「資通安全管理法子法草案分區座談會」第三場次
會議紀錄

時間：中華民國 107 年 8 月 8 日（星期三）下午 2 時 30 分

地點：臺大醫院國際會議中心 202 會議室

【記錄開始】

主席徐嘉臨副處長：

各位大家午安，今天非常高興各位來參加這一次資通安全管理法第三階段的座談會。大概從去年到現在，我們辦了兩個梯次，也徵集一些意見，這次是把前兩次徵集意見裡面作了子法版本的調整，現在跟各位作一個請教，原則上這個版本我們已經在 7 月作了預告，所以在網站上大家可以看到這個版本，也可以提出一些意見討論，今天只是透過實體的方式再請各位看一下現在的版本有沒有提出建議的地方。

今天議程會由同仁先就資通安全管理法後來調整版本跟各位作一個說明，接下來開放討論，討論的方式就是每個子法逐一討論，今天發言有作逐字稿，逐字稿之後都會在網路上公開，這個部分請各位注意一下，等一下我們有發言規則，同仁在簡報後會把發言規則跟各位說明，如果各位對今天議程沒有意見，我請同仁就簡報作一個說明。

王詠萱分析師：(略)

主席徐嘉臨副處長：

接下來開放各位進行討論，發言規則等一下請同事說明，今天的簡報也會放在網站上，在行政院資通安全會報有一個資安管理法的專區，讓各位下載，所以各位可以不用拍照。

王詠萱分析師：

今天的發言規則原則上會依據我報告的順序六個子法逐一進行討論，其順序如下：「資通安全管理法施行細則」、「資通安全責任等級分級辦法」、「資通安全事件通報應變辦法」、「特定非公務機關資通安全維護計畫實施情形稽核辦法」、「資通安全情資分享辦法」、「公務機關所屬人員資通安全事項獎懲辦法」。

討論各子法草案之發言規則：請各與會單位推派一人代表發言，發言次數以一次為原則、每次 2 分鐘為限，發言單位如尚有其他意見，請以書

面方式補充提供主辦單位會後處理，書面意見提案單由主辦單位提供。主辦單位原則於每 3 位提問後，進行回應說明，每次回應時間 4 分鐘。回應重點以就子法條文文意釐清事項進行說明為主。會議紀錄將於會後公布於國家資通安全會報網站，今天的簡報內容也會放在國家資通安全會報網站，以上報告。

主席徐嘉臨副處長：

謝謝，再提醒一下各位，我們今天實體會議時間很有限，各位如果今天會議之後還有一些問題或建議的話，請到國發會的公共政策網路平臺（JOIN 平臺），就你們的建議提出來，在那個平臺上我們也都會回應。

我請同仁先就坐，接下來由我來主持，會兩位同仁先就各位的問題先作回答，不夠的部分我會補充。右手邊這位王詠萱分析師，是這次資安管理法的承辦人；左邊的部分是賴妍帆分析師，主要針對關鍵基礎設施或通報應變的部分來負責，等一下的問題我會請這兩位先回答，如果需要補充我會再補充。

現在先針對第一個子法「資通安全管理法施行細則」請各位提出建議。

臺灣集中保管結算所：

各位好，針對施行細則第 6 條第 1 項第 7 款，資通安全維護計畫應包括資通安全風險評估，我們參考一下說明欄一、（五），最後有提到風險評估的範圍包含第 6 款所盤點之資訊、資通訊系統及相關資產。我們依照現行的國際標準，像 ISO27001、ISO9001、ISO31000 等等，風險管理是依照內外部議題以及利害關係人的期望跟要求，已經不再強調以資產為出發點，所以上述第 6 條說明欄一、（五）的內容，是否有跟國際趨勢不一致的疑慮？以上。

主席徐嘉臨副處長：

有沒有第二位要發言？

財團法人金融消費評議中心：

依照細則草案第 4 條第 1 項第 5 款的規定，受託業務包含客製化資通系統開發者，受託者應該提供第三方安全性檢測證明。我們想請教一下，這邊所稱的「開發」，是指全新系統的開發建置？還是系統建置後的功能增修？「第三方」是指使用第三方工具產出之檢測證明？還是必須要由第

三方單位提出檢測證明？如果是由第三方單位提出檢測證明的話，因為我們的資通系統有時候因為業務需求不同，可能規模性沒那麼大，如果要由第三方單位提出檢測證明的話，動輒是數 10 萬以上起跳，這樣的費用成本一定是轉嫁到委託單位自行吸收，造成我們使用檢測的費用會比我們需求增修的費用還高很多，像這種情況我們實際上要怎麼克服這樣的問題？以上，謝謝。

主席徐嘉臨副處長：

有第三位要發言的嗎？

國家衛生研究院：

第 4 條第 1 款受託者應該具備完善的資通安全管理措施，還要通過第三方驗證，以及第 2 款。像我們雖然是財團法人，但是我們所有的委外都是公開招標，不知道參與的廠商投標的時候是不是具有這些完善的資通安全管理措施或者有第三方面驗證？那個在現場是沒有辦法確認的，所以這個在受託前如何去證明是有這些完善的措施好像有點困難。或者他一定要有驗證的證明才可以嗎？因為不是所有的業者都有資通安全的驗證，我們要怎麼去確認他來投標的時候是具有資通安全管理完善的措施？畢竟投標只要他的規格符合就可以來投標。

主席徐嘉臨副處長：

這三個問題先請王詠萱分析師就可以回答的部分先回答。

王詠萱分析師：

首先針對金融消費評議中心回應，我們第 4 條第 1 項第 5 款，有關於客製化資訊系統的開發者，這邊的「開發」不限於建置或增修，只要委託他開發的話，他就必須要提供第三方安全檢測證明。這邊要求第三方的原因主要是公信力跟客觀，如果是廠商自行檢測的話，可能會懷疑它的公信力夠不夠客觀。所以這邊是增加第三方安全檢測，原則上這是要由第三方單位提出的。考慮到成本會增加的話，後續我們可能還會看看用什麼辦法讓這個產業能夠提供更優惠的價格、更促進這樣的產業發展，例如利用共契的方式。

第二個，有關於國衛院針對第 4 第 1、2 款受託者應該具備的條件。雖然是公開招標，如果評選標或者最低標，都是可以設定一些廠商的條件，如果是評選標的話，在評分項目裡面，受託者的資通安全管理措施、

是否具有足夠的資通安全證照，當成是一個評定的標準。在投資的時候，如果是要求用評選標的話，其實你是可以去選哪一個廠商比較好；如果是最低標的話，廠商的資格那邊也是可以作要求的。第 1 項第 1 款是否一定要通過第三方驗證？條文上是「或」，只要是具有資通安全管理措施或是第三方驗證，但第三方驗證只是證明他具備有妥善資通安全管理措施的一個條件而已，所以我們不會要求一定要有第三方驗證，只要他有足夠的管理措施，我們原則上都是可以接受的。

針對集中保管結算所有關 ISO27001 風險評鑑的趨勢，您說的沒有錯，風險評鑑我們的確要識別內部、外部的議題還有一些關係人的意見，主要還是會針對每一個資訊系統面對內部的脆弱性跟風險不一樣，最後我們要求在資訊系統或機關有一些內部的控制措施，所以在我們的說明裡面，針對你所盤點到的資產跟相關系統，要對每一個威脅跟脆弱性作一些盤點，盤點可能考量的問題就是您所提到的跟內外部議題跟關係人的意見，所以我覺得跟我們的標準其實是沒有違背的。

主席徐嘉臨副處長：

請問各位針對剛剛三個問題還有什麼不清楚的地方還需要詢問的嗎？我再補充一下第三個問題，選擇受託者應注意的事項，其實這些事項就是希望在未來擬定需求說明書或針對建議書徵求文件的時候，就應該把你的需求放進去，譬如應具備完備的資通安全管理措施，假設今天是一個系統開發的案子，可能就要求你的委外廠商在做任何的系統開發過程中，從他維護開發的環境是否安全、有沒有跟他們組織內部的環境混合在一起、或者未來的開發程式上版的過程中有沒有按照一定的安全標準？類似這種東西的需求，就應該反映在需求說明書上，以利未來徵選廠商的時候，他可以依據這樣的需求滿足你的需求，你當然可以在這麼多的廠商裡面去選擇你要的。所以寫這個目的只是希望提供各位未來在作採購需求說明書的時候，能夠把這些議題放進去，並針對各種不同資通安全委外的類型去作必要的安全規範，目的是這樣子。

司法院資訊處：

也是第 9 條的問題，現在我們在辦理資訊委外，大家都用第 22 條第 1 項第 9 款，我記得之前行政院唐政委他們在要求各機關有關 Open Data 跟 API 的部分，有跟公共工程委員會協調過，在他們公版的契約上有作一些

調整，增加 Open Data 或 API 的部分增加一些條款。所以相同的道理，在資通安全管理辦法及相關細則施行的時候，是不是請貴院跟公共工程委員會協調一下，提供一些公版給一些機關辦理採購的時候，這些可能比較有統一的一致性，以避免大家定一些契約條款無法落實，甚至到驗收的時候無法驗收，因為兼辦單位可能會要求，標準怎麼定出來？驗收標準是什麼？到時候可能會有很多的爭議，以上，謝謝。

