資通安全管理法子法草案分區座談會（第三階段）（中區場次）會議紀錄

時　　間：中華民國107年8月14日（星期二）下午14時30分

地　　點：國立國家公共資訊圖書館第二會議室（台中市南區五權南路100號）

出席人員：（略，如簽到單所載）

【記錄開始】

主席徐嘉臨副處長：

各位大家午安，牆面上的時鐘比較慢，我看一下時間其實已經過了2點30分，所以我想會議就開始。

今天開這個會議的目的，其實是就現在已經預告有關《資通安全管理法》中子法的預告版本，請各位提供一些建議。

這一個版本其實從今年年初到現在，陸續大概開了十一場的座談會，我們針對這幾場座談會裡面，將聽到各位的意見調整成現在的子法，即現在預告的版本其實是經過前幾場分區座談會討論後，蒐集各位的意見、結果調整而成的。

我們現在就這個版本，看各位還有沒有什麼建議需要再提供的？這個版本其實之前隨著開會通知的時候就已發出，所以這個子法草案的內容，各位手上應該都有。

今天議程作業進行的方式會請同事就現在調整版本的子法來作簡要地說明，我們再開放各位提供建議，看有沒有請教或是請我們再作調整的地方，歡迎各位再提出說明。

等一下會有發言規則，等到同仁簡報完之後就會接續說明發言的規則，等一下發言的時候請各位遵照發言規則進行發言。

另外，今天會議上每位發言者都會做成逐字稿，之後會公布在網站上，這部分也再次提醒各位。

請詠萱開始進行簡報，簡報完之後再說明一下發言規則，謝謝。

王詠萱分析師：(略)

主席徐嘉臨副處長：

請說明一下發言規則。

王詠萱分析師：

今天子法的草案一共有六個子法，會依照剛剛的報告順序逐一進行討論，依序是「《資通安全管理法》施行細則」、「資通安全責任等級分級辦法草案」、「資通安全事件通報應變辦法草案」、「特定非公務機關資通安全維護計畫實施情形稽核辦法草案」、「資通安全情資分享辦法草案」、「公務機關所屬人員資通安全事項獎懲辦法草案」。

發言規則如下：請各與會單位推派一人發言，發言次數，每一個子法以一次為限，每次2分鐘為限。發言單位如果有其他的意見，請以書面方式補充，主辦單位會後處理；書面意見提供單剛剛已經有提供給各位。

主辦單位原則上是每三個提問之後進行回應，回應一次是4分鐘，回應的重點會以子法條文的釐清事項說明為主。

會議紀錄會後公布於國家資通安全會報網站，請各機關同仁發言的時候，可以先提一下自己的單位及姓名。

主席徐嘉臨副處長：

我們現在開始請各位提問，針對六個子法的第一項，《資通安全管理法施行細則草案》，如果想要發言的就請舉手，麥克風就在面前，各位 on 起來之後就可以開始發言，有沒有哪一位要先發言的？

農糧署：

農糧署第一次發言，針對這個細則草案，我只有看到一個，第12條有一個缺漏字，「特定非公務機關業涉及數『個』中央目的事業主管機關」，缺了一個「個」字，小地方而已，我先針對這個發言，謝謝。

主席徐嘉臨副處長：

謝謝。

各位對於施行細則有沒有建議？（農糧署代表）可以一次講完，一個機關原則上是發言一次，沒關係。

農糧署：

不好意思，農糧署第二次發言，剛才那一點我事先看到的。

另外這點是在翻的時候（看到），第6條第1項第12款「公務機關所屬人員辦理業務涉及資通安全事項之考核機制」，因為這個機制必須要列在資通安全維護計畫裡面，這個考核機制一般公務人員可能有公務人員規定

相關考核辦法之類的，因此這邊講到的是有別於公務人員適用考核辦法之外，特別針對資安部分來作考核機制。

在這一次報告裡面還有最後一個法，即「公務機關所屬人員資通安全事項獎懲辦法草案」，這個考核機制是獎懲辦法及公務人員應該適用的獎懲辦法之外，再訂一個考核機制？又或是可以參照「公務機關所屬人員資通安全事項獎懲辦法草案」之類的？以上。

主席徐嘉臨副處長：

謝謝，我再蒐集第三個問題。

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我請詠萱先簡單回答。

王詠萱分析師：

首先針對第12條的「『數』中央目的」，我文字可以看一下要怎麼樣修改，是不是修成「『數個』中央目的事業主管機關」。

針對第6條第1項第12款的考核機制及獎懲辦法，其實獎懲辦法這次修改之後，是希望各機關能夠自行修正機關內部的獎懲辦法，跟「公務機關所屬人員資通安全事項獎懲辦法草案」來接軌，因為這個獎懲辦法裡面只有訂定獎勵及懲處項目，額度要回到各機關的獎懲辦法去訂定。

考核機制應該各機關針對平時考核項目，要如何在平時考核中考核公務人員，事項可能是參考獎懲辦法。另外，各機關如果自行還有一些其他的規定，也可以寫在裡面，以上說明。

主席徐嘉臨副處長：

簡單來講就是不用另訂，訂在現在的人事考核制度裡面就可以了，只是現在人事考核裡面或許沒有特別針對資安事項，可能回去可以解釋一下，把一些資安的事項加在「獎」或「懲」的事項裡面，這樣就可以了，所以再次強調，不用另外訂一套機制。

還有其他的問題嗎？

如果沒有的話，就直接到第二個子法，是「資通安全責任等級分級辦法草案」。

苗栗縣政府稅務局：

主席、各位長官，苗栗縣政府稅務局發言。對於資安等級分級辦法第5條，B 級的部分在我這邊來看，像稅務局當然個資一定是屬於區域性、是屬於 B 級，但是像稅務局整個系統就像戶政一樣，我們系統是向上集中，我們的系統部分就比較趨向於 C 級，像有委外開發，但針對核心系統來講是屬於稅務，因此這個部分在 B、C 級當中，我們不是很確定我們是屬於 B 或 C 級，雖然我們有機房，但核心稅務的主機已經在財政部那邊，因此我們有這一個疑惑，其實 B、C 級做的東西有時差滿大的，因此有這一個疑問，謝謝。

