「資通安全管理法子法草案分區座談會」第五場次
會議紀錄

時間：中華民國 107 年 8 月 15 日（星期三）下午 2 時 30 分

地點：蓮潭國際會館 101 會議室

【記錄開始】

主席徐嘉臨副處長：

各位午安，非常感謝各位來參加今天辦理的「資通安全管理法子法草案分區座談會」，今天開這個會的目的各位都知道，資通安全管理法在 5 月 11 日立法院通過，總統 6 月 6 日公布之後，後續很多施行上執行的方式或做法，我們透過子法的方式把細節在子法裡面作說明。目前子法已經作立法前的預告，從 7 月 9 月已經開始在網路上同步預告，我們今天也透過實體的會議辦理座談會，看看各位對於子法目前的版本有沒有意見、想法可以提出來。

首先會由我們的同事就現在這個版本子法的內容先跟各位作一個報告，之後會開放作討論，六個子法逐一討論。有發言規則，同仁做完簡報之後，再把發言規則作說明。今天的議程辦理方式是這樣，如果各位沒有意見的話，我就請同仁開始就資通安全管理法子法草案內容跟各位作一個報告。

王詠萱分析師：(略)

主席徐嘉臨副處長：

我們就開始今天的問題討論，在開始之前，我先跟各位說明一下，我們今天與會者的發言都會作逐字稿，逐字稿後續都會公布在網站上，這部分先跟各位說明一下，我們就開始針對六個子法逐一聽聽看各位有什麼需要調整或建議的地方。

第一個子法「資通安全管理法施行細則」，各位要發言之前先舉手，同仁會遞麥克風，發言之前先說明你的機構或機構的名稱，有沒有哪一位要提出建議的？

屏東縣政府：

資通安全管理法對上級機關跟監督機關有比較高責任工作的要求，需要作監督、演練、彙整資料、稽核等工作，而且本法能不能實施真正落

實，跟上級與監督機關的能力息息相關。以地方政府來看，要讓 2 個專職的資安人力已經有困難，事實上沒有辦法監督上百個機關，能否在法律或其他方面幫忙，針對上級機關監督設計資安專職人力之規定或資安單位的規定？以上。

主席徐嘉臨副處長：

你的建議是在哪邊設置專職人力？

屏東縣政府：

在子法裡面，或者是用各種方式，或許在子法裡面要設計專職人力的規定要考量很多，如果不容易的話，是不是其他的方式來推動監督跟上級機關的人力或單位的設置？不然的話，如果很少人但監督很多的機關，很難完善。

主席徐嘉臨副處長：

你說在法律裡面規定機關要設置專職人力這件事情？

屏東縣政府：

對，針對上級跟監督機關。

主席徐嘉臨副處長：

第二個問題。

財政部南區國稅局：

這邊想要請一個問題，「眾開講」7 月 9 日放的內容跟說明會附的內容好像不太一樣，你們放的是一個對照表，就以資通安全管理法施行細則草案第 5 條，對應到實際附的第 6 條，條文不一樣、內容也不一樣，不知道是放的版本不一樣嗎？

主席徐嘉臨副處長：

你說的是 7 月 9 日現在我們預告版本草案的內容？

財政部南區國稅局：

你們放的是對照表。

主席徐嘉臨副處長：

等一下我馬上上網查一下就知道了。

財政部南區國稅局：

分級辦法 B 級裡面「專職人員」，「眾開講」看到的是 1 人，可是你附的 B 級機關又是 2 人，到底我要看哪一版？

主席徐嘉臨副處長：

等一下我們查一下，還有沒有第三個問題？

高雄捷運公司：

因為本公司非屬於公務機關，但是可能是屬於本法關鍵基礎設施提供者，在整個配合事項中，希望能針對本公司或者是相關的非公務機關、機構完整提供相關的維護、資安相關的作業，能夠有合適的績效考評之後，適時由國家提供適當的補助或獎勵，讓我們能夠在這方面從事更多、更好精進的作為，畢竟我們跟一般受政府所補助或者編列預算，包含臺北捷運、桃園捷運、臺中捷運是不一樣的體制，所以我們有以上的請求，請參考，謝謝。

主席徐嘉臨副處長：

「眾開講」的部分我們等一下先查一下。

剛剛屏東縣政府提的部分，我們現在在資安專責人力的規範裡面是從A、B、C級機關作規範，A級要4個人、B級2個人、C級1個人，這個都是基本要求，機關如果要增加都可以，我們沒有說不可以，如果你認為有需要再增加的話，是可以再往上加的，這是先跟各位作一個說明。

高雄捷運公司的部分我們會帶回去參考，但是我不敢給你保證，法的施行如果都要透過政府來補助，我不知道其他的法在做法上是怎麼樣，但是我們回去再參考一下。

王詠萱分析師：

有關「眾開講」的問題，其實我們在 Join 平臺上面有兩個地方是在討論資通安全管理法，一個是第二階段座談會的時候，我們其實就有把第二階段的版本放到「眾開講」的網路，另外在這一次子法預告，第三次說明會的時候，我們有子法預告的網頁透過行政院公告轉到「眾開講」。因為版本混亂，所以我們在第二階段說明會、座談會完，那邊已經 mark 我們有新的子法預告，請大家一定到那邊討論，如果是7月9日子法預告的版本，理論上裡面的內容應該都是這一次座談會發開會通知裡面的內容一樣，如果這邊還是覺得不太確定的話，會後可以再看一下。