主席徐嘉臨副處長：

你說的是施行細則第幾條？

司法院資訊處：

第 4 條。

主席徐嘉臨副處長：

原則上你是建議這些東西可以反映在工程會公版的採購契約上。接下來有沒有第二個問題？

中華電信：

有關於施行細則第 7 條這次有提到整個核心業務的定義，其中二點說到，特定非公務機關維運或者是提供關鍵基礎設施所必要之業務或該機關之主要服務或功能。這個部分我們建議把「該機關之主要服務功能」調整成「或中央目的事業主管機關監理列管之業務」，因為這個部分比較會是我們的中央目的事業主管機關關心的一些核心業務，是不是能夠把這樣的字眼調整，讓我們特定非公務機關也比較容易遵循？以上建議。

主席徐嘉臨副處長：

第三個問題？

中華顧問：

請問一下第 2 條所謂的「特定非公務機關」，是不是適用於特定非公務機關的子公司？因為有時候會成立子公司或孫公司，在母公司特定非公務機關所有資安相對的要求是不是及於子公司跟孫公司？

第二個，第 4 條，受託者辦理受託業務的時候，相關程序及環境是否具備完善的資通安全？今天假如我們機關是委外辦理，但是他在執行這個計畫的時候，譬如代操作，但是代操作的地點是在業者這個地方，在這種情況之下，那個承包商是自己的公司要符合這個事業這個要求，還是在業務執行的地點要符合這個要求就可以了？

主席徐嘉臨副處長：

剛剛提到第 4 條要有完備安全措施這個嗎？

中華顧問：

對，「受託者辦理受託業務相關程序及環境」，這個環境是指他業務執行地點只要符合就好？還是受託者他們公司也要符合這個要求？

主席徐嘉臨副處長：

這三個問題先請王詠萱分析師先回答。

王詠萱分析師：

就公版契約的部分，之後我們會跟公共工程委員協調，看是不是有一些共同項目可以修正，這個我們會處理。

第二個，有關於核心業務的定義，是否可以改成中央目的事業主管機關監理的業務？我們現在條文第 7 條是寫針對特定非公務機關是該機關的主要服務或功能，改成中央目的事業主管機關監理的業務，這邊會有一個小小的問題，基本上有一些特定非公務機關，他的中央目的事業主管機關可能不是那麼明確，譬如像地方的公營事業，本身就是依照主要服務的功能去定中央目的事業主管機關是誰，所以這樣會有一個先後的問題，這邊有點沒有辦法這樣修改。如果只是納管中央目的事業主管機關監理的業務，一個機關可能有很多業務，可能有一個主要的業務是由中央目的事業主管機關監管的，可是他有另外一部分是業務是其他中央目的事業主管機關，可是可能不是他主要的，舉例來說，譬如交通部的郵局，郵政的業務可能是歸交通部管，交通部是他中央目的事業主管機關，可是他的儲匯的業務可能在金管會，如果這邊這樣定的話，可能會不夠全面。所以我們原則上還是以機關的主要服務或功能，中央目的事業主管機關監管他哪一份業務，可能只是他主要服務或功能一個決定或是參考的項目。

針對中華顧問這個問題，特定非公務機關的子公司，所謂特定非公務機關子公司是指財團法人捐助的子公司嗎？如果是財團法人捐助的子公司，可能要看一下是不是符合公營事業的定義，如果不是屬於公營事業的定義，原則上就不會是本法所納管的特定非公務機關，如果是公營事業在投資其他的子公司，一樣要看符不符合本法公營事業的定義，我們會決定他是不是本法定義的特定非公務機關。

第 4 條有關委外辦理的部分，受託者辦理受託業務相關的程序跟環

境，所以你是問機關所在的環境還是操作的環境？主要還是要看跟他受託業務相關的程序跟環境在哪裡，譬如機關有幾個辦公地點，可是有些辦公地點完全跟受託業務都沒有關係的話，可能就不是在子法規範的程序跟環境裡面。所以還是要回去看他受託業務到底牽涉到哪一些部分，去決定他是哪一些部分要具備完善的資通安全管理措施，以上簡單回答。

主席徐嘉臨副處長：

原則上剛剛的問題，以你委外的範圍為主，其他公司很多業務可能不是你所受託的對象，你可能只是請他開發一個系統，但是這個公司還做其他的製造或者是其他的整合商的服務，原則上那一塊是不管的，譬如你委託他是開發系統，只要確保他的開發環境或者其他安全的設計開發程式等等是符合你的安全措施就可以了。假設你今天的操作系統就是在某個區域，你關心的就是那個區域，其他的區域不是你的業務範圍，當然不用特別去管他，但是要小心，他的區域有沒有作區隔？病毒會不會從他另外一個區域影響到你這邊？這是你要去關心的。

遠傳電信：

針對第 6 條資通安全維護計畫第 4 項，專責人力及經費的配置，這個經費的部分我們之前也有反映過，因為經費每年依照不同的狀況會有不同的編列，實際上運用的情況也會依照每一個時間還有機關內部自己的資源統籌編列跟運用。所以這個部分我們之前有建議，希望不要列入，免得會有失偏頗，因為可能在建置的當年度有大筆的投資，可是在後續的強化或補強，那個金額又會變，可能沒有像建置金額那麼大，如果這個部分列去的時候，不曉得會不會對這樣的計畫或這樣的數字反而會有質疑？實際上在非公務機關裡，它的資源運用是會有很多種考量的，所以在經費的部分我們是建議刪除。

主席徐嘉臨副處長：

有沒有第二個問題？有關剛剛遠傳建議經費的這件事情，我們在思考一下如何去呈現這一塊，因為對於公務機關的部分，我們會希望在經費上知道怎麼配置，大概是配置在哪裡，特定非公務機關的部分，如果有剛剛的顧慮，我們可以思考一下怎麼去作一些調整，因為資通安全維護計畫我們未來會提供範本。你剛剛提到刪除這一塊，我們會帶回去思考一下應該怎麼呈現，因為對於特定非公務機關，畢竟你們還是屬於私部門，主要目

的是希望你們在作資通安全建置的時候，應該要注意到資通安全這一塊、投入一定的資源。至於我們知不知道、或者是你們中央目的事業主管機關如何看你們投入的資源合不合理、或是應該投入在什麼地方、有沒有投在對的地方？這個可能是在資通安全裡面去呈現的，不是要呈現細部的數字，但是怎麼呈現，我們再跟中央目的事業主管機關討論一下。接下來還有沒有其他的問題？

中華經濟研究院：

因為我剛剛聽到簡報，在訂定公務機關跟特定非公務機關的區別，之前你們通知我們參加會議的時候，我們幾乎都參加特定非公務機關，我們是這樣認為，因為我們是財團法人。可是剛剛講到母法在區分公務機關跟特定非公務機關的時候，依據是否政府捐助成立的財團法人，如果照這樣的解釋的話，我們中華經濟研究院就歸為公務機關，是這樣解釋嗎？

主席徐嘉臨副處長：

有沒有第二個問題？

親民黨團：

我想請問一下施行細則第 4 條，前面講到委外要注意哪些事情，這個牽涉到一個問題，如果是行政機關或公營事業的時候，很容易有一個同業規範，但是第 4 條是根據母法第 9 條來，這牽涉到一個問題，請問特定非公務機關也要依循這個規範嗎？你們為了行政機關或國營事業打造一個公版的東西，請問是屬於民間的非特定公務機關也要遵守嗎？

第二個，上禮拜我已經有問過，但是並沒有問很清楚，第 4 條後面，要講它是忠誠考核也好、保防考核也好，請問你們統一的公版要產生嗎？還是它有一個統一的 SOP？可以讓要去做這件事情的人去做這個事情嗎？謝謝。

主席徐嘉臨副處長：

請王詠萱分析師先回答。

王詠萱分析師：

就中華經濟研究院的問題，我們的公務機關在母法裡面有特別說明，是指依法行使公權力之中央或地方機構或公法人，不包括軍事跟情報機關，這邊我們針對公務機關應該是依照組織法設立的中央或地方機構才會是公務機關，原則上政府捐助的財團法人應該是屬於特定非公務機關。之

前邀請你們開會是參加哪一個場次，不會是決定什麼機關的因素，還是要回到母法的定義來看。

針對委外應注意的問題，承如您所說的，我們委外應注意事項是根據母法第 9 條這邊的規範，公務機關或特定非公務機關於本法適用範圍內委外辦理資通訊系統建置、維運或資通服務的提供，應該考量受託者的專業能力與經驗、委外項目的性質跟資通安全需求，選任適當的受託者，並且監督他資通安全維護情形。所以我們在細則第 4 條有定義，包括委外之前如何選任，跟委外之後如何監督的事項，這個事項不管是公務機關或特定非公務機關都需要適用的。

如果針對特定非公務機關除了我們細則以外，認為還有其他應注意的地方，也是可以另外訂定的，在資通安全維護計畫的項目第 11 款，包括資通安全服務或委外辦理之管理措施，這個也是資通安全維護計畫的一環，如果特定非公務機關覺得第 4 條公開密度不夠的話，在這個維護計畫裡面是可以另外定覺得哪些事項還必須要作為選任的參考或監督的依據，都是可以在這裡另外訂定的，以上。