主席徐嘉臨副處長：

謝謝，第二位要發言嗎？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

這個辦法當中的附表有提到資通安全專責人員，公務機關有特別寫「須以專職人員配置之」，特定非公務機關就沒有這一句話。我們這邊想要請教，「專職」與「專責」的區分是什麼？「專職」人員跟「專責」人員的資安工作範圍與項目是什麼？以我們公司現在既有的 IT 是資訊人員與 OT 即工控系統操作人員的工作項目有何區分？

第三，「專責」人員的意思是不是可以以既有的資訊人員或者是工控系統操作人員去兼任，因為長官在配置人力時會向我們詢問到這塊。

主席徐嘉臨副處長：

謝謝，有沒有第三位？

苗栗縣議會：

資安等級的分級制度當中列為 C 級，C 級這邊有涉及如果有建資通系統，那就算 C 級，鄉鎮市民代表會裡面，其實我們都有 server，我們的網站只是一些資訊的揭露而已，我們算有 server。

等級這樣區分的話，公務機關至少都是 C 級以上，資安的人力配置上，應該要考量機關的人力配置，像我們人全部是二十四個，資訊人員幾乎是零，我們如何專責這個部分？因為要設專責的話，連資安長都設不出來，因為我們的承辦人員是約僱人員，如果列為 C 級的話，整個業務的推動上，人力問題要考量，謝謝。

主席徐嘉臨副處長：

謝謝，這三個問題先請詠萱回答。

王詠萱分析師：

我先回答台灣中油有關於「專責」及「專職」人員的問題，「專責」人員是負責資通安全業務的同仁，那就是「專責」人員，「專職」人員是更進一步指該位同仁主要負責資通訊業務，原則上不會兼任其他與資安業務無關的工作，可能有一些少數的其他交辦事項，但是大部分的業務還是以資安業務為主，我們會定義為專職人員。

公務機關的「專責」人員應該要「專職」人員配置，特定非公務機關的話，我們沒有要求要專職人員，只要專責就好。至於怎麼樣的人員算是專責人員？簡單來說，他的工作跟資通安全有關，如果有一些資安事件的話，資通業務由他來負責，就算專責人員，主要是看業務性質來訂定。資訊人員或是工控系統操作人員是否算專責人員，還是要看擔任的資訊業務是不是跟資安有關。

針對苗栗稅務局詢問稅務局的資訊系統是向上集中，如果有機房、server 的話，算是 C 級機關或者是 B 級機關？雖然稅務的資訊系統是一貫體系的系統，但 server 放在一個機房裡面，你的那一台主機會不會有一些民眾的個人資料，比如本身主機當中還是存放一些區域性個資的話，我們原則上就會把這個機關定義為 B 級機關，因為就必須要有一定資通安全事項來進行防護。

有關於縣議會問資訊系統的問題，基本上如果有網站伺服器的話，我們也會把它算成 C 級機關資通訊系統之一；有關於人力配置的話，基本上 C 級機關因為有網站，因此在應辦事項裡面，我們會有一些對應的要求。這部分我們會建議後面看是不是用資訊集中的方式，是不是可以把伺服器其中在其他的機關裡面，如果還是設有網站的話，原則上就是 C 級機關。

主席徐嘉臨副處長：

我這裡補充說明一下，有關於苗栗稅務局剛剛提到，如果以目前責任等級看起來你們應該是 B 級機關，你剛剛說如果你們所有的系統或 data 全部放在財政部的財政資訊中心，當然你就可以註明一下機關裡面沒有所有苗栗縣政府民眾的財務資料、財稅資料，這是第一點。你也沒有提供所有民眾來線上申辦財稅的任何服務，這你都要講清楚。如果完全沒有，你們這邊完全不提供這樣的服務，都是由財政部財政資訊中心統一提供的話，

這樣沒有問題，你們就可以不用列 B，原則上就是這樣，但你自己必須要檢視清楚是不是符合這樣的條件。

第二，我剛剛提到台灣中油到底是「專責」或者是「專職」，剛剛同仁有解釋過。至於，你們是 OT 或者是 IT 的人擔任，這個我們沒有意見，你們可以自己調配，但是以中油來講是關鍵基礎設施，重要是公共系統的維護，應該是納為關鍵基礎設施最主要的目的，防護重心應該要放在關鍵基礎設施，你應該配置什麼樣的人來當成你的「專責」或「專職」，這是你們內部要去思考的。

接著是苗栗縣議會的問題，C 級機關就是要配置一個專職的人力，這是法裡面必須要求的。尤其是在地方政府，其實我們每次在做攻防演練的時候，地方政府的網站通常是弱點，老實說各位看到你們被攻擊的紀錄就知道，其實很多被攻擊成功，大部分都是地方政府的網站上，通常是防護沒有做到位。

所以不管你們是只有內部系統或者有外部系統，即使是外部系統，只要有弱點沒有修補好，甚至在開發的同時沒有注意到安全管控措施，其實就常被駭客利用作為攻擊別人的跳板工具，因此各位必須要注意。不是現在沒有做而代表未來就不用做，未來法通過之後，因為有感於這樣的風險是需要因應的，因此才說各位要配置一個人力，原則上是這樣，麻煩各位配合一下。

未來的資安人力，C 級機關應該是一個人力，B 級是兩個人力，A 級是四個人力，在未來人力的配置上會有過度性的做法給各位建議，我們會後續提供給各位。不過各位應該要向內部爭取，如果未來屬於 A、B、C 級機關配合專職人力的時候，事實上這個時間點，你們開始啟動內部人力配置作業，依人事行政總處的規定，未來人員總額度上、公務員總額度上是不太可能大幅增加的，因此優先要請各部會或各地方政府在自己機關的員額上作優先配置，這部分先作這樣的說明。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