主席徐嘉臨副處長：

接下來有沒有其他的問題？

健保署資訊組高屏駐區：

有關自身核定等級的部分，我想請問一下，這邊要我們每 2 年提交自身的分類等級，第一個，有沒有報表？有沒有一個時間或什麼時候之前要提報？還是會來文通知？因為這個部分要提報給誰根本也不知道、什麼時候提報也不曉得、提報的格式跟內容也不清楚。

第二個，每 2 年提報一次，我們目前是寫給主管機關，主管機關在母法指的是行政院，在這邊分類等級的主管機關指的是什麼？譬如公立的醫療院所要給誰？像我們是屬於 3 級機關，我們要給誰？因為這個部分大家都第一次做，可能要規定更詳細大家會比較清楚，免得 1 月到 12 月都有人在提報自身的核定，以上。

主席徐嘉臨副處長：

謝謝，還有沒有第二個問題？

金門縣政府：

我這邊有兩個問題，第一個問題，像剛剛屏東縣政府提到專責人員，因為現在有分級，A 級有 4 個資安的專責人員，B 級有 2 個，我想屏東縣政府的意思，譬如 B 級 2 個專責人員似乎還不太夠，是不是有明文規範再增加這些資安的專責人員？因為 2 個人確實會處理不完。

第二個問題，金門縣是離島，離島的關鍵基礎設施這些的主管機關是地方政府還是經濟部？像自來水、臺電，這一部分好像還沒有那麼明確的規定他的上級機關是誰？以上兩個問題，謝謝。

主席徐嘉臨副處長：

有沒有第三個問題？

高雄市政府衛生局：

我們是屬於上級機關，底下有 41 個單位，我們是屬於 C 級單位，有管理到 B 級單位的醫院，如果依據子法來看，我們只有 1 個專責人員，以 C 級機關來講，大部分都不會有 1 個專責人員，請問上級機關在法條上主管機關會不會規範一個方式讓我們有機關去產生 1 個或 2 個的專責人員？

第二件事想向你們請教，ISO27001 看起來好像不是那麼好做，因為我們不用參加，但是起碼我們要作這些事情，有沒有一些表格讓我們參照、依循來做？謝謝。

主席徐嘉臨副處長：

請問你有 41 個機關是指？

高雄市政府衛生局：

我總共有 38 個衛生所、4 個醫院、1 個研究中心、再加上本局，總共有 42 個單位。

主席徐嘉臨副處長：

這三個問題先請同仁作說明，不夠我再補充。

王詠萱分析師：

首先回答健保署關於資通安全責任等級提報的問題，第一個問題，提報給誰？這個問題應該在第二個子法資通安全責任等級分級辦法有提到，如果是行政院的機構，向上是提報給行政院的直屬機關（構），向上是提供給衛福部，由衛福部彙整之後報行政院核定，這個在我們的子法裡面已經有作一些定義。第二個問題，後續我們是不是會統一發文？還是怎麼樣通知各機關提報？後續的做法可能請我們同仁再補充。

另外針對金門縣政府提到 B 級機關有 2 個資安專責人員可能會不夠的問題，其實 B 級機關的態樣蠻多的，對縣（市）政府來說它是 B 級機關，可是對中央的一個部會下面一個局處可能是 C 級機關，下面所管的公務機關數量不一樣，不過我們這邊 B 級機關原則上是以應辦事項的規定，來訂定這邊資通安全管專責人力需要的數目。對於像縣（市）政府這樣的機關，下面管轄比較多的公務機關這種情形，可能要請你們彈性去調整專責人員的數目來因應未來的業務。

同樣 C 級機關高雄市衛生局也是一樣，可能要跟長官稍微徵詢一下，C 級機關基本上就要配置 1 個專職人員，是不是需要更多？可能要看機關的業務來調整。

ISO27001 是否有表格？這一次我們會要求公務機關要提出資通安全維護計畫，行政院會提供資通安全維護計畫的範本，裡面有一些表格，供上級機關或中央目的事業主管機關參考，上級機關或中央目的事業主管機關可能會稍微修訂之後提供給他們的所屬機關參考，以上說明。

陳奕州科員：

這邊補充說明一下，剛剛有關提報的部分，在資安責任等級提報的部分，我們這邊原則上會先發文給各機關，格式的部分我們這邊也提供，所以這部分各機關在這方面應該不用擔心。如果是公務單位的話，應該之前都有提報過，格式的部分，我們這邊會統一提供責任等級提報的格式，以