主席徐嘉臨副處長：

上次有提到適任性，應該是適任性查核嗎？

親民黨團：

我的問題很簡單，其實你們沒有回答我，我可以先回答中華經濟研究院，根據資安法的規定，中華經濟研究院是政府捐助的財團法人，他就是屬於特定非公務機關。

第二個，我覺得你們沒有回答我的問題，你們一定會對公務機關以及國營事項生出一個公版，今天委外要注意什麼事情，不管是法規命令也好、不管是行政規則也好，或者是採購契約也罷，你們總會有一個共通的版本，我的問題很簡單，我就直指核心，請問民間的特定非公務機關要遵守這個東西嗎？還是你們要另外再生一個？

主席徐嘉臨副處長：

依據本法第 9 條，就是要定這個規範。

親民黨團：

母法第 9 條是說要注意這個事情，行政機關要注重的東西跟民間的特定非公務機關的結構本身就不一樣，你認為是同一套標準要民間一律遵守

嗎？我的問題就是這樣。

主席徐嘉臨副處長：

對。

親民黨團：

當然你可以直接搶答，我今天根據行政機關以及國營事業定的公版以後，我希望民間的特定非公務機關也遵守，沒關係，那個就是你的答案，我當然還是可以表達不同意見。

第二個，不管是忠誠考核還是保密防諜，你有沒有一個 SOP？你們要怎麼去做？你們要定一個作業流程，要做的人要怎麼去做這件事情？總是會有一個作業辦法。

主席徐嘉臨副處長：

我針對你的第一個問題，依據母法第 9 條，不管是公務機關或特定非公務機關，它的規範是「於本法範圍內委外之建置系統…應考量受託者之專業經驗」這些東西，所以不管是公務機關或非公務機關，它在委外的時候都要考量，答案是確定的，所以我們也認為他需要定這個規範讓各個機關參考，原則上就是這樣，不管是公務機關或特定非公務機關，這就是我們的看法。

適任性查核的部分，有這麼多要查，這比較是屬於公務機關，因為公務機關才會接觸到國家機密，大的前提是你的受託業務涉及國家機密者，才會執行委外人員的適任性查核，所以這個查核的部分我們後續會告訴機關要怎麼查，我們會有 SOP 出來。針對第一個子法「資通安全管理法施行細則」各位有沒有什麼建議？（無）沒有的話，我就進入下一個。

第二個子法「資通安全責任等級分級辦法」。

海外信用保證基金：

我想問一下，因為我們服務的對象是已經僑居海外的僑民跟臺商，我們所持有的個資數量不多，按照第 4 條是全國性的民眾，第 5 條是區域性或地區性的民眾，我們這個移居海外僑民的個資，是否在這個規範範圍之內？如果有的話，是隱含在第 6 條？因為第 6 條沒有規範全國、也沒有規範地區或區域性，這個不定性的話，是不是隱含在第 6 條裡面的規範？謝謝　。

主席徐嘉臨副處長：

有沒有第二個問題

國家衛生研究院：

我想要問附表一的問題，附表一 A、B 級應辦理事項，有寫在核定等級之後 1 年之內完成資通分級還有控制措施，2 年內要導入相關的標準。像我們財團法人的預算都是前年編列的，即使我們已經有付費，有導入部分的 ISO27001，但是如果要照附表一、附表六的要求，其實在 1 年內要達到，真的有點難度，這個時程好像真的有點趕，因為明年就要開始實施。剛剛在簡報上也有報告，明年就開始實施，等級的部分，也是從明年 1 月等級就要核定嗎？

主席徐嘉臨副處長：

在導入 ISO27001 是初次之後核定的 2 年內。

國家衛生研究院：

如果已經完成導入，其實這個還好，主要前面還要完成那個分級還有控制措施，包含附表六要作的技術面，那邊跟預算跟人力都有關係，其實在核定等級之後 1 年內要完成所有的措施，其實真的有難度，不管是從預算或者是人力，不是每個單位都有這麼充足的人力跟預算，我覺得這個時程對我們而言是有點太趕。

主席徐嘉臨副處長：

所以你講的是附表一跟附表八？

國家衛生研究院：

附表一跟附表六。

主席徐嘉臨副處長：

你講的特別困難應該是附表八。

國家衛生研究院：

我可能是上一版的，附表六有一個資通系統防護基準的分級。我剛剛的問題有相關，在 2 年內要導入核心系統，所以只有核心系統要作這些控制措施嗎？還是全部都要？

主席徐嘉臨副處長：

接下來還有第三個問題嗎？

金管會：

這邊有一個問題，因為我發覺這一次的版本跟比較早期草案的版本有

一個比較大的差異，是在第 4～7 條，原來在第 4 條～第 7 條第 1 項的文字裡面都有提到它的影響程度，比方原來在第 4 條有提到會導致民眾的生命、身體、財產、隱私權的損害、急迫損失而產生全國性影響的才列為 A 級；好像在這一次的版本，這個影響層次的文字已經拿掉，把它搬到第 5 款屬於關鍵基礎設施的文字裡面。

有一個地方我想進一步請教，在第 4 款提到公務機關涉及全國性的能源等事項，這個事項因為公務機關有兩個不同的角色，第一個角色是純粹的公務機關，本身營運重要的核心系統；第二個角色是中央目的事業主管機關，比較多的工作是在行政管理，這邊所謂「事項」的定義是指公務機關本身營運重要的核心系統？有沒有包含中央目的事業主管機關的行政兼管事項？

連帶在後面責任等級的應辦事項裡面，因為整個架構比較偏向本身維運一個重要的核心系統，必須要注意很多資訊安全的防護措施，對於中央目的事業主管機關，如果在前面也要適用的話，其實對很多項目來講，似乎不是見得那麼適用，這點請教。

主席徐嘉臨副處長：

這三個問題請王詠萱分析師回答。

王詠萱分析師：

先回答海外僑民的個資，第 4、5 條提到的是全國性民眾或公務人員資料檔案，或區域性、地區性個人資料。全國性是指出全國大部分人民的資料；區域或地區性是指這個區域或地區性大部分民眾的資料都在你這，只是你的資料來源是全國性或地區性，但是你的資料數量沒有達到全國性或區域性、地區性的話，原則上不在法條文義裡面。如果這邊只是海外僑民的個資，看起來應該不會是第 4 條第 2 款或者第 5 條第 1 款的事宜。至於你是不是適用第 6 條的規定？可能要看看第 4、5 條其他款這些項目有沒有符合的。

海外信用保證基金：

我們只有海外的僑民部分的個資，作身份的認證而已，我們也沒有對外公開網路設 Web 這種服務，如果不在管理範圍之內的話，是不是隱含在第 6 條？或者根本不在管理範圍之內？

主席徐嘉臨副處長：

你們任何的資訊系統都沒有？

海外信託保證基金：

不是，我們有持有個資，以前是紙本，現在有建入電腦作查詢跟身份認證的問題。

主席徐嘉臨副處長：

它就會在C級，自行或委外開發資通訊系統。

海外信用保證基金：

所以第 6 條是不是隱含這個問題？因為它不是全國性、也不是區域性，是不是有這個意思？

主席徐嘉臨副處長：

對。

海外信用保證基金：

還是要明定一下，非屬第4、5條的話，個資就屬於第6條？

主席徐嘉臨副處長：

因為不是只有個資的問題，你現在提的這個服務，我們講 CIA 裡面的 C 而已，還有很多 A 的問題。我也必須特別提醒你，假設你有很多是非本國的個資，現在歐盟的 GDPR 就要特別去小心，有沒有適用那個規定，原則上看起來，你們應該是屬於第6條裡面的C級。

王詠萱分析師：

金管會有關第 4～7 條，目前的版本跟第二階段的座談會相比，影響程度是拿掉了，雖然影響程度拿掉，但是全國性或公務人員個人資料檔案之持有或處理，很難想像你的持有或處理有點狀況的話，不會造成他們的影響。第 4 條第 4 款，公務機關涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項，這邊的涉及，我們會指實際營運上面去涉及，行政兼管事項不會在涉及的解釋範圍裡面，是指實際上有營運這些業務，會造成實際影響的機關，條文上是這樣解釋的，不會中央目的事業主管機關去兼管到這些業務，影響到你的資通安全責任等級，原則上不會。

主席徐嘉臨副處長：

簡單來講，這個條文不是指金管會的兼管業務，而是純粹就金管會的資訊維護系統裡面所維護的範圍。國家衛生研究院剛剛的問題，這個資訊

系統分級及防護基準，現在規定 A 級機關是 1 年內要完成，所以你覺得 1 年還是沒有辦法完成？你的問題是這個嗎？

國家衛生研究院：

我也不曉得我們算 A 還是 B，因為我們有時候會研究，所以可能會截取到各個年齡層的資料，所以不曉得到底算 A 還是 B，但是記得 B 也是 1 年之內就要完成，對我們而言，時程很趕，不管是預算或人力。

主席徐嘉臨副處長：

後續如果有任何需要協助的地方，我們可以協助，但是時程的部分，立法就是明年 1 月 1 日正式施行，所以其實現在就可以作一些前置的準備工作。

國家衛生研究院：

但是因為你們的範本到 8 月才會出來，像我們原本已經有一些資安認證，所以我們可能要補強的只有少部分；但是有些單位可能原本什麼都沒有，等你們範本提出來再去做，我不知道其他單位會不會跟我們一樣有這樣的困擾。