澄清一下，如果目前 OT 的人員原來業務與資安有關，所以我們只要指定 OT 人員負責這一塊業務就算專責了嗎？還是可以做原來 OT 的業務。

主席徐嘉臨副處長：

你的意思是中油未來要配置 OT 的人來當作你們的專責人力，是不是？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

其實我們 IT 跟 OT 的業務本來就跟資安有關，剛才的解釋是只要業務有關，就可以算成是專責人員，因此我們只要指定哪一位同仁，他雖然還是做原本資訊或 IT、OT 的業務，我們指定他是專責人員就可以了。

主席徐嘉臨副處長：

應該先這樣講，配置專責人力的目的是什麼？必須因應保護核心系統，另外一個是要做資安法所規定的法遵事項，你配置的人力相對要朝這方面去思考，但就我來看，重要的關鍵核心系統是關鍵基礎設施，也就是你們做油品工業控制系統，人力配置應該要朝這個方向去配置。

至於內部要如何配置，我們不會給你任何的權力去干涉，還是回到你們公司自己內部去作人員的配置，但是要想的是必須能夠保護到你的核心系統，這才是最重要的。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

長官給我們的想法是，原本的人員做的跟資安有關，只是因為資安法出來之後會再多一點事情，所以長官可能想說我們原來有 IT 人員跟 OT 人員了，我們指定一位或兩位，甚若是 A 級的話，是要指定到四位。

現在是長官在配置人力的時候，會說看這個法，「專責」跟「專職」，專責如果只是跟業務有關的，原本 IT 跟 OT 的人都跟資安有關，所以我只要指定出來就可以了，不需要再配人力了。

主席徐嘉臨副處長：

你現在已經有這樣的制度當然就可以了，你現在已經有了，如果符合法裡面的規定就可以了，不是說額外現在有了，然後還要再配置四個，不是這樣子的，現在有了就 ok，但是回歸到剛剛所講的，必須要回到這個法，專責人力的目的是要保護你的核心系統，所以人員的執掌、職能相對是要能夠呼應到這樣的條件與要求，以上說明。

對不起，你們是針對剛才特別的意見要再補充說明，不過原則上下次可能注意一下，一個機關就一次把問題講完，因為我看其實還有其他機關，如果要問的話，也要讓他們有機會。

農糧署：

第4條第1項第2款有提到「全國性民眾」是指 A 級機關，這邊所謂「全國性民眾」的定義為何？因為「全國性民眾」是指大部分的民眾，但

大部分民眾的人口比例是多少才算是？或是「全國特定類型的民眾」？第4條是提到 A 級機關，第2款是提「全國性民眾或公務人員……」，我是針對全國性的文字來提，可能是全國大部分，還是特定類型。

像教育部國教署是國民及學前教育署，可能是處理全國高中職以下學童的資料，像我們農糧署可能是持有及處理全國大部分農民的資料，像這兩個機關是不是符合 A 級的條件，這邊我建議全國性民眾或者是第5條講到「區域性」或「地區性」民眾的這個部分，是不是要做比較明確的定義？這是第一點。

第二點，有關附表1，之前前輩有提到專責人員的部分，A 級機關是要配置四名專責人員，目前現況是這樣子，主席大概知道全國所有的公務機關受限於總員額法的限制，人員大概沒有辦法自己增加。行政院二、三級機關資訊單位的人力，其實在成立的時候就定案了，有多少人就多少人，沒有辦法變動，有的單位幾十個而已、有的單位幾個人而已，雖然機關的首長可以調整各單位人力的配置，但目前機關只會增加，而人不會增加，都是在缺人，所以要機關首長按照這個規定去把人力從別的單位調到資訊單位，我覺得非常非常地困難。

因為每個單位資訊的人員數不一樣，所以這邊規定「配置專責人員四人」，但是這四人在資訊單位的比例可能不一樣，假設有一個單位的資訊人員有四十個人，所以四十個人就佔10%，看起來是 OK，但假設某個資訊單位只有六個人，四個人的比例高達67%，而且有一種情況是專責人員，像剛剛主辦有提到主要辦理資通安全相關的業務。如果指定專責人員，他說他是負責專門做資安的，其他如果臨時交辦的小工作，那就 ok，如果大的計畫給他，他也許會說：「我是專責人員，所以我不接。」這或許會產生一些衝突的狀況。

因此我建議是不是可以修「配置四個人」或「不低於資訊單位編制人員的20%」，考量看看。

主席徐嘉臨副處長：

為什麼是20%？

農糧署：

不一定。我是說各機關資訊人員的數量不一致，如果以我們署來講是六個人，六個人的20%是1.2，那就是兩個人，兩個人在我們署來講是還

可以接受，如果是四個人，我們是沒有辦法，六個人去掉四個人，因此建議可以考量看看。

專職跟專責或許也可以考量，不要定義這麼死，也就是專職而已，或者協調成專職或專責人員，或許有一些彈性。

第三，附表1至附表6都有備註，而這個備註第一點就發揮我國文字精美的特性，非常長，結果看下來看不懂，這個句子當中有兩個「或」、兩個「頓點」、三個「之」，所以整個句子看下來，我看不懂定義要做什麼，「資通系統之性質為共用性系統者，由主責設置、維護或開發之伺服器……」，我不唸了，看不懂它的定義，因此我的建議酌修一些白話文一點。

