下一個子法，通報應變辦法，這邊我們主要修的是 2 個地方，第 1 個是有關聯性資安事件，一定時間內發生多起資安事件，這樣的話可以由上級機關額外通報 1 個資安事件來做統籌規劃、處理。第 2 個是事件發生的時候，中間的損害控制、復原作業，上級機關可以請發生事件的機關做一些調整、修正、說明。有關這 2 點修法部分，有沒有機關有問題想要詢問？（無）

下一個是特定非公務機關的稽核辦法，這邊主要修改的是 OT 的稽核，因為特定非公務機關會涉及到很多工控系統，工控系統的稽核與 IT 系統稽核不太一樣，需要由那個領域的專家來協助稽核作業，所以在人數與小組組成限制上，我們降低範圍限制。針對特定非公務機關的稽核，有機關有問題嗎？（無）

再來是情資分享，資通安全情資分享辦法，這個很單純，主要修的是鼓勵特定非公務機關，中央目的事業主管機關可以適時獎勵，把它明定，讓獎勵有所依據。情資分享的部分，有機關有問題嗎？（無）

最後是獎懲辦法，公務機關所屬人員資通安全作業事項獎懲辦法，主要修的是當未符法遵情節重大，在評估懲處的時候，將主管與上級機關也一併納為檢視範圍。有關獎懲辦法的部分，有機關有問題嗎？（無）

主席林春吟高級分析師：

沒關係，如果大家就簡報、母法、子法沒有要在現場用發言的方式提供我們意見的話，你們手上有 1 張紙也可以提供我們書面意見，待會離開的時候提供給我們工作人員，我們會回收，後續我們會去檢視，看看有沒有哪一些需要釐清的，或者會後要再做細部交流也可以，如果沒問題的話，今天說明會到這邊，謝謝大家。