主席徐嘉臨副處長：

A、B 級機關，以政府機關來講或者公部門的關鍵基礎設施，在過去的幾年當中，他們應該多多少少都已經有導入 ISO27001，所以去符合這個資通安全管理法施行，我想比較不會有太大的問題。你剛剛提到資通安全系統 1 年的部分，那個跟範本比較沒有關係，因為是在資訊系統的防護上面要做到哪些。

國家衛生研究院：

像我們有驗證 ISO27001，驗證公司會依據你的公司整個經費、人力或者是組織的決策，譬如有 100 多項的控制措施，我們不是每一項都要做，因為我們經費跟人力有限；但是我看你們出來的這個版本，感覺是所有措施都要做，其實我們要補強的很多，即使我們已經有認證了。

主席徐嘉臨副處長：

這個應辦事項其實算是基本的，如果要導 ISO27001，它有更多的管理，必須在這個範圍之外。

國家衛生研究院：

因為 ISO27001 適用性聲明書是我們自己可以去選擇組織因為人力或

經費。

主席徐嘉臨副處長：

沒有關係，我知道你的問題，如果你的 ISO27001 適用聲明書認為不適用，你就寫在你的資通安全防護計畫裡面。

國家衛生研究院：

可以這樣嗎？

主席徐嘉臨副處長：

你必須敘明理由，最重要的是你要保護你的核心系統，衛生研究院畢竟保有很多民眾醫療資料，你其實是一個很重要的機關，你覺得你的控制措施應該到哪裡？還是回去看一下你所保有的個資。

國家衛生研究院：

其實你們要的資料都已經匿名化了。

主席徐嘉臨副處長：

沒有關係，如果已經做到這樣子，就在你的維護計畫寫清楚就好了。

國家衛生研究院：

剛剛沒有回答到我另外的問題，有說要完成完驗證，是只有核心系統才需要，其他就不需要嗎？是這個意思嗎？附表一第 2 項。

主席徐嘉臨副處長：

對，核心系統。接下來還有其他問題嗎？

農糧署：

第一個，有關資安等級分級辦法的草案，第 3 條大概有提到，行政院直屬機關每 2 年要提交自身的責任等級報主管機關核定，但是整個分級辦法裡面好像沒有看到，如果我們自身提報的責任等級跟核定等級不同的時候，我們是希望建議主管機關核定的時候有一個理由，跟你所報送的責任等級不同的時候，可能要提供一個理由。要提供申覆或陳述意見的機會，至少要提供一個核定不同理由的時候，讓所核定的機關可能有一個申覆的機會。

第二個，在第 8 條裡面有一個各機關不具資通系統且不提供資通服務，這個部分設 E 級的條款，這邊所講不提供資通服務，不曉得是不是指對外的服務？類似我們常講網站對外的服務，如果內部只做一個 File server，內部使用的東西，或是有一些會計系統、人事相關系統的部分，

是不是內部系統就不包含在這個範圍裡面？

第三個，這邊規定有 A、B 級的資安責任等級，A 級要專責人員或專職人員，這個「專責」跟「專職」定義差在那別？據我了解，農委會底下的農金局，全局資訊人員就 2 位，又設為 A 級機關，可是這裡講專職人員要 4 位，明明就達不到，就只好送懲處，這個也是一個比較麻煩的單位，其實除了農金局之外，也有很多單位人力都不足，這個部分可能沒有辦法實際達到這個辦法的要求，是不是有其他的配套措施？

主席徐嘉臨副處長：

再徵求第二個。

臺灣大哥大：

我想請教附表一，有關於技術面部分，這邊有提到安全性檢測跟資通安全健診還有資通安全監控管理機制，在檢測的部分，第 1 項提到，要做網站安全弱點檢測，辦理內容是全部核心資通系統，每年辦理 2 次。我想請教，以電信業者來講，交換機一定是核心資通系統，但是它絕對不會有一個網站放在外面，所以這個部分我們是要勾不適用？還是就不符合？

另外系統滲透測試，可能是找白帽駭客從外面來試，但是我們交換機可能是在很內網的深處，所以基本也不會執行到這一塊，這部分是不是會有適用性的問題？

針對資通安全健診的部分，這邊有提到要作惡意活動檢視、漏洞檢視等等其他項目，我想請問這部分是自己執行就可以？還是要委外執行？委外執行就剛剛衛生研究院先進所提到，就是預算編列的問題，這個部分是不是可以給我們一個明確的指示？

接下來資通安全監控管理機制，因為這邊寫得蠻粗略的，完成監控機制建置，什麼樣的標準、水準才算是完成監控機制建置，會不會有認知上的問題而有懲處的結果發生？以上。

主席徐嘉臨副處長：

再徵求一位。

遠傳電信：

主要針對附表二 A 級應辦事項的部分，應辦事項這裡提到所謂安全性檢測這種全部核心資通系統每年辦理 2 次，系統滲透測試也是全部核心資通系統每年辦理 1 次，這個在執行次數跟執行範圍真的會牽涉實務執行面

還有預算資源面，所以我們建議全部改為「擇定」，由業者依照風險的高低，每年也依照資源的可行性，擇定核心資通系統，辦理的次數我們建議改為1次。

主席徐嘉臨副處長：

先就剛剛這幾個問題回答。

王詠萱分析師：

有關農糧署提到，如果是提報或核定的等級不同，原則上我們都會給機關申訴意見的機會，最後真的不一樣的話，我們也會提供理由，這點可以放心。第8條資通服務，是指對內、對外的資通服務都算，第8條不具資通系統或不提供資通服務，原則上是指整個系統基本上沒有資通訊環境的建置，內部可能連個人電腦都沒有。你剛剛提到File server或財會系統，這個原則上都會屬於資通服務的一部分，所以不管是對內、對外都會算，一個機關如果有File server或財會系統的話，應該就不會屬於E級機關。

針對專責跟專職人員的差別，所謂「專責」，資通安全業務有一個專門負責的人員，出事的話，他要作一些處理，這叫「專責人員」；「專職人員」比專責人員更進一步，他主要的工作業務都是跟資通安全工作有關的，可能也有少部分其他交辦的業務，但是業務大部分的工作都是資通安全業務，這樣我們叫「專職人員」。我們這邊會要求在公務機關的專責人員要以專職人員來配置，以上報告說明。

主席徐嘉臨副處長：

剛剛臺灣大哥大有針對網站安全性檢測滲透測試到底適不適用，我請同仁說明一下。

賴妍帆分析師：

在附表提到安全性檢測的部分，不管是哪一級，如果有提到安全性檢測的部分，你們可能是關鍵基礎設施的公共系統，或是剛剛先進提到是屬於交換機的部分，沒有辦法作相關網站檢測，這個部分可以在你們維護計畫裡面去敘明為什麼沒有辦法做的原因。

至於次數的部分，原則上我們建議還是維持現在目前，弱點檢測部分至少每年要辦理2次，滲透測試次數部分還是維持每年至少要辦理1次。

主席徐嘉臨副處長：

我想次數的部分因為 1 年只有 1 次，我覺得已經是最基本的要求，未來如果真的有一些不適用的檢測，例如很多是交換機，它沒有辦法作網站安全性檢測，就在你的維護計畫裡面作說明。

臺灣大哥大：

我剛剛講的問題，一定要委外嗎？

主席徐嘉臨副處長：

如果你有能量的話，你可以自己執行，這沒有問題，但是你就要講怎麼執行的，這個是 OK 的，不一定要委外。

我補充一下農糧署提到農金局，農金局其實過去是 A 級機關，如果以現在的資安責任等級，他應該不會是 A 級機關，這個部分可能回去作一個轉達，因為他沒有保有全國性的個資，應該也沒有區域性的個資，他所有的金錢業務全部是委託金管會來做，未來他的資安責任等級應該不會比照過去做處理，所以未來他專職人力的設置應該是可以降低的。

遠傳電信：

針對全部核心資訊系統及範圍的部分，是不是可以由業者這邊依照風險的高低去擇定？因為核心資通資系統現在如果框下來的話，可能在業者這邊是很恐怖的認證，1 年有沒有辦法給這麼多資源？這個在特定非公務機關，我覺得這個部分真的建議要考量，是不是給我們一些彈性，由特定非公務機關依照他的風險狀況來擇定核心資通訊系統？

主席徐嘉臨副處長：

我們可以考量，但是我想電信公司之所以會被指定，是因為關鍵基礎設施提供者非常關鍵，就是因為很重要，所以才需要作這麼多的資安防護。讓你們針對不同的核心系統，我想以電信公司來講最重要就是整個骨幹網路或者其他機房等等維護，是你們的核心，所以大概會是在這個範圍裡面，我不太清楚你的核心系統會多，是多到哪裡？或許你可以告訴我們一個你自己認為的，我不曉得我們認知有沒有差距？會後或許我們可以就這個部分作討論，不過原則上我們應該不會變，核心系統都應該作這些應辦事項裡面的作用，之所以為核心就是因為它很重要，所以才需要做，我們現在所列的應辦事項每年辦理 1 次，這個都是基本要求，應該不至於是太過分的要求，更何況現在的資安議題，尤其是電信業者其實是很容易，因為你們是所有基礎裡面的基礎，所有的數位服務大概都是基於在你們基