可是我超過三個問題了，我還有問題可以問嗎？

主席徐嘉臨副處長：

（點頭）

農糧署：

附表9的備註1，這裡是指靜態資訊，這個靜態資訊的定義，我們覺得很長，看不懂，因為這樣子聽起來不太清楚，我這邊建議一些酌修的方式，他把定義都寫成一行，可是理解上不容易，或許可以把它拆成不同行數。比如「靜置資訊」是指位於資訊系統特定元件，這個勒體可以舉例像上面；並與系統相關且需要保護之資訊，例如防火牆、閘道器等等的這些組態或規則。這個回去考量看看，這一些我全部都有文字檔，我會後會給你們承辦。以上，謝謝。

主席徐嘉臨副處長：

謝謝，有關於文字性的修正，我們回去再看一下，謝謝。接著我們看第二個問題。

苗栗縣政府稅務局：

我們看到那個附表，不管是 A、B、C 級裡面的安全性檢測部分，辦理內容是講「全部核心」的資通訊系統，每一年辦理一次。安全性檢測，我剛剛在看是網站安全性弱點檢測及系統滲透測試的部分，我們對照資通安全防護中，有一個對外服務核心的通訊資訊系統，那部分我們有一點搞不清楚，如果真的是網站來講，應該是對外服務，像內部如果不對外的，是不是也要作弱點檢測及滲透測試，這是我們比較不清楚的。如果只是針對

網站，我們建議「全部」改成「具有對外服務」核心資訊的資通訊系統，我的意見到此，謝謝。

主席徐嘉臨副處長：

你剛剛講的是資通安全防護不一致是哪裡？

苗栗縣政府稅務局：

附表裡面的應辦事項。

主席徐嘉臨副處長：

你現在講的是附表1的技術面安全性？

苗栗縣政府稅務局：

附表1、2、3就是 A、B、C 級裡面的安全性檢測，安全性檢測中的應辦內容是針對全部核心的資通訊系統，如果看前面是網站的話，不見得是各個機關的核心系統在外面。

像我們之前的應辦事項，其實是針對網站部分而已，但這樣來看又變成全部了，我們就有一點納悶，因為又對到後面對外服務的核心系統。

主席徐嘉臨副處長：

你講的「後面」是哪裡？

苗栗縣政府稅務局：

是資通安全防護那一點。

主席徐嘉臨副處長：

第幾頁？

苗栗縣政府稅務局：

附表1、2、3的技術面那一塊，也就是應辦事項技術面那一塊。

主席徐嘉臨副處長：

第幾項？

苗栗縣政府稅務局：

資通安全防護那一項。

主席徐嘉臨副處長：

防護裡面的哪一個？

苗栗縣政府稅務局：

比如有防毒軟體的防火牆、郵件過濾器、入侵防禦，後面那一項是針對要運用程式防火牆的時候，有特別說必須是對外服務的核心，就是資通系統，這個有特別說。但是前面卻是講「全部」。

主席徐嘉臨副處長：

我瞭解你的意思，這個我們等一下再一起說明好了。就這個問題嗎？

苗栗縣政府稅務局：

對。

主席徐嘉臨副處長：

接下來。

苗栗縣頭份市公所：

請問一下，如果 C 級單位也要有專職人員，而且還要有資通安全專業證照、資通安全職能評量證書，對我們要求好像還滿高的，因為其實我們資訊人員是一般的公務人員，慢慢在工作當中學習摸索，我也不太瞭解為什麼像我們有 server 就是 C 級機關，我承認對這一方面很多都還不是很瞭解，但是有這樣專職的話，好像壓力還滿大的。

主席徐嘉臨副處長：

先請詠萱回覆，從農糧署。

王詠萱分析師：

針對農糧署詢問的問題，有關於第4條全國性民眾的資料，所謂的「全國性」為何？我們在訂細則草案的時候，原則上「全國性」是指全國大部分民眾有那樣規模的話，我們會把它算在 A 級機關。

因為母法第7條有提到「保有資訊種類性質與數量」，如果農糧署只是全國性，限制在農民範圍裡面的話，原則上我們不會把它解釋為「全國性民眾的個人資料」，這邊先說明。

針對資通安全 A 級機關要「配置四人」及「單位大小」不同的話，其實配置人數是根據 A 級機關所持有的個資、維護的資訊系統或所管轄的業務有關，你看 A 級機關大部分都是全國性的業務，業務的重要性就是需要這麼多人來進行資通安全防護。

如果機關真的有這麼重要的業務，可能需要擴大資訊單位的編制，然後去補充人力，才能做到這樣的事，我們整個應辦事項跟後面的保護基準都是對應的。

如果機關真的沒有辦法的話，畢竟資安法通過之後，是有一定的法遵義務，公務人員依法行政是一個很基本的要求，我是覺得可以拿這個來跟單位長官來要求，能夠配置這麼多的人來進行這麼多的業務；文字的部分我們會帶回去再酌修。

針對稅務局講到 A、B、C 級的安全性檢測，內部網站要不要做？要，內政網站也必須要進行網站弱點檢測及系統滲透測試，全部的核心系統是 A、B 級機關要依照規定的頻率來做。這個對外核心系統的網路防火牆是不一樣的規定，因為運用程式防火牆主要是防外部的攻擊，但安全性檢視及滲透測試，有可能內部的系統受到跳板的攻擊，防禦的面向是不一樣的，所以即使是內部的網站，如果是核心資通訊系統的話，我們也會要求做這一些安全性的檢測。

針對頭份市公所有關資安專職人員關於資安證照很大壓力的部分，我們會希望資安專責人員還是有一定的訓練，有一定的職能才可以進行資通安全維護的業務，因此我們會要求人員可能要有相關對應的證書及教育訓練。後面看看專責人員到職後多久之內需要具備這樣的證書或訓練，我們來作對應，謝謝。