上說明。

主席徐嘉臨副處長：

格式的部分當然比較沒有問題，因為現在機關已經在提報，這個不是因為法才新訂出來的，定期都有請機關提報更新資安責任等級這件事情，本來就有既定的表格。

至於時間要不要在法裡面規定？這個各位可以思考，有好有壞，定了以後就要在這個時間裡面做；如果沒有規定的話，還有一些彈性在，這個部分可以再聽聽各位的意見。如果各位傾向明文，我們就訂定隔年的 1 月就是要完成所有的提報，這樣時間上會很明確，各位就要謹記在心，因為在 1 月那個時間就會法遵的議題產生，所以這個部分可以再討論。

有提到 B 級機關或 C 級機關可能能力不夠，因為要定多少個人，其實還蠻難的，剛剛同仁也講，我們回去再考量一下，看看各位普遍在 B 跟 C 級機關裡面，平均所要管理的下屬機關他們的性質、規模、人數等等，我們再來看有沒有辦法作一致性的考量。再加多少人才是合理？這個是比較難去定的，這個部分我們再思考一下，看後續用什麼樣的方式再跟各位作一個說明。

各位針對這個子法還有沒有什麼建議？

高雄市政府衛生局：

主管機關有沒有想法協助我們培養一些專職人力？

主席徐嘉臨副處長：

還有第二個問題嗎？一個機關一次發言完，如果還有後續的問題，可以透過書面的方式，我們這次還是讓各位可以發言，之後可能要依照我們的發言規則，各位可以先思考你的問題，儘量一次性問完。

財政部南區國稅局：

因為已經多了一個 E 級，也沒有應辦事項，可是本法裡面還是屬於一個機關，還是要設資安長、資訊安全維護的組織嗎？

主席徐嘉臨副處長：

還有第三個問題嗎？如果沒有的話，我就先請同仁就這兩個問題作說明。

王詠萱分析師：

回答南區國稅局的問題，有關我們在這個法裡面定的 E 級機關有兩

種，這個也是分級辦法的問題，第一種，本身連資通訊環境都沒有；第二種，它的資訊業務是由上級機關兼辦或代管。針對第一種，可能連基本的資訊通環境也沒有的話，其實分級級別裡面規定應辦事項跟母法裡面的義務是不太一致的，所以這邊還要資安長或組織？這個我們再討論看看；第二種，所有的業務是由上級機關兼辦或代管的話，原則上就是由上級或其他幫他兼辦或代管的機關，代為執行他所有的資通安全義務，這個時候資安長或資安的組織可能就會回到兼辦或代管的機關作認定。

主席徐嘉臨副處長：

我補充說明一下，剛剛同仁講子法跟母法，其實它的規定是這樣，母法裡面本來就規定每個機關都要設資安長，原則上就是要設，不管是 A、B、C、D 級，每個機關都要設。因為現在多了 E 級機關，可能你的業務是由上級幫你代管，你自己沒有人員、也不需要維護任何的資通系統。如果是這樣的情形下，你的資安長就可以委託你的上級機關一起擔任資安長這樣的工作，這是可以的，應該可以作這樣的調整，但是必須在上級幫你們提報的資通安全維護計畫裡面敘明清楚。

剛剛高雄市政府衛生局有提到，對於專責人員是否有培訓的方式？其實資通安全管理法的目的就是希望機關設置專責人員，這個專責人員是真的具備資安管理的專業能力，所以各位可以看到整個法的設計，為什麼要配置資安專責人力？這只是其中一個目的，更重要的是他必須取得很多的訓練、證照、每年要有培訓，其實在這個應辦事項裡面都有規定，所以專責人力跟他基本能力的要求是必備的，必備的前提就是透過應辦事項非常多的教育訓練培養這樣的人、具有這樣的專職人力，所以它是連結在一起的。教育訓練的課程，在 A、B 級裡面如果要取得資通安全相關證照，這個證照目前由技服中心每年都會開固定的課，我們會發文給各機關要求你們可以派員來參加，只是現在你們派的人不見得是資安的人員或資訊人員，可能是有時間的人就來上；可是未來依據這個法，資安專責人員每年就是固定來上課，把他的能力每年不斷的培養、不斷的提升，這邊跟各位作一個說明。

接下來還有問題嗎？

中油公司煉製事業部大林煉油廠：

像剛剛講到訓練那一部分，像我們煉油廠算是關鍵基礎設施，也是 B

級單位，下面這一個問題，技服中心課程的名額始終都是透過總公司撥下來，但是我們煉油廠一直沒有這個名額，是不是未來真正要求煉油廠也需要資安專責人力的時候，能夠直接把這個名額指定給我們單位，而不是任由總公司去分配？因為總公司都把名額卡走了，變成我們現在 B 級連 1 個人 1 個課都沒有上，像這種狀況，我們真的不曉得這個名額要去哪裡要？而且在那個技服中心的報名系統上我們不能由自己報名，只能夠透過總公司去報名，這個問題是不是能夠請資安處一併協助解決？