礎網路上去做服務的，所以電信網路如果一旦有這些資安事件發生，其實影響的層面範圍會很大。原則上我們還是依據現在的規定，會後我可以請教一下你們所認為的核心系統會多到哪裡，這個部分我們可以稍微了解一下。

針對資安責任等級還有沒有其他的問題？

親民黨團：

後來我有回去查一下，衛福部有關於公立區域醫院跟公立地區醫院的名詞，是從醫院評鑑等級來的。可是上次你們同仁有提到，其實你們是從緊急醫療救護的觀點來看這個問題，我覺得你們可能自己要跟衛福部協調一下，因為醫院評鑑等級只是一個硬體設施及人力的設置標準，這個東西跟資安有沒有很直接的關係我不知道，這要問你們，你們認為越多人的醫院、越大的醫院，它的資安等級要越高？也許你們設定標準就是這樣，其實我就沒有意見；如果你們是以緊急救護或者緊急醫療，顯然就不是這樣子，因為我上次有跟你們講過，他們緊急醫療救護的設置標準又是另外一套，所以我覺得這個你們可能要再跟衛福部研究一下，用公立醫院跟區域醫院到底是不是你們需要的？

主席徐嘉臨副處長：

接下來有沒有第二個？

行政院資訊處：

本法裡面有講到資通系統與資通服務，我不知道這兩個實際上真正的區別是什麼？我舉例像是之前資訊系統分級以及資安的防護基準規定，這個規定主要是針對一些看起來像是應用系統開發需要遵守的分級跟規定，裡面其實也有排除 email 的系統，或者是 AD 或防毒軟體，我不知道資安相關的子法裡面講到這些系統到底是什麼？如果說像資通系統的話，看起來就是要作分級，機關裡面的 email 系統，或者機關裡面的基礎網路服務，是不是也要作分級的判斷？

我們在資安法施行之前，我們有針對一些資訊系統作過一些分級的評估跟核定，那資安法施行之後，這些核定評估是不是要重做？還是以先前的核定就可以了？

另外應辦事項裡面像 GCB 裡面，有一些事項有一些例外，或是我們設定的比 GCB 更嚴格的時候，我們會採取一些例外管理，這些例外管理將來

是不是也要報主管機關備查？

主席徐嘉臨副處長：

有沒有第三個問題？

亞太電信：

詢問一下有關這次版本的附表二，這個資通安全等級A級的特定非公務機關應辦事項裡面，認知與訓練裡面提到，資通安全專責人員總計要持有 4 張以上的證書，我們記得之前先前的版本是提到 2 張，我們想要知道為什麼這個部分新增變成 4 張？

第二個問題，新版的部分資通安全專責人員總計持有 4 張以上證照，這個專責人員是不是 4 個人 4 張？還是有 2 個人相關證照有 4 張？我希望能夠釐清這個辦法的規定，到底實際上的要求是什麼？

王詠萱分析師：

先回答有關於資通安全專業證照的問題，在這一次預告的版本，A 級機關有 4 名資通安全專職人員，證照提高到 4 張，計算方式是 4 個人加起來有 4 張就好的，可能 2 個人各 2 張，另外 2 個人沒有是可以的，但是我們還是會希望既然已經指定資安專職人員，可能還是要給他足夠的訓練，所以證照跟人員的訓練我們會作一個對應，還是希望給資安的專責人員足夠的訓練，讓他可以去執行資安的業務。

另外提到公立區域與公立地區醫院，我們現在的分級方式是公立的區域醫院列在 B 級，公立地區醫院列在 C 級，主要是依照衛福部現在公立醫院責任等級分法就是如此。我們在這個應辦事項是裡面，先前有跟衛福部討論過，就是維持現在的機制，公立的區域醫院在 B 級，公立的地區醫院在 C 級。至於衛福部怎麼分區域醫院與地區醫院，我們會後要再去了解一下，以後這樣的分法是不是適當，我們之後也會跟衛福部作一個討論，如果覺得需要作一個調整的話，我們會再作一個調整。

親民黨團：

我覺得你們每次都不針對我的問題回答，我已經幫你找到答案了，衛福部會這麼回答你，他是根據醫院評鑑標準，醫院評鑑標準是依照醫院的規模、設置的人數與科別，去設立醫學中心、區域醫院、地區醫院、診所，就是按照這個規模大小。

我的問題很簡單，如果你們認為醫院規模越大，資安等級需要要求越

高，上次你回答我的是，按照醫院的緊急救護的責任區分的，我當場提供告訴你們，按照衛福部另外一個公告的標準，以北部來講，緊急救護醫院的區分跟你所認知評鑑的標準是完全悖離的，譬如說像仁愛醫院那麼大，他是中度，不是重度的，民生長庚醫院，他也不是重度緊急救護醫院，這個時候醫院的規模大小跟是不是緊急救護沒有一致性。我的問題很簡單，如果你們認為醫院規模大小作為區分標準，我也沒有意見，如果你們不是按照這個標準去區分資安等級的話，我提醒你們可能要再作一個修正，因為緊急救護的責任等級，跟醫院評鑑標準不是同一種標準，醫院有很多種標準，衛福部的標準太多了。

主席徐嘉臨副處長：

我們的考慮點是醫院負擔了很多角色，第一個它有緊急醫療的功能，他的緊急能量大小…

親民黨團：

我跟你講過了，譬如在民生東路的長庚，他看起來很大又屬於長庚體系，他應該是屬於重度的緊急救護醫院，對不起，按照衛福部公告他不是。

主席徐嘉臨副處長：

我說明一下，我們現在資安等級講的是公立醫院，我們先確定我們的目標，你聽我講完。

親民黨團：

有很多例子，我們先不要管是不是公立，醫院規模大小跟他是不是緊急救護的責任等級，沒有一致性，如果你們堅持一定用醫院規模大小作為判斷標準，我也認了，反正這個是衛福部的意見，我無所謂，到時候有沒有達到你們的目的，你們自己比較清楚，因為如果你們認為緊急救護責任，就是擔任起重度緊急救護才是你們應該維護資安的目標的話，應該是以另外公告的標準為準，而不是按照醫院設置評鑑標準。

主席徐嘉臨副處長：

我先說明一下，醫院裡面的很多的系統，甚至醫療系統、support 開刀或任何醫療救助的系統，很多都是在 IT 跟 OT 系統裡面支持它的，換句話說，如果今天他負擔起緊急醫療的責任，他沒有把 IT 與 OT 系統維護好，萬一國家發生重大災難，需要大量傷患進去醫院的時候，他是不是應

該把 IT 跟 OT 系統維護到一定的程度，所以這是為什麼我們考慮，把醫學中心這種醫院列在 A 級的原因，因為他的服務能量大，因為現在很多的緊急醫療都是靠 IT 或 OT 系統支持它的。

第二個，醫院裡面保有很多的個人資料，尤其是醫療病歷資料。以上個月新加坡發生的醫療、醫院個資外洩的事件，就可以知道其實它影響衝擊層面有一定的程度，所以這兩個點是我們在考量醫院分級不同等級的因素，這樣子有回答到你的問題嗎？

親民黨團：

我沒有意見，如果你們認為醫院規模比較大，你們就這樣子去設置好了，因為不要講說緊急醫療救護，因為緊急醫療救護那個名單跟醫院評鑑標準是分別的兩件事情。

主席徐嘉臨副處長：

我剛才已經回答你的問題了，就是我們考量的點就是這樣，這個部分也有跟衛福部去討論過，這就是我們現在的看法。

再來資訊處剛剛有提到幾個問題，資訊系統防護需求分級，大部分指的是資訊系統，你剛剛講的 Email、AD 其實它不在範圍內，所以你只要特別針對資訊系統必須針對機密性、完整性、可用性，去分出高、中、普三個等級，接下來你剛才提到 GCB 的部分，你先前也有提過，你認為做得比他更嚴格或是不適用，都可以提出來說明這個沒問題的。

資訊處：

有需要送主管機關備查嗎？因為像 11 條有特別講，像是有未執行的部分有說要做一個備查的動作，所以說像 GCB 的不一致性的狀況，是不是到時候也要作一個備查？不知道我的解讀有沒有錯？或者是說，其實應辦事項有講到專責人員，如果到時候真的沒有辦法執行。

主席徐嘉臨副處長：

我請同仁說明一下。

王詠萱分析師：

第 11 條第 2 項，各機關辦理附表一或附表七所辦應辦事項或執行附表九，如果是因為技術的限制或資通訊系統之設計結構或性質因素顯有困難的，這邊指的「顯有困難」指的是，整個應辦事項根本就沒有辦法做到，譬如說剛剛有一位先進提到，他的系統是非常內部，沒有辦法從外部

滲透測試到它，顯有困難是說這整個應辦事項，這一項就做不到；如果你已經有做到 GCB 的政府組態標準，只是有一些例外管控措施，是你們機關自己內部控制的話，這個不算是所謂的顯有困難，這個程度上是不太一樣的。

主席徐嘉臨副處長：

我特別補充一下，GCB 未來主管機關在對公務機關進行稽核的時候，會特別去看的一個指標，所以這個部分，機關依據後面的應辦事項去辦理，這個是沒有問題，但是未來稽核的時候，那個部分會被看到的。接下來還有其他的問題嗎？