主席徐嘉臨副處長：

我再補充一下農糧署剛剛的問題，其實專職人力的數量跟機關人數的大小未必有直接關係，如剛剛同仁所講的，主要是回到核心業務是不是屬於全國性的，是不是提供跨公務機關共通性服務等等的這些東西，因為這樣的系統重要，所以需要投入更多的防護資源，而這個防護資源包含你打 ISO 27001，其實 ISO 27001 就有非常多的事情是每天日常維運必須 follow 的，包含資產管理、應用系統程式開發管理、委外管理、機房管理等等，各位打 ISO 27001，其實有非常多的事情要去做。

加上未來法裡面，可能未來上級機關對所屬機關要做稽核，或法裡面其他規定的事項都是未來專職人力要做的，是不是可以用機關的人數比例去定義，這個我們可能回去要看一下。

另外一個合理的比例是多少？你剛剛提20，有人會提為什麼不是30、10？如果機關沒有很重要的核心業務系統，但因為人很多，所以一定要設置這麼多的專職人力，倒也未必，所以我想人數跟機關的規模大小比例，未必是直接一對一的關係，這部分要先作說明。

接下來，苗栗稅務局（同仁）提到核心系統，剛剛我們同仁已經有解釋了，核心系統的網路弱點掃描或滲透測試，跟你裝 WAF，WAF 其實是不一樣的概念，WAF 大部分是放在對外的通道上，所以大部分能夠偵測及防堵的是對外服務的網站，大概是這樣的思維。

像剛剛有提到頭份市公所，像基層公所的部分，這也是我們很擔心的，因為基層公所的網站，我們每次在做攻防演練的時候，都會發現因為裡面投入的人不多，警覺性也不是很高，所以才希望在這個法做這樣的規定，也希望把你們人的能力透過訓練之後把它提升上來，這是這個法的目的。未來後續如果人力配置上有需求的話，優先一定是從內部配，如果真的不行的話，我們再看如何協助。

但是其他地方政府，像六都的話，基層公所其實多多少少都會把系統向他們的直轄市政府去作集中，他們會有統一的機房提供這一些服務，我不知道苗栗縣政府現在是不是有這樣做，這個我就不知道，後續再瞭解一下，謝謝。

還有其他的問題嗎？我先讓女士優先，因為你剛剛已經有發言過了。

台中銀行：

沒有。

主席徐嘉臨副處長：

不好意思，女士優先好了。

台灣自來水股份有限公司：

第4條講到資安等級是 A 級，自來水公司是依據第5項為「關鍵基礎設施的提供者」，是不是因為用戶數，所以我們自來水公司會被列為 A 級？所謂的「用戶數」是市場的佔有率嗎？

事實上我們地區的供水，像台中、台南地區有十二個區處，真正的關鍵基礎設施的那些設備、監控系統其實是在區處。如果改天提列安全等級時，自來水公司還是要列成A級嗎？

主席徐嘉臨副處長：

對不起，你剛剛講的是？

台灣自來水股份有限公司：

我的關鍵基礎設施，像台中地區是第四區的管理處，台中地區的供水跟台南地區的供水，我們是分開，而且分散式的系統，並不是集中在總公司這邊。

以目前來講的話，我們被列成 A 級，是用總公司的概念去管理，因為第5條是用關鍵基礎設施的整個用戶數多少，把我們訂成 A 級？又或者是市場的佔有率（訂定）？因為我們是獨佔市場嗎？又或是將來提列的時候，是不是用十二個區處？就是我們的管理處提列是 B 級，因為我們是地區性的，他是區域性的，像台南停水，不會影響台中。

主席徐嘉臨副處長：

瞭解，謝謝。我可以瞭解你們現在公司的組織架構。

還有第二個問題嗎？剛剛這一位先生。

台中銀行：

台中銀行第一次發言，在附表2裡面資訊安全責任分級裡面的非公務人員當中有提到，而且剛剛主席有提到在 ISO 27001的驗證過程中，這邊有提到資通專責人員，資通專責人員到底是負責 ISO 27001的驗證或是由資訊人員做 ISO 27001的驗證，這是有差別的。在法當中是不是應該定義清楚到底由誰來發動、執行？以免到時權責會有不清的狀況。

第二，因為這邊所定義到的全部核心系統，核心系統當中如果假設導入 ISO 27001，會有所謂的驗證範圍，使用者算不算驗證範圍的一部分？如果使用者算是驗證範圍的一部分，表示資訊、資產人員也是資訊資產，我們要蒐集的是包含所有使用到核心系統的人員，也都算資訊資產，要做到剛剛簡報上所提到人員的風險評鑑嗎？

第三，剛剛有提到滲透測試的部分，必須做全部資通訊系統的滲透測試，滲透測試是由內部打或者是外部打？這個是有差別的，如果一樣要做滲透測試，要先入到核心系統，發動者可以由外做發動，或是從內做發動、OA 環境發動，這是兩種不同的意義，因此要瞭解一下滲透測試是由外面打進來或是由 OA 打進去，謝謝。

主席徐嘉臨副處長：

謝謝，我們還可以再蒐集一個機關發問的問題。

（與會者皆無意見）

主席徐嘉臨副處長：

先請同事就剛剛兩個機關的提問來說明。

王詠萱分析師：

首先回答自來水公司的提問，可以看一下資通安全責任等級分級辦法第3條最後一項，第1項至第5項的公務機關辦理資通安全責任等級提交或核定，就公務機關或特定非公務機關內部單位有另列與機關不同等級必要的話，得依其業務性質第4-10條來認定，如果以自來水公司的話，各個分區有不一樣認定的必要，是可以依照這一項的規定，各分區來提報資通安全責任等級。

接下來是針對有關於台中銀行的問題，所謂 CNS 27001到底是由資安人員或是資訊人員的權責？其實我們資安法沒有規定 ISO 27001是由資訊人員或者是資安人員負責，這其實是授權各機關自己認定。

我們在資通安全維護計畫裡面有一項要求要有專責人員及經費的配置，到底是資安人員或資訊人員，可能是牽涉到專職人員的配置，到底哪一些人要負責哪一些工作的配置，如果機關已經在維護計畫裡面有定義的話，就依照維護計畫裡面訂定的方式來實行，權責就是這樣子來劃分。