主席徐嘉臨副處長：

謝謝。

高雄市立凱旋醫院：

根據本法第 4 條第 1 款：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」這個部分我在裡面的規則仔細看過，並沒有很明確的告訴我們，怎麼樣才叫做「完善之資通安全管理措施」？第三方的驗證範圍應該定多大？我們是否可以從任何管道取得相關的細項？

主席徐嘉臨副處長：

接下來還有沒有第三個問題？

義大醫療財團法人義大醫院：

這邊有指設置專責人員，但是目前所指的專責人員應該都是屬於 ISO27001 的主導稽核員，但是主導稽核員其實在整個資安制度裡面是屬於稽核而不是屬於防護，對於整個資安的防護裡面到底政府有什麼資源？其實這方面的人非常難取得，即便是具備這樣的能力的廠商不多，在政府的資源上有多少可以分配？在 93 年實施電子病歷的時候，當時政府有提供很多資源來協助機構取得主導稽核員的訓練跟資格，這次不曉得有沒有這個資源可以投入？

主席徐嘉臨副處長：

這三個問題先請同仁先回答。

王詠萱分析師：

首先針對中油大林煉油廠的問題回答，大林煉油廠是屬於特定非公務機關，在我們分級辦法應辦事項裡面針對特定非公務機關資通安全專業證照的要求，只要求持有資通安全專業證照，沒有特別要求需要具備資通安

全職能評量證書，這邊先簡單說明一下。至於公司內部的治理方式，可能還是需要內部來協調。

第二部分，有關於細則第 4 條第 1 項第 1 款，在機關進行委外的時候，要如何確認受託者已經具備了完善的資通安全管理措施或通過第三方驗證的範圍？首先第三方驗證的範圍就是根據你受託業務的範圍，哪裡是屬於受託業務的範圍，在那個業務範圍就是他需要通過第三方驗證的範圍。我們這一條是要求具備完善的資通安全管理措施或第三方驗證，第三方驗證只是證明他有完善管理措施的一個條件而已，如果比較小的受託者他沒有通過第三方驗證的話，機關要根據委外業務的性質去檢視受託者是否具備完善的措施，譬如內部資通安全的管理、對一些管理面或技術面的措施，視這個專案本身的性質來確定是否已經達到專案需要的水準。

有關於專責人員是主導稽核員稽核或是防護？其實資通安全專業證照有很多，除了 ISO27001 主導稽核員以外，還有針對技術面向的證照，我們在專責人員證照要求上，並沒有一定要求主導稽核員，所以看你們需要什麼，尤其是醫院，可能醫院內有一些特別的資安規範需要特別遵守，這些證照原則上都可以，可能要依照這個需求來訓練。

主席徐嘉臨副處長：

我補充說明，第一個問題是中油公司的問題，因為你們是關鍵基礎設施，不是屬於公務機關，資通安全專業證照及職能訓練證書這一欄，關鍵基礎設施是不用取得資通安全職能評量證書這一項，它是只針對公務機關。中油在這裡面的角色不是公務機關，是屬於關鍵基礎設施提供者，所以原則上可以不用取得。我不知道經濟部在轉發文的時候有沒有轉給你，你們有機會就可以來上，在這個法裡面也沒有強制要求。

第二個問題是高雄市立醫院的問題，細則第 4 條所謂「具備完善之資通安全管理措施或通過第三方驗證」的範圍到底在裡面？就是你委外的範圍，如果你委外的公司業務範圍不是只有光做你這個，其他的部分不用受這個法的管制，你委給他的範圍裡面必須確認是有好的管理措施或者通過第三方驗證。什麼叫做「具有完善之資通安全管理措施」？就要看你委外的範圍是什麼，因為資通安全的委外業務還蠻多種的，你可能是委外開發系統、可能是一個 SOC 系統、可能是一個落點掃描、可能是滲透測試，那個樣態是不一樣的，就看機關裡面的需求是什麼？

我舉一個例子，假設是委一個 SOC 系統，你可能要知道他幫你蒐集過去這些 log 怎麼作處理、怎麼作保護，這個可能是你應該關心的，這可能就是你跟他合約簽訂的時候就應該放進去，機關就要思考，哪些是基於機關的特性、遵守機關內部資通安全政策的前提之下，這些基本的要求就要放進去。或者他有通過第三方驗證，當然這個是「或」，並不是強制要求一定通過第三方驗證，我只是先舉一個 SOC 例子，假設你是委一個資通系統開發，可能就要要求他的開發環境是一個隔離、乾淨的環境，沒有跟他們內部辦公室系統有任何的網路連接，必須確保你的網路開發環境是乾淨的，沒有任何惡意的程式或者其他病毒入侵的可能，我只是舉個例子，我想這個會有不一樣，這個部分就是端看每個機關在委外的形態、需求、等級，可能都會不一樣。