中華電信：

第一個，有關於剛才說的第 11 條，希望能夠再作一個釐清，這個部分是各級機關針對 A 級或 B 級，依主管機關指定的方式提報第一項事項的辦理情形，事實上這些情形，目前在母法裡面在資通安全維護計畫裡面就要說明整個控制措施的執行狀況，而且是送給中央目的事業主管機關，但是在這條看起來又是要給行政院，所以是不是在這部分可以釐清未來我們的辦理情形？建議能明確的指出非公務機關的部分，就是給中央目的事業主管機關。剛剛講到的顯有困難送交主管機關備查，是誰送？是中央目的事業主管機關送給行政院，還是這個部分特定非公務機關只需要提供給我們的中央目的事業主管機關核定就可以？

第二個，針對附表二的部分，我們有幾項可能要釐清：一、有關於存取控制第 20 頁圖的部分，這次有新增一個並採用伺服器集中過濾機制檢查使用者之授權，這個部分能不能說明是指什麼樣的方式，假設因為我們普級系統原來是沒有集中認證，為了這個再增加集中認證，反而會增加新的風險管控點，所以這個部分如果不清楚要怎麼執行的話，建議能夠把它作刪除。

二、在稽核可歸責性的紀錄內容，這個上次有反應過，針對單一日誌紀錄的機制，我們通常會依據日誌收容需要的格式去產製，不會是單一的日誌紀錄格式，所以建議把它刪除，因為這個實務上、目前執行上也會有困難。

第三個，識別與鑑別裡面，有提到內部使用者的識別跟鑑別，其中有一項是對帳號的網路或本機存取，採取多重認證技術，一般我們事實上我

們能夠到本機登入的時候，一定是到了機器的前面使用 console 進去，而且會有實體管控，所以這個部分建議把本機這樣的字眼刪除，因為我們很難做到，譬如交換機要 two factor，到本機登入還要 two factor 的認證這個部分實務上執行有困難的。

第四個，在這次身份驗證管理也有增加一個帳號達三次失敗後，至少 10 分鐘不允許繼續嘗試登入，這部分把 10 分鐘改成限定時間內，這個部分主要在防密碼被暴力破解；可是萬一我們遇到惡意嘗試，故意把它登入失敗，造成我們設備反而被鎖定的時候，可能會影響我們重要設備搶修復原的時間，因為這個部分事實上我們也已經有要求要使用多重認證技術，所以應該是可以防範暴力破解的風險，建議把時間作彈性的調整。

第五個，針對系統服務，上次有反映，有關於滲透測試的部分，建議是移到系統發展部署跟維運階段，因為上線環境與測試環境不一樣，滲測其實是在接近上線環境作的時候效果比較好。

第六個，針對系統通訊保護的部分，這次有新增針對演算法的要求，我們是建議把第 3 項使用演算法支援的最大長度金鑰能夠刪除，因為事實上使用者端的環境支援度都不一樣，我們不見得會用到最大、最長的長度，只要確定這個演算法沒有被破解就可以了。

主席徐嘉臨副處長：

我先回應中華電信的問題，你剛才會前有提供，你講的部分因為有很多細節的東西，會議上我沒辦法回答你，會後我們會針對你的建議逐一研究一下，會後把結果再跟您這邊說明，後續針對你提的，我們會回應思考的點是什麼、決定怎麼樣都會跟你說明。

接下來還有其他的問題？

臺北市政府消防局：

關於公務機關應辦事項裡面，資通安全責任人員是以專責人員配置，這個專責人員配置除了下面寫到的證照，還有職能訓練之外，是不是在人員的資格上有一些規定，譬如必須要是資訊職系的人員之類的規定，如果機關沒有這樣的人力配置的話，有沒有其他的可以解決？

主席徐嘉臨副處長：

有沒有第二個問題？

行政院原子能委員會：

附表三、附表五，資安的專業證照及職能訓練的要求，這邊可不可以限定被指派專職人員一定期限內取得就好？他一被指派就要這個證照，有可能這個機關只有 1 個人有，之後還要商調會不會被禁止？所以建議限定一定期限內取得就可以了？

第二個，有關資安職能證照的部分，因為現在有很多國際證照，在有效期限內取得一定量的教育訓練，或者相關的經驗時數，就可以延長有效期，有關職能證照的部分可以改成類似取得訓練或經驗就可以了，不用每次都要去重新考一次。

主席徐嘉臨副處長：

中華電信剛剛提的，報給主管機關，還是報給中央目的事業主管機關的問題，接下來的問題我們後續再作一併的思考。

臺北市政府消防局跟原能會的部分，先請王詠萱分析師說明。

王詠萱分析師：

就中華電信提到的第 11 條第 3 項，依主管機關指定的方式提報第一項辦理的情形，這個部分後續到底要向主管機關報還是向中央目的事業主管機關報，就是比照資通安全維護計畫的實施情形方法提報，這個部分容我們會後再跟主管機關討論一下，我們再看看要怎麼調整。

有關第 2 項顯有困難的核定，其實是由中央目的事業主管機關來核定，核定後是由中央主管機關送備查還是由各機關送備查，這個部分也是容我們再跟中央目的事業主管機關再溝通。

主席徐嘉臨副處長：

原則上關鍵基礎設施提供者，面對的就是中央目的事業主管機關，所以這個文字我們後續再做調整，原則上主管機關大概不會直接面對關鍵基礎設施提供者，所以我們後續會作文字的調整，之前定的還是以公務機關為主，比較沒有思考到關鍵基礎設施提供者提報權責的部分。

王詠萱分析師：

針對臺北市消防局，有關專責人員是有其他的要求，在責任等級裡面對專職人員的要求，第一個是教育訓練，第二個可能是專業證照，跟職能證書，它沒有要求一定要由資訊人員擔任，如果機關沒有專職人員的話，依照我們法的要求你還是要配置專職人員，就看您這邊人員是由現有業務的調整，或者在進用相關的專職人員，總之依照法的規定，就是要配置專

職人員。

接下來針對原能會，有關職能評量證書是否被指派後一定時間取得？基本上我們這邊主要規定證照的數量，就是有關專職人員 A 級機關持有 4 張，B 級機關 2 張、C 級機關 1 張，以總數來看，機關這邊人員流動，是正常的流動，只要流動完在一定的時間內有把證照補強，我想這個認定上是可以接受，不會造成人員無法流動的問題。

資安職能證書，因為也是有期限，也是有更新的機制，更新就我所知，是上維護證照的有效課程就可以了。

主席徐嘉臨副處長：

我大概簡單補充一下，資通安全專責人員取得專業證照這項，就法制的文意上應持有 2 張，沒有說一上任就一定要 2 張，其實在實際運作上也沒有這麼強制性的要求，或許我們思考一下後續要不要補充文字，在指定後多久之內取得，這個部分我們可以來思考調整一下文字。

另外一個是剛剛我們同仁有講，專責人員不一定要資訊職系，這個考慮到機關目前的現況，因為我們在設置 A、B、C 等級的時候，都希望各機關專責的資安人力。對於公務機關的部分，我們現在也在思考一下怎麼讓各機關有一個過渡性的做法，從實行後在多久時間內補足這樣的人力，但是在補足人力之前這個過渡性作法我們還在研擬當中，我們會給機關一個參考，到時候會再跟各位說明。

原則上資通安全專業證照要持有 2 張，是要有效的 2 張，不是持有之後然後過期或其他原因無效，這個不是立法的目的。至於證照如何維持，每個證照的做法會不一樣，這個部分還是回歸每個證照的做法。

行政院原子能委員會：

剛剛在問職能訓練的部分，因為職能訓練是行政院在辦，職能訓練是上完課還要考試，我的意思是可不可以比照像是國際證照，你有一定的經驗或者訓練時數，就可以延長職能訓練證照？

主席徐嘉臨副處長：

我可以直接回答你，應該是沒有辦法，因為這個課程會隨著攻擊手法改變增加不同的內容，所以有時候請上過的人再來上的目的，是希望你們了解新的攻擊趨勢，再去經過一定的考試維持這張證照，這個部分是沒有辦法的，還是一樣要持有，而且必須再經過重新發證的過程。

司法院資訊處：

附表一的部分備註二，資通安全專業證照，指由主管機關認可這些規定，不曉得將來主管機關會列出一張清單，所謂的專業證照包含哪些？跟發照的機關。這邊沒有定義到所謂的職能訓練證書，只有寫證照，這個問題是不是也有一個主管機關把認可的證照，發證的單位，作一個列表，讓將來公部門派人受訓的時候，不會拿到一個無效的證照或證書。

主席徐嘉臨副處長：

有沒有第二個問題？我先回答這個問題，其實現在市面上資通安全的證照非常多，我們當然可以列出來給各位參考，但是也不限於我們列的那些，臺灣一些訓練機構在辦的很多。至於評量證書的部分，發證目前就是行政院資安處底下的技服中心在發，所以沒有所謂的你剛剛希望它能夠列表。

司法院資訊處：

定義的問題，因為備註二有寫，是由主管機關認可，那職能訓練證書沒有特別說明什麼叫做職能訓練證書，它是不是有定一個時數？還是像主席講的，由技服中心所發都算是？

主席徐嘉臨副處長：

應辦事項下面那一項叫做資通安全評量證書的部分，是行政院資通安全處委託技服中心在辦，這個部分直接去上課就可以，這個比較沒有太大問題，剛剛另外的問題，資通安全專業證照的部分，那個是坊間或國際性開的課程的證照，那個部分我們後續提供參考清單，但是我覺得不限於那些清單，只要有資通安全相關的，最重要的是回到業務上，是業務上需要的才是最重要的，而不是盲目的考證，但是對於機關的對於資通安全的幫助一點都沒有。接下來還有嗎？沒有的話我們進入下一個。