針對27001的驗證範圍，使用者是不是驗證範圍？是的，核心系統使用者也是在核心系統的驗證範圍內。

主席徐嘉臨副處長：

接下來我再補充一下，ISO 27001到底誰來做這一件事？在法裡面確實沒有明訂，明訂之後其實有好、有壞，機關的人力是不是從此就被限縮，或者是有自己能力配置的空間，這其實都有好、有壞。

我們在資通安全維護計畫裡面，因為我們未來會訂一個版本，在這個範本當中，其實會希望各機關寫到專職人力的配置，可能會包含專職人力的工作內涵。在那個範本當中，我們可能會提供初步的工作內涵給各位參考，但那純粹就是參考，各位如果認為你們機關還有一些業務需要專責人員來辦的話，其實機關都可以自己調整，我們沒有一定的規定，這個部分先說明。

接下來，剛剛有提到滲透測試是往內或是往外打，往內或者是往外打的價錢都不一樣，原則上印象中比較低的是從黑箱打，原則上往外打就可

以了，尤其銀行系統這麼重要，你們要視業務的必要性來做額外地強化或是更多的測試，這個我們沒有意見，原則上這是基本要求。

回答到此。有沒有其他的問題？針對這個子法還有沒有其他的建議事項？

苗栗縣頭份市公所：

我想到的都是執行面的問題，我們可能會需要中央、上級機關給我們的一些輔導，像導入 ISO 27001，或者像專業訓練取得專業的證照這些，我想知道資通處會不會有一套辦法，不只是由法令而已，也要讓我們知道該如何執行、完成。

主席徐嘉臨副處長：

我簡單回答一下，導入 ISO 27001通常就要派人去上課，在業界有非常多這樣的教育訓練課程，首先可能要找人家去上課，瞭解一下怎麼 run 資通安全管理系統。

另外一個，技服中心其實本來現在就有提供資通安全職人很多的課程，配合《資通安全管理法》，我們就會陸續開法遵、資安專責人力應該要具備什麼條件，我們會開這樣的課程出來，到時各機關都可以來參加。但首先你必須要把你們的人送去教育訓練，這是最基本的，坊間現在有非常多的教育訓練都可以參加，先作這樣的建議。

還有其他的問題嗎？

苗栗縣政府稅務局：

剛剛講的滲透測試是往內打的部分，我們有一個狀況是，像我們的核心系統是屬於實體隔離，根本接觸不到網際網路的部分，很明顯往外打是不可能的，一定是在實體的，而且是內部（打），我不知道內部是不是一樣要這樣執行？謝謝。

苗栗縣議會：

剛剛頭份市公所的提議，我們建議專職人員或是專責人員不管怎麼樣，至少資訊是職系的，或是政府開了一些資訊課程要合格過的，要找一般的行政去當，根本不曉得這什麼東西，我是說執行面（問題），因為在基層機關裡面要找資訊人員已經很少了，他們都只是兼辦而已，只是負責不要當掉，若當掉還是找廠商。

因此有關於專責人員、專職人員的話，要資訊職系的或我們在中央開課，就是像我們要轉職系，要具備哪一些課程通過，你才可以執行這個業務，我覺得這樣對人力的配置，我不會強制說一定要（配置）資訊（人員），但是政府有一套培訓機制，讓這些人是合格的（資訊人員），人力的部分我想這樣會比較妥適，不然對我們這一種小機關，像我們是一、二十個人的公務機關），你要他提一個人出來是有一點難度的，謝謝。

主席徐嘉臨副處長：

謝謝。要不要資訊職系，這個我們可能再考慮一下，因為其實滿多機關都不是資訊職系的，不能說很多，他們好像也可以把資訊工作做到一定程度，所以這部分我們再考慮一下。

剛剛特別提到如果是內網的系統，是不是應該可以嘗試從內網裡面去做滲透測試？因為外網做其實你也接觸不到，做了也沒有意義；但也很難講，你的內網有沒有通外網，其實很多機關自己不見得那麼清楚，或許你也可以從外網的角度試試看，可能在某個連接點，你過去從來沒有注意到、意識到那邊是有從內網通到外網的地方，所以從不同的角度去思考這個問題。如果是這個 case 的話，倒沒有強迫一定是要從內網測試或外網測試，這個是簡單回應。

針對這個子法還有沒有一些意見？

衛生福利部中央健康保險署：

請教一下，有關於資通安全負責人員總計有四張以上的證照，其中是有關於資通安全的專業證照、資通安全職能證照，這是取其一或是兩者之一？有兩種。

主席徐嘉臨副處長：

各位還有沒有其他的問題？我們蒐集三個問題之後再一起回答。

（與會者皆無意見）

主席徐嘉臨副處長：

沒有。請詠萱針對剛那個問題說明。

王詠萱分析師：

公務機關的話，這邊會要求資通安全專業證照與職能評量證書，都是各四張，也就是兩個都要具備。針對特定非公務機關的話，我們要求資安專業證照。

主席徐嘉臨副處長：

好。各位還有建議嗎？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我們就到下一個子法，「資通安全事件通報及應變辦法草案」，有沒有哪一位要先發言的？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

資通安全事件定義，剛剛簡報也有提到，主要著眼點是在違反資通安全政策或保護措施，但是我們在解讀時，會看到前面的字眼，前面寫的是「可能有違反」，後面是寫「影響」，所以這個認知可能主管機關跟特定非公務機關的認知會不一樣，因為按照法令的話，如果未通報資通安全事件是沒有改正期，只要是發現就會被罰鍰。