剛剛義大醫院提到的問題，你們的主管機關是衛福部，你可以跟他問問看。接下來還有沒有其他的問題，如果沒有的話就進到下一個子法。

第二個子法「資通安全責任等級分級辦法」。

財團法人電信技術中心：

我想請教一下，剛剛有講到資安專職人員的部分，剛剛一直在強調證照或者一些證書的部分，這邊指的專職人員是不是只有公家機關才需要 follow 這樣的人員配置？

因為我們的業務範疇，有檢測、有資安還有 NP，譬如我們某一項業務的責任等級可能被歸類到 B，甚至到 A，因為它只是我們眾多業務的其中一項，因為某一項業務它涉及的範圍是屬於 CI 提供者的話，是不是我們整個中心都要 follow 這樣的制度，去制定相關的計畫或機制嗎？

主席徐嘉臨副處長：

你舉個例子來說。

財團法人電信技術中心：

假設我們中心有攜碼（NP）的業務，這個有可能有跨電信業務，有可能會被編到 A 或 B，我們其他也業務有設備的量測或是一些資安的業務，可是這個都是屬於比較特定範圍內的，不會有跨全國性的，如果我們有其中一個業務可能會跨全國性，這樣的話我們中心怎麼訂定責任等級？因為這樣的業務，整個中心就要 follow 這樣的作業去定我們的維護計畫或應變機制嗎？

主席徐嘉臨副處長：

你現在講的跨全國性業務是指現在資安責任等級 A 級裡面的哪一條？

財團法人電信技術中心：

就是攜碼業務，通訊的部分。

主席徐嘉臨副處長：

可是你們也沒有像電信公司提供通訊服務。

財團法人電信技術中心：

電信公司會提供我們某些民眾要進行攜碼作業，會需要通報我們，這只是我們眾多業務的其中一項，我們怎麼去看待這樣的業務？

主席徐嘉臨副處長：

看起來那個應該不算是 A 級機關的業務。

財團法人電信技術中心：

怎麼去評定它？

主席徐嘉臨副處長：

等一下請我們同仁說明一下 A、B 的制定方式。接下來有沒有第二個問題？

屏東縣政府財稅局：

剛剛很多長官提到是資安專責人員的設置，譬如我們的人事人員在行政院有一個「行政院所屬各級行政機關、學校事業機構人事人員員額設置標準表」，這個資安專責人員是不是能夠參考？因為它有分中央跟地方，還有分機關的員額是 50 人以下或者 50 人以上，取它的比例，變成人事人員的標準。在資安專責人力是不是有機會用這樣的標準劃分？譬如 B 級機關有大有小，同樣都只設置 1 個人，確實蠻奇怪的，請資安處參酌。

主席徐嘉臨副處長：

還有沒有第三個問題？如果沒有的話，就先請我們同仁就剛剛的問題說明一下。

陳奕州科員：

首先回應財團法人電信技術中心的問題，第一個問題是有關專責人力配置部分，母法裡面的要求，專職人員主要是針對公務機關的部分，財團法人是屬於特定非公務機關，所以配置是專責人力，在這邊說明一下。本法有關資安責任等級分級的部分，主要是考量個資的持有數量還有業務的

屬性、你提供的服務是屬於全國性、或者提供資通系統的服務是屬於全國性的共用或區域性共用的資通系統來作認定。以財團電信技術中心剛剛舉的攜碼業務的話，這個部分應該不會被我們分在 A 級的部分，這邊是指關鍵基礎設施提供者，如果是財團法人，應該不算是關鍵基礎設施提供者，所以在這部分的認定上，應該不會是A級。

有關中心內部這個業務如果是被認定為特別重要，可能會分類為 A 級，其實我們在資安責任等級分級辦法第 3 條 7 款有提到，公務機關、特定非公務機關如果有特別必要，針對內部的單位可以另外作分級，可以避免跟中心的等級掛在一起。以臺大為例，臺大可能是 B 級，底下的臺大醫院是屬於臺大的內部單位，可以依照他實際上的業務性質，另外提報他的資安責任等級，這部分補充說明。

主席徐嘉臨副處長：

不過原則上，不管是關鍵基礎設施或者是公務機關的業務有各個 A、B、C 級表列的項目，你就是那個機關的等級，既使它只是你其中一項業務，你就是那個等級，所以後續任何的防護措施就是要比照 A 級的方式去作。剛剛我們同仁只是特別補充，除非你的組織非常的龐大，很多的子公司，可是你關鍵的業務是在母公司做的話，可能母公司資安責任等級還是要列為表列裡面所列的，因為表列有這一項，所以母公司就會是那個等級。以電信技術中心組織的性質，應該不至於被列在A級。

第二個問題，屏東縣政府財稅局提到，是否比照人力人員有一個比例劃分建置？其實昨天在座談會上也有提過類似的概念，譬如我的人是 1000 人，用 20%去作人力的配置；但是我要強調的是，資安責任等級的A級跟機關裡面的人數不見得有 1 對 1 的直接關係，A、B、C、D 的等級劃分是看你這個組織裡面負擔保有機密的大小，國家機密、個人資料或者服務的可用性等等，它的重要等級來區分，而不是針對機關的大小就必須配置更多，不是用這樣的角度在分。所以剛剛這樣建議我們可以回去思考看看有沒有參採的空間，現在可以回答的是，它的關係不是這麼直接，但是我們可以帶回去思考一下。