第三個子法「資通安全通報及應辦辦法」。

遠通電收：

剛才有提到資通安全事件定義，裡面有句話叫「違反資通安全政策」，這句話有沒有更白話一點？或是能讓我們了解什麼叫做「違反資通安全政策」。我們剛剛看有分 1~4 級，現在看起來只要是違反了，只要是非核心的、在可容忍中斷時間內、可以復原的，也要去作通報，這樣會造成會造成關鍵基礎設施很大的 loading 存在。

主席徐嘉臨副處長：

有沒有第二個問題？

國家衛生研究院：

在所有的子法裡面，如果有特別寫核心系統，就是那些措施就是指針對核心系統，如果沒有特別指針對核心系統，是所有系統都通用嗎？不管是哪一個子法都一樣？

主席徐嘉臨副處長：

可不可以舉個例子？

國家衛生研究院：

譬如說像前面分級，像導入驗證就有特別指出核心系統，但前一項核定等級內要完成安全措施，就沒有特別指出是核心系統。

主席徐嘉臨副處長：

你說的是哪邊？

國家衛生研究院：

責任等級附表那邊，管理辦法。我不懂整個子法裡面，哪些是針對核心系統？哪邊是所有的資通系統都要去做的？

主席徐嘉臨副處長：

原則上，有特別指明核心系統的部分就是針對核心系統。

國家衛生研究院：

如果沒有特別指明，就是所有資通系統就要做嗎？

主席徐嘉臨副處長：

應辦事項裡面其實它著重大部分都是核心系統，當然其他的使用者或者是伺服器。

國家衛生研究院：

或是像 1 年之內要完成所有的控制措施，是針對所有的資通系統嗎？還是核心系統？

主席徐嘉臨副處長：

我了解你的意思，就是針對分級的部分，這邊現在沒有特別寫，是所有的系統。

國家衛生研究院：

像委外也是所有資通系統也要嗎？因為我看有一些子法會特別指出核

心系統，有些是寫資通系統。

主席徐嘉臨副處長：

沒有的話，就是全部。其實委外的系統更需要，現在很多資事件都是發生在委外的管理上與委外的系統上面。

國家衛生研究院：

但是它可能只是很小的資通系統。

主席徐嘉臨副處長：

如果不是很重要的話，基本上就會落在普，普需要做的安全措施相對是少的。

臺灣大哥大：

針對資通安全事件通報，這邊有分 1~4 級，這邊分級可能會針對核心跟非核心，非核心大概 1~2 級，核心 3~4 級起跳，從邏輯的角度，核心加非核心大概是 100%，一般電信業者光是主機都好幾千臺以上，一臺 server 如果發生 outage，如果在可容忍的時間之內回來的話，依定義來講可能是第 1 級，那第 1 級照你們的規定也要 1 個小時內通報，我想這樣幾千部主機的數量，這樣通報會不會不小心去排擠到重大事件的通報？會不會資訊過量的問題？剛剛遠通有提到一點，到底哪些設備要進來這個範圍之內？其實我們有一個想法，如果關鍵基礎設施會被納入特定非公務機關，最重要當然是通訊相關，可是現在的電信業在通訊之外，還有其他加值服務的部分，譬如說電子商務、電子書、音樂等等，這些應該不是我們被納入特定非公務機關的考量，這個範圍可不可以限縮或界定，讓我們把資源放在需要的地方？

主席徐嘉臨副處長：

再徵求一個。

中國輸出銀行：

就以第 1 級事件來講，非核心業務或非核心資訊系統運作受影響或停頓，於可容忍時間內恢復正常運作，是不是說所有的機器只要一當機，就要列為資安事件就要 1 小時之內回報？如果剛好資安專職人員請假，由誰來回報？因為我們關心資安專職人員不可以兼其他事務，做其他事務就不可以作資安，如果我們機關內只有一位資安專職人員的話，那誰來回報？以上謝謝。

主席徐嘉臨副處長：

我先就這幾個問題請王詠萱分析師回答。

王詠萱分析師：

針對幾位先進提到，資通安全事件分級的部分，我先回答一下，資通安全管理法第 3 條就在名詞定義已經講資通案件事件的定義，譬如說違反資通安全政策、資通訊系統是受影響或停頓於可容忍的中斷時間之內恢復，有沒有規範資通安全政策應該是這樣來看，重要的系統可能有備援的機制，你會認為重要的系統是不應該停頓的，假設你備援的機制裡面一臺系統失效，但是你備援機制有起來，整個資通訊服務是沒有中斷，沒有造成資通系統機能運作的影響，就不是屬於我們資通安全事件的定義。舉一個違反資通安全政策的例子，基本上你的防護措施沒有失效，或是說沒有影響到資通安全系統機能運作，原則上就不會是資通安全事件的定義。

剛剛另外一位電信業者先進提到，有一些加值服務跟範圍界定的問題，這個問題在通傳會有討論到，如果原本不是我們的公營事業或財團法人，是關鍵基礎設施以外的提供者，到時候我們在認定他的核心業務、非核心業務，或關鍵基礎設施的範圍，我們會以被列管的關鍵基礎設施的業務來認定他的核心業務、非核心業務跟關鍵基礎設施，其他不屬於關鍵基礎設施的業務，我們不會認定，在認定上我們會作一個調整。

主席徐嘉臨副處長：

我補充說明一下，關鍵基礎設施提供者，我們關心的是關鍵基礎設施的服務，譬如中華電信 MOD，那不是我們關心的，我們關心的是你們關鍵基礎設施上面資安事件的通報。至於怎麼界定關鍵基礎設施之外非核心的部分，我們內部也討論過怎麼明確定義，但是還蠻難的，初步的想法，至少把關鍵基礎設施的提供者界定出來，因為你們很多子公司，子公司絕對不會是我們要定義的提供者，我們會針對你們的骨幹或是電信服務，這個電信服務到底是哪個子公司，它提供的服務一定是關鍵基礎設施，接下來在關鍵基礎設施以外的服務我們才定成是非核心的業務，目前初步是這樣，不會把所有的公司，除了關鍵基礎設施所有的集團公司都全部納進來，不會的。

賴妍帆分析師：

我們先回答剛剛中國輸出銀行有關於通報的部分，剛才提到通報方式

如果資安專責人員請假或不在怎麼通報？原則上，以目前的通報系統來看，那個帳號是機關帳號，回歸到一般業務的代理人，應該有代理機制，大家會比較在意的一點是，目前的通報機制上面要需要填的資料比較繁瑣，會造成如果不是由資安專責人員去填的時候會有一些困難的點，這個部分我們未來會簡化初次通報所需要的欄位跟數量、內容，應該會減少代理人在填報代理通報時候的困難。

剛剛提到如果是在可容忍中斷時間內恢復正常運作的話，是不是還要通報？原則上這個部分以目前來看，如果說它符合這一項，還是需要作通報。

主席徐嘉臨副處長：

我補充說明一下，通常各位在作資訊安全管理的時候，會把一個系統訂定 RTO、RPO，就是一旦發生災難的時候，你預計你要花多久時間恢復，這個就是可容忍時間，假設你在這個時間內恢復的話，依照法律的規定，它是屬於 1 級，因為它是於可容忍的時間內恢復正常運作，那個可容忍的時間是指這個，所以你剛剛提到一當機，我們就要問一下，看起來是在可容忍的時間內恢復嗎？後面比較嚴重的等級，就是在於不可容忍時間內去作處理，才恢復的話，就是比較高級的資安事件，目前資安事件的等級定法是這樣子。

中國輸出銀行：

只要一當機就要回報？這樣主管機關會煩死。

主席徐嘉臨副處長：

如果你是個核心的系統你應該不會讓它當機吧？

中國輸出銀行：

可是你這邊寫非核心，所以非核心也要通報嗎？

主席徐嘉臨副處長：

所以目前現在的定法是非核心系統一旦有資安事件、停頓的話就要通報，原則上因為你的保護措施沒辦法保護它，讓他當掉了，所以就要通報。

中國輸出銀行：

所以非核心也要通報？

主席徐嘉臨副處長：

對。目前就是這樣。

中國輸出銀行：

如果半夜呢？

中華經濟研究院：

內部資訊系統算非核心，內部資訊系統當機我需要昭告全部的人？

中油公司：

因為系統核心就有定義核心，只要不被納入核心就是屬於非核心。

主席徐嘉臨副處長：

我知道目前就是這樣子。

中國輸出銀行：

像我們內部表單系統一當機我就要馬上通報，這樣對嗎？

主席徐嘉臨副處長：

我了解，這個問題我們回去思考一下。

中國輸出銀行：

譬如半夜當機了，我們還是要半夜被 call 起來，1 小時內通報？

主席徐嘉臨副處長：

資安事件的處理沒有所謂的白天或晚上，如果你要當資安人員你就要有這樣的認知。

中油公司：

核心系統是 OK，但是非核心的？譬如剛剛說的門禁系統，因為只有核心與非核心兩個。

主席徐嘉臨副處長：

我了解，我回去做一個通盤的考量，我們還是要視必要性，我想以我們的角度在看時候，我們比較關心的是，今天假設一個機關發生了資安事件，既使是非核心的，如果過沒多久或同一時間其他機關也發生了，那可能是我們行政院比較關心的，會不會有其他隱藏的資安事件沒有被發現，或者後續有更大威脅的可能？這個部分容我們再作一個思考，不過現在就目前公務機關的運作規則，現在應該是這樣，各位不會不知道吧？