因此我們希望有關於資通安全事件的定義，是不是可以再解釋清楚一點？比如參照第3條有關資通安全的定義，資通安全的定義是防止資通系統或資訊遭受未經授權之存取使用等等的侵害，是不是可以把它定義成如果只有遭受未經授權的事件才會被定義成資通安全事件？這樣比如軟、硬體的當機或是網路中斷，如果不是因為未經授權而引起事件的話，就不算資通安全事件。以上。

主席徐嘉臨副處長：

你剛剛提的第3條是不是指母法第3條？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

對，母法第3條就資通安全事件有一個定義，上面有一個資通安全的定義，定義就是遭受未經授權。

意思是如果我們只是機器故障的話，基本上就不算資通安全事件，可以這樣解釋嗎？因為並不是「遭受未經授權」。

第3條第4項資通安全事件的定義寫成「可能有跟影響」，機關跟主管機關可能認知上會有很大的差異，因為這個名詞太模糊、範圍太廣。

主席徐嘉臨副處長：

接下來還有沒有第二個問題？

苗栗縣政府稅務局：

對於資安等級緊急事件的部分，像第三級、第四級若核心有狀況時，有一個問題是「於可容忍中斷時間回覆或無法於可容忍中斷時間回覆」，這部分我們實際上看到的情形是，我們之前碰到停電，那時不是我們可以判斷到底可不可以在我們容忍的時間內回覆，我無法判斷的時候，我們要直接從第4級開始嗎？或是原先既然無法判斷，就先寫成第4級，然後再改第3級、第2級，可以這樣改嗎？在通報的時候。

主席徐嘉臨副處長：

就這個問題嗎？

苗栗縣政府稅務局：

（點頭）

主席徐嘉臨副處長：

接下來有沒有第三位要發言的？

農糧署：

農糧署第三次發言，在條文當中第2條，有訂定資安等級四級，在第2項、第3項及第4項的最後一行，這裡都有寫到「有前項各款情形的資通安全事件影響兩個以上機關者」，好像還沒有 ending。這邊是不是要增加一句？有影響兩個以上機關的話，等級必須要向上提升一個等級，這是對應到簡報第2項、第3項有講到的，對應到第2條第2事、第3項及第4項的話，好像不太對應，這個請看一下。

第9條的部分有定義到資通安全事件通報的作業規範，第10條是定義到有關資通安全事件應變的作業規範，所以各機關要有這兩個東西，有些機關裡面是有打 ISMS，ISMS 裡面有規範，然後規範裡面有訂定相關的規定，所以大部分的機關可能就有資通安全事件通報及應變程序之類的，如果這個程序已經符合第9條、第10條規定應包括的事項，這樣 ISMS 的規範就可以拿來作為通報、作業規範、應變措施規範，不需要另外再訂這兩個規範，ISO 裡面已經有了、且符合了，是不是可以不用另外訂定？以上。

王詠萱分析師：

先就資安事件的定義來說明：母法當中定義的資安事件，資安事件就是可能有違反資通安全政策或保護措施失效而造成影響，這部分恐怕沒有辦法限制是只有未經授權的存取。

在一般的認定上，其實系統不是未經授權人存取，比如系統上版，但上版的問題導致系統掛掉不能用，還是經過授權的版根，但是它不能用了，解釋上來看也是資安事件，資安事件的解釋上並不是只有未經授權的存取會造成資安事件，可能像剛跟先進所說的，像電力中斷或者是一些操作的失誤都有可能會引起，因此解釋上並不會只限於未經授權的事件。

有關於資通安全事件還是要以母法第3條第4項來定義，也可以參酌資通安全事件的分級面一些規定來看資通安全的定義是什麼。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

不好意思，我補充一下，因為我們是 CI 單位，所以成控那一塊，如果是一些影響領域是走工安系統緊急應變的通報機制，所以不見得會走資安通報，但如果在資通安全法出來之後，你的範圍這麼廣，我們在界定要走哪一個系統通報會有一些不一樣。因為我們看到的重點是「可能有」跟「影響」，這個範圍真的太廣了，幾乎只要我們跟核心系統有問題的話，幾乎都符合。

主席徐嘉臨副處長：

只要是你的 OT 系統在可用性、完整性、機密性上有任何的失效，你沒有辦法確保它，導致你的核心系統，不管是你的系統停止，原則上就是資安事件，所以你剛剛講的設備當掉、不能運作，它就是資安事件了，因為它已經不符合所謂的可用性了。

「資通安全」的意思是確保它的機密性、完整性及可用性，講白話一點，資安事件就是這三個性你都沒有辦法確保了，就是你已經產生資安事件了，因此你剛剛講系統既然已經停止運作了，假設是伺服器當掉或機台當掉了，原則上就是資安事件，所以就是要通報，未來的通報體系可能不是只有工安這一塊，還有法裡面要規定通報的體系。

這樣可以嗎？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

喔。

王詠萱分析師：

接著是針對苗栗事務有關於事件等級的部分，通報的時候是不是可以改？我們在通報應變辦法第4條第2項，如果機關在通報之後等級變更的話，是可以續行通報去改資安事件等級的。

接著是農糧署這邊，我們有涉及二機關者，可以看一下條文「有前項各款情形」，其實「前項各款情形」在第2款、第3款及第4款，分別指的是一、二、三級事件，所以二級事件，就是有一級事件發生以後，影響數個機關以上，那就是二級事件。

法條的文義大概是這樣來看的，後續是不是要修正，我們回去再看看怎麼樣，讓大家更清楚。

有關於通報應變作業程序裡面，ISO 程序書已經有了，是不是還要再訂一個事件通報應變的程序，可能要看一下 ISO 程序書裡面，你說項目符合，那他的適用範圍是不是也符合，因為我們這邊要求的事件通報作業規範是指全機關的規範，但是一般 ISO 在導入的時候，不一定會針對全機關導入，因此可能要看一下範圍是否能夠符合，如果都可以符合的話，可以用程序書的規範來取代作業規範。