接下來有沒有其他的問題？

屏東縣萬丹戶政事務所：

我想請問一下，戶政事務所有部分有處理到全國性的民眾資料，它算

不算在A級？

還有另外一個問題，戶政事務所有分有主機點跟沒有主機點的，他們的等級會不一樣嗎？

主席徐嘉臨副處長：

還有嗎？如果沒有的話，這個部分請同仁先回答。

陳奕州科員：

有關屏東萬丹戶政事務所提到關於全國個人資料，在法條我們有注意到，敘述部分可能會再作一些調整。這邊特別說明，以屏東萬丹戶政事務所為例，如果你們有主機保有民眾的個人資料，是屬於區域性或地區性的話，會分在 B 級；如果你們沒有主機，只有設置主機伺服器，應該是屬於 C 級。如果主機點有保有個人資料的話，原則上會被我們分類在 B 級的部分，作以上說明。

主席徐嘉臨副處長：

這樣有清楚嗎？如果沒有問題的話，我們就往下一個子法。

第三個子法「資通安全事件通報及應變辦法」。有沒有哪一位要發言的？

屏東縣政府：

這個子法第 6 條規定，應該依時間完成損害控制，完成之後 1 個月內要送改善報告。建議 1、2 級的資訊安全事件就不用送改善報告，比較嚴重的等級才要送改善報告，不然我推測有可能會造成機關的承辦人不知道怎麼寫改善報告，或者覺得麻煩，就會減少資訊安全事件的通報。當然沒有通報是機關承辦人的責任，可是我們務實來看，如果真的每個事件都要送改善報告，以後資通安全事件的通報量會減少，以上。

主席徐嘉臨副處長：

謝謝，有沒有第二個問題？通常子法公務機關跟特定非公務機關建議都會非常多，各位可以再仔細看一下，如果沒有的話，我請同仁說明一下。

王詠萱分析師：

針對 1、2 級事件的改善報告，因為現在事件通報公務機關都是在技服的網站上通報，針對 1、2 級事件後面網站在改版的時候，當他在作事件結案通知的時候，可能會簡單填一些欄位，按提交的時候，就會送連改

善報告一併提交。

主席徐嘉臨副處長：

還有建議的嗎？

中油公司煉製事業部大林煉油廠：

因為我們的組織是總公司、再來是事業部、再來是大林廠，這樣分層的結構，但是我們可以看到一開始只有 1 個小時，想請問這 1 個小時之內是要通報到哪個層級？是到總公司？還是總公司出去到國營會?到經濟部？萬一我們沒有在 1 個小時內達到的話，如果真的要懲處，是要在哪個時間點懲處那個階段的問題？因為如果這樣層層推下來，像我們這種下級單位的下級單位有多少時間可以來通報這件事？

主席徐嘉臨副處長：

有沒有第二個問題？

高雄捷運公司：

針對特定非公務機關知悉資通安全事件 1 小時之內要依中央目的事業主管機關指定的方式進行通報，這個部分對我們這些通報的核定層級，在 1 個小時之內到底要到哪一個層級？核准之後再請通報，是由我們自己組織內部來作確定就可以了？還是這部分的內容也需要陳報上到中央目的事業主管機關確定核准之後才可以實施？還是由我們自行內部作確定就可以了？這邊想請教一下。

主席徐嘉臨副處長：

有第三個問題嗎？

義大醫療財團法人義大醫院：

我想請教一下，因為針對資安事件的通報，針對各級事件，其實我們對於主管機關他們的審核有分事件層級的不同，定不同等級事件應該在幾個小時之內完成應變，回覆給相關的機構等等。但是就我們發生這些資安事件的單位、這些機構、機關，他們通報的時間全部都是規定在 1 個小時，通報應該要具備基本的內容在辦法草案第 3 條有規定，事實上因為這些事件我們有一些要通報的項目，可能會依照事件的不同，複雜性有不一樣。我們比較擔心會不會有一些事件比較困難在 1 個小時之內完成這些資訊的蒐集，回報到機關那邊？所以是不是有機會針對不同的事件的層級，去訂定個別比較適合通報的時效？

主席徐嘉臨副處長：

這三個問題先請我們同仁作簡單的回答。

王詠萱分析師：

首先回答大林煉油廠的問題，1 個小時要通報到哪？依照我們的子法，1 個小時就是要通報到中央目的事業主管機關，不管是大林煉油廠知悉或事業部知悉或是總公司知悉，就是在知悉後 1 個小時之內要通報中央目的事業主管機關，機關內部要怎麼樣因應這個法、要怎麼樣整合？可能是組織內部自己的問題，但是就是要配合法的義務。如果沒有達到的話，因為中油是特定非公務機關，在我們的資安管理法裡面，針對特定公務機關，如果沒有正確依照第 18 條通報的話，會有罰則的問題，請很慎重看待這個問題。