中國輸出銀行：

這個牽涉到通報還有罰則的問題。

主席徐嘉臨副處長：

因為這次有特定非公務機關的加入，所以我們會在做審慎的考慮，謝謝。

中國輸出銀行：

請問一下，半夜要做通報，所以沒有人敢做資安人員，因為半夜要被call起來。

中華經濟研究院：

你可以上班時間再通報嗎？

主席徐嘉臨副處長：

這個問題我沒有辦法回答你。

中國輸出銀行：

沒有通報就要被罰然後被懲處，這樣誰敢做資安人員？

主席徐嘉臨副處長：

我們還是回歸到這個問題，什麼樣的等級要通報，怎麼樣 1、2 級、3、4 級，詳細的把分野拉出來，這是後續我們會去考慮的，接下來還有其他問題嗎？各位可能只關心通報的問題，對不對？

中油公司：

最後一頁，第 20 條，有一個文字是誤植，第 20 條的倒數 4。

主席徐嘉臨副處長：

這個我們知道，我們後續的調整過程會調整。

主席徐嘉臨副處長：

第四個子法「特定非公務機關資通安全維護計畫實行情形稽核辦法」。

親民黨團：

延續預告草案之前的問題，顯然沒有一個答案，在之前的會議就有提到，從法條來看，從第 7、16 條，規定主管機關要定一個特定非公務機關的稽核辦法，第 16 條，目的事業主管機關還要定一個稽核辦法，但是差別是母法第 7 條是得，第 16 條看起來就是「應」，我們現在討論的是主管機關「得」稽核的辦法。請問一下，目的事業主管機關應稽核的辦法，如果真的像你們預定的明年就要上路的話，目的事業主管機關哪時候就要定出來？而且最大的疑問就是，到底兩個辦法的相似度有多少？如果目的事業主管機關看起來是「應」的話，主管機關還有必要去定嗎？

主席徐嘉臨副處長：

中央目的事業主管機關要不要定嗎？

親民黨團：

我不曉得是誰的問題，因為在立法上就出現重複的地方，第 7 條是主管機關得稽核非特定公務機關，所以會訂定相關的稽核辦法，第 16 條的目的事業主管機關沒有「得」，最後提到第 6 項又規定第 16 條，目的事業主管機關第 2 項到第 5 項去訂定稽核辦法，顯然的這個就是中央目的事業主管機關針對特定非公務機關的應辦事項，因為沒有「得」或「應」的問題。我覺得在實務上這兩個稽核辦法應該不會相差太多，先不管去管立法技術，當初立法院去立法有沒有錯誤的問題？在實務上有必要嗎?因為目的事業主管機關，本來就應該要訂定一個稽核辦法，現在主管機關得稽核的辦法先出來，請問目的事業主管機關的稽核辦法哪時候會出來？如果到時候目的事業主管機關定出來了，結果還是跟主管機關的稽核辦法長得很像，有這個必要嗎？其實你直接委託給目的事業主管機關每年稽核 1、2 次就好了，你知道嗎？就是主管機關也要稽核，然後目的事業主管機關也要稽核。

主席徐嘉臨副處長：

好，我知道了，有沒有第二個問題？

中華電信：

有關於辦法第 5 條，前面已經有提到會用現場說明，我們只是建議在文字上略作調整，就是主管機關辦理第 3 條第 1 項之稽核「得要求受稽核機關之人員進行維護計畫實施情形之說明」，前面加一個「現場說明」；然後把「配合措施」改為「必要協力」；最後是「提供相關文件或證明資料」加五個字「供現場查閱」，以上建議，謝謝。

主席徐嘉臨副處長：

你這個文字剛剛才一樣有提供嗎？

中華電信：

有。

主席徐嘉臨副處長：

好，還有第三個問題嗎？沒有的話，我們先就這兩個問題作說明。請王詠萱分析師針對特定非公務機關的時程跟稽核辦法，跟各位說明一下。

王詠萱分析師：

我們資通安全管理法對特定非公務機關的稽核定在三個地方，第 7 條第 2 項，主管機關對特定非公務機關「得稽核」，第 16 條中央目的事業主管機關對關鍵基礎設施，這裡是「應稽核」，第 17 條，中央目的事業主管機關對關鍵基礎設施以外，就是對公營事業跟財團法人，這個是「得稽核」，這個三個稽核，母法都有要求訂定相關的辦法，基本上在這個子法裡面是主管機關對特定非公務機關的稽核，原則上中央事業主管機關對特定非公務機關的稽核，不管是應稽核或得稽核，他們都要去訂定他們的的辦法，這個辦法是法規命令的層級。原則上我們已經有跟中央目的事業主管機關開會溝通過，原則上是希望他們在 9 月中之前把這個辦法進行預告，因為法規命令我們要踐行一定的程序，這些行政程序我們希望在 9 月中旬能完成，行政院在 8 月中旬會提供稽核計畫相關辦法的範本，這個稽核計畫相關辦法的範本會參考子法的草案，只是因為各機關可能還需要一些彈性，譬如稽核的通知或稽核報告什麼時候交付，這邊他們是想中央目的事業主管機關對特定非公務機關，就是公營事業跟財團法人這邊是「得稽核」，所以也會有一些通知的時間，這個地方可能還是會讓主管機關依照他們的一些性質去彈性調整，但原則上其他的條文會比照稽核辦法的條文，我們會提供範本給中央目的事業主管機關，希望他們在 9 月中就把這個定出來開始預告，這是一個進行的時程。

主席徐嘉臨副處長：

針對中華電信提的文字修正建議，這邊有提到維護計畫事實情形相關之現場說明，我想這個現場部分沒有太大問題，我們後面版本沒有強調現場，這次有強調了，這邊再加一個現場，我們回去看一下，會不會有贅字，如果可以的話，我們會同意用你們的文字；後面「必要協力」，我不太懂你的意思是什麼，因為法規比較少用「協力」兩個字，這個 4 個字我不太知道語意是什麼，我會後跟你請教一下，回去再跟法規單位作文字意見上的討論，才有辦法決定，先作這樣的說明。接下來還有意見嗎？

遠通電收：

就我知道行政院資安處每年都會針對政府機關與關鍵基礎設施作一個資安查核，未來資安管理法的查核跟未來行政院的資安處的查核會不會有所不同，譬如今年我要被我的主管機關查核，又要行政院的資安處查核，

1 年卻有 2 次以上的查核，這兩個以後會不會併在一起？

主席徐嘉臨副處長：

現在行政院資安處沒有對關鍵基礎設施作特別的查核。

遠通電收：

有，我們今年就被別列為侯選機關，也有去參加說明會，他說如果中選就會發文通知。遠通電收其實在 103 年就遇過一次了，那個時候是因為高公局還有交通部的要求，我們也做過一次，未來他也把我們列為侯選機關，所以今年我們也有可能會抽到作這樣的稽核，我想知道這兩個有什麼不一樣？這兩個會不會併一起作？

主席徐嘉臨副處長：

你講的是現在這個特定非公務機關稽核辦法跟現在行政院對公務機關做的辦法有什麼不一樣，是不是？好，第二個問題？如果沒有的話請賴妍帆分析師針對這部分說明一下。

賴妍帆分析師：

剛剛遠通電收提到稽核的部分，之後這個法施行後，你講的兩個應該是同一個稽核，未來主管機關行政院會每一年辦一個稽核，對象會包含公務機關跟特定非公務機關，之前座談會比較多機關在意的是主管機關行政院辦理稽核，跟所謂的中央目的事業主管機關辦理稽核會不會重複，造成您剛剛提到，1 年會重複稽核的狀況，這部分我們未來主管機關在訂定相關稽核計畫的時候，會先跟各個中央目的事業主管機關協調，假設今年已經敲定要去哪幾個單位、已經選好了，原則上我們就不會再重複稽核打擾大家。

主席徐嘉臨副處長：

先跟各位報告一下，其實我們現在對公務機關做稽核，我們也不會每年稽同一個機關，除非這個機關屢次發生重大資安事件，我們才會這樣子，不然其實不會每年都稽核同一個政府機關，未來中央目的事業主管機關跟主管機關的稽核會是錯開，假設今年中央目的事業主管機關已經做了，我們大概也不會今年或明年就去做，實務上不會這樣子，這個我們跟中央目的事業主管機關可以去作協調的。還有其他問題嗎？如果沒有的話我就進到下一個。

第五個子法「資通安全情資分享辦法」。這個部分有建議嗎？（無）

如果沒有的話我就進到下一個。

第六個子法「公務機關所屬人員資通安全事項獎懲辦法」，這個部分有建議嗎？（無）如果沒有的話，我們今天六個子法都討論完畢，後續還有意見的話，可以到我們 JOIN 平臺上面，我們有作子法預告，提出相關的建議，今天會議就到這邊，謝謝。