針對高捷的問題，你們也是向中央目的事業主管機關通報，但是機關內部要審核要到哪一個層級通報？這個內部自己決定就可以。

針對義大醫院的回覆，其實我們事件通報是求快，並不是求完整，所以希望各機關在第一時間知悉資安事件的時候，能夠快速的先把資安事件反映，由上級機關或主管機關看看這個範圍是不是需要特別的協助。第 3 條規定一些通報的內容，因為內容都是很簡單的內容，並不會要求大家要寫很長，只要簡述就好，求快、先通報。如果事後發現通報之後有一些內容要改的話，是可以依照第 4 條第 2 項續行通報，可以修改通報的內容，所以第一時間只要簡單填、求快就好。

主席徐嘉臨副處長：

原則上通報就是發現之後，1 個小時之內趕快跟你的中央目的事業主管機關通報，你的責任就了了。網站上要提的內容其實是非常簡單，但是中央目的事業主管機關跟你們的上級主管機關的通報內容可能會再有另外指定的方式請你們通報，那個內容後續都會找你們作一些了解，後續在跟他們討論的時候，就可以溝通一下，到底在第一時間該通報什麼樣的內容給你們的中央目的事業主管機關。

義大醫療財團法人義大醫院：

我想針對剛剛的回應進一步作一個釐清，因為第一個目的就是要求快，趕快反映相關的機關，剛剛有提到，如果後續我們要再進一步補充，或者有一些通報的內容，我們是要準用第 4 條第 2 項的規定變更我們通報

內容嗎？因為第 4 條第 2 項的規定，資安的安全事件責任等級變更的時候，公務機關應依前項的規定續行通報。這個是在規範資安責任等級變更的時候可以續行通報。也就是說，即便我們的資安等級並沒有變更，可是如果我們的通報的內容有要作一些補充或一些調整的話，我們可不可以準用第 4 條第 2 項的規定？是這樣的意思嗎？

主席徐嘉臨副處長：

你要變更的內容會是什麼？除了等級要變更之外還會有什麼？因為一開始通報通常會是發生的時間、狀況的描述，這個應該大概都不會再變了，除了等級的評估，這個幾項大概都不會再作變動，我們只是考量到，可能當時評估是 2 級，後來發現這個事件擴大，比你想像還要嚴重，可能需要升一個等級，所以就會透過這個方式調整當時報的資安責任等級。

義大醫療財團法人義大醫院：

我們剛剛提出來的問題是針對第 3 條的通報內容，萬一有一些事件複雜度比較高，怕來不及在 1 個小時之內能夠有完整通報的內容，所以我剛剛第一個問題的時候提到，是不是有機會能夠針對不同等級資安事件它的通報時效有一些不同的規定。剛剛主辦單位的回應，如果有這樣的情形，我們後續有一些繼續作補充的話，可以用同樣這個辦法第 4 條第 2 項的規定作補充說明。所以我才針對第一次發言作一個釐清，因為第 4 條第 2 項是針對事件等級變更的時候才可以作，主辦單位的意思是不是我們可以準用這個規定？因為其實規範的事項不太一樣。

主席徐嘉臨副處長：

原則上只有等級變更才適用第 4 條第 2 項，第一次作通報的時候，內容就是在第 3 條裡面已經規定，就是照這個內容作通報，其實內容就在這邊，我不知道你後續有可能要補充的內容是什麼，如果這些補充的內容或許在第一次就應該講清楚的，我們可以建議再放進來，但是目前看起來這些內容應該是足夠的。

第二個，因為你們是醫院，未來是衛福部會指定你們通報的方式跟內容，他們可能會參考這個部分再去定你們跟他們之間的通報內容，所以這個後續可以再跟他們作進一步的了解。

還有其他的問題嗎？

中油公司煉製事業部大林煉油廠：

我回應一下剛剛的回應，我們現在面對的問題是在應變通報網站上我們煉油廠連帳號都沒有，都只能透過總公司去回報，所以才會有 1 個小時的問題，聽起來像是公司自治，之前我們有同仁反映過，既然要求我們 1 個小時內通報，像我們這種直屬的，是不是直接給我們一個帳號，這個 1 個小時的責任就由我們這個單位自己承擔，就不用透過總公司再去應變通報網站？今天以中油公司的規模來講，總公司承辦的人必須面對全臺灣島上所有中油公司的應變通報，基本上他的壓力很大。所以才說像我們這種，能不能之後給各自單位一個帳號能夠填通報應變網站，由各個單位自行去負責？

主席徐嘉臨副處長：

有沒有第二個問題？如果沒有的話，我先說明一下，因為中油的主管機關應該是經濟部，經濟部從去年開始，開始就你們對他通報應變機制怎麼建立、資安的情資怎麼作分享，就是 ISAC 這件事情，其實他們都已經在進行中，所以未來的通報方式你應該是對他。

至於他們怎麼把這個訊息接到主管機關這邊來？是我們會去跟他們談的，所以以後你就是 follow 他指定方式去作通報，不見得會到我們現在的通報網站通報。還有其他問題嗎？如果沒有的話，就接著下一個子法。

第四個子法「特定非公務機關資通安全維護計畫實施情形稽核辦法」。

高雄捷運公司：

我們是屬於特定非公務機關，在受稽核的時候內部會有承辦的單位，承辦單位需要具有資訊安全這方面背景的單位來接受或承辦受稽核的業務嗎？還是不一定需要有這些資訊背景的單位來承接？這邊想請教一下。

主席徐嘉臨副處長：

還有第二個問題嗎？我先回答一下高雄捷運公司的問題，承辦單位需不需要有資訊背景？主管機關針對特定非公務機關作資通安全維護計畫實施情形的稽核時，主要目的是要希望看你之前提的資通安全維護計畫裡面說的、你打算怎麼做跟你後面所做的有沒有一致，可能會有一些稽核的辦法，需要有人配合回答他的問題，或者會看一下你們的機房實地的場地，或者捷運公司有儀控的系統，大概就會看這些東西。

至於你說承辦單位的問題，我現在沒有辦法回答承辦單位負責的角色

是什麼？他只是作行政文書？還是在維護你們整個捷運儀控系統的單位？這個部分不是我們關心的，我們也不會要求未來受稽核時他的承辦單位是誰，這個你們可以自己安排，我們只是希望你們去看一下之前提的資通安全維護計畫這些想要做的東西，是否有按照你所說的去做。還有沒有要提出建議的？沒有的話，接著下一個。

第五個子法「資通安全情資分享辦法」。有哪一位要發言的嗎？

健保署資訊組高屏駐區：

我請教一下有一些單位的主管機關，因為在這個辦法並沒有寫得很清楚，我只知道母法指的是行政院，有一些機關可能上面的頂頭上司一大堆，到底主管機關要到那邊？像有一些機關可能業務都跟高雄市政府或跟中央機關都有一些關係，這個時候主管機關要找誰？「主管機關」寫這樣子實在是比較模糊。

主席徐嘉臨副處長：

還有沒有第二個問題？沒有的話，我先請同仁針對剛剛的問題作說明。

王詠萱分析師：

在資通安全管理法跟相關子法裡面，只要看到「主管機關」就是指行政院。

主席徐嘉臨副處長：

我再補充說明一下，假設你們是關鍵基礎設施，你們面對的是中央的目的事業主管機關，在這個法裡面的角色大部分要負責主管業務或者像行政院主管機關、中央目的事業主管機關，大概都是中央的角色；地方政府原則上就是屬於一般的公務機關，就是必須履行你的法遵責任，原則上的劃分是這樣子。地方政府唯一有一個要擔任主管機關就是地方政府的角色，因為必須幫所屬的機關提報資通安全責任等級，所屬機關的資通安全維護計畫也必須送交給他作一些審查。如果其他屬於特定非公務機關的部分，管理的責任大部分都是落在中央目的事業主管機關。請問各位還有沒有其他的問題？如果沒有的話，我們到最後一個。

第六個子法「公務人員所屬人員資通安全事項獎懲辦法」。各位有要提出問題或建議的嗎？

屏東縣政府：

因為這個子法的第 1、2 條有寫到，公務機關就其所屬人員辦理業務涉及資通安全事項，因為條文內容有提到「辦理業務」，建議是不要講「辦理業務」，界定比較模糊，這個獎懲對象是對於機關內所有人員，不是只有針對資安業務的人員，有時候機關的人員違反資安的事項，像是在發生電子郵件演練的時候每次都失敗，或是隨意安裝盜版軟體導致惡意程式的現象，這個情況就很難說是辦理業務的資安事項，怕之後懲處的話會導致有爭議，以上。

主席徐嘉臨副處長：

還有第二位要發言的嗎？如果沒有的話，我先簡單回應剛剛的問題，這個文字修正建議我們回去再看一下，不過你剛剛提到一般的人員點 email 或上網，如果他已經違反你們內部的規定，其實就可以適用第 4 條第 3 款：「其他違反依本法授權訂定之相關法令，或機關內部規定之行為情節重大者」，本來就可以適用這一條去作相關的懲罰，如果就你剛剛的案例，在作懲罰上應該沒有太大問題

王詠萱分析師：

你的問題第二階段座談會也有提出來，我們這邊也有跟法規會討論一下，我們會加「辦理業務」這個限制，主要是稍微限縮一下，如果機關所屬人員只要涉及資通安全事項就獎懲的話，不是在「辦理業務」這件事情，恐怕牽連很廣。

屏東縣政府：

可能在機關內。

王詠萱分析師：

在機關內部做的時候，應該都算是你的業務，可是如果把這個「業務」拿掉，我怕解釋上或許平常在公務的業務之外都會被解釋進來，會牽連太廣。所以我們這邊後來討論的結果，還是把「辦理業務」留下來，這個「辦理業務」可能會解釋公務人員在機關內公務的業務都算，以上。

主席徐嘉臨副處長：

還是其他要提問或建議的嗎？如果沒有的話，我們今天會議就開到這邊，各位後續如果有一些建議，也可以上現在子法預告的網站提問，今天我們會議就到這邊，謝謝各位。