主席徐嘉臨副處長：

我補充一下苗栗稅務局剛剛講可容忍與不可容忍，每個系統通常會定義所謂的 RTO 跟 RPO，這個 RTO 可能就是所謂的「可容忍時間」，今天一旦發生斷電，可能就要事先評估，假設這個系統四小時之內要回覆，就要評估台電要斷電多久，如果今天斷電兩小時，你預計可以恢復，但問題是你已經中斷了，你還是要依照現在的通報等級，像你通報一個級數，但後來發現台電還是沒有辦法在兩小時，可能需要六小時，就已經超過原本可容忍的時間，你就要再往上通報、提升你的級數，因為你已經在不可容忍的時間內去做回覆。

重點是如何確保你的業務能夠持續因應，這是在 BCP 的計畫當中要去設計的，當你整個 IT 不能運作時，要有其他的替代方式，讓整個機關的業務可以運作，這是做通報應變，甚至要訂定通報應變程序部分是需要去著墨的地方，大概作這樣的說明。

剛剛農糧署這邊有特別提到影響兩個機關者，其實大部分判斷的角色是行政院這邊，我們本來就有打算未來文字要再做詳細地說明，如果兩個

以上的機關同時通報同一個等級或同一個類似事件的話，我們可能就會向上再提升一級，因為有更大潛在的資安威脅在我們的政府機關中，這部分我們後續會處理。

現在回應到這邊，看一下各位有沒有其他的問題？

苗栗縣議會：

前面法裡面，責任分級當中，縣（市）政府的做法是提出自身資安通報等級及所屬區域的直轄市縣（市）政府，會送主管機關核備。但這邊第5條是直接對主管機關，這邊沒有重複嗎？因為之前會送給縣政府、再送主管機關，這邊是直接送主管機關，我不知道前後的子法有沒有……

主席徐嘉臨副處長：

你是指「資安事件通報」這邊嗎？

苗栗縣議會：

對。所以這邊一個第5條、一個第3條，前面責任分級是第3條，會送縣政府再送主管機關，第5條是直接到主管機關，這兩個條文有沒有關係？

主席徐嘉臨副處長：

第5條你是不是指議會？你指的是第5條的哪一項？

苗栗縣議會：

第5條倒數第2項，總統府、國安局、立法院，縣政府是直接通知主管機關，前面是會送縣政府再通報，這邊做法有沒有一致性？

主席徐嘉臨副處長：

接下來有沒有第二個問題？沒有嗎？

台灣自來水股份有限公司：

請教一下，假設我們這個場所是實際上淨水廠的處理單位，如果一時台電跳電，因為淨水廠幾乎都備有發電機，馬上啟動發電機的話，這算是資通安全事件嗎？

再者，在供水操作的部分都會放一些公共監測單元，比如像水壓或者是濁度、開度會透過 PLC 拉回監控室。大部分都是走向專線，透過數據線進來。這時因為線路或者是某一個單元的機器故障，這個層級也要列在資通安全事件當中，其實這個狀況應該是不少見的。以上。

主席徐嘉臨副處長：

還有其他的問題嗎？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我先就這兩個問題回答。

王詠萱分析師：

首先針對資通安全責任等級跟事件等級的問題來看是不是有一致性，首先資通安全責任等級，地方民意機構是透過縣（市）政府會送，這主要是請縣（市）政府協助我們，不要一次對到這麼多個鄉鎮區公所。

至於資通安全事件通報等級審核的話，原則上整個公務機關的資通安全事件通報就會在事件通報網上進行，各縣市議會在網站上去審核資通安全事件等級，本身就是先對主管機關進行提交，兩邊規範可能不一致，因為是實務運作，這是必然導致的。先回答到這邊。

自來水公司淨水廠跳電馬上啟用發電機，這是不是資安事件，要看一下淨水廠跳電到馬上啟用發電機的中間是不是有間隔，整個設施的運作是不是有停頓，如果有停頓的話，應該還是資安事件，如果沒有停頓的話，就不是資通安全事件。

同樣的，有關於外廠公共監控的單元，某個單元故障是不是資安事件，一樣是要回頭去看這個監控單元在整個系統當中，擔任什麼角色？是不是這個監控單元故障了，而導致這系統某一個區域是不是就沒有辦法做監控了？或是這個監控單元故障，但是有其他的監控單元可以代替這個監控單元，以提供這個區域水質監控的責任，又或是要看資訊系統的設計或看監控單元本身提供的責任。如果是造成那一區的水質沒有辦法再監控的話，那應該資安事件，如果有其他監控單位可以代替他提供這樣供用的話，我覺得那就不是資安事件，簡單回應。

主席徐嘉臨副處長：

我再補充一下剛剛資安責任等級的提報程序跟資安事件通報程序的對象不一樣，主要其實考量發生資安事件比較緊急，所以直接對到主管機關就可以，就不用再透過地方政府再轉通報，原因是這樣子的。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

回覆一下剛剛回答的問題，基本上公共系統 PLC 應該是不太屬於資安的部分，因為基本上 OT 會納入資安是因為有伺服器、網路的關係，那邊控制器 PLC 是本身控制器單元的問題。

那個問題基本上像卡片壞掉，那個東西就是 ISO 9000下去通報就可以了，除非真的是伺服器受到入侵，又或者是伺服器有異常，跟資訊系統相關的才會做資安通報，應該說這樣才合理。

主席徐嘉臨副處長：

在《資通安全管理法》裡面管的關鍵基礎設施包含 IT 及 OT，所以 IT 是所謂的公共系統，就是所謂關鍵基礎設施，是含在所謂資通訊的定義裡面，這邊要跟你說明一下。一旦 OT 發生事情，因為那才是最重要、最關鍵的，他一樣要通報。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

但是內容是屬於電的部分，並不是資通那一塊。

主席徐嘉臨副處長：

你所謂的資通是指 IT？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

類似 IT 那一塊。

主席徐嘉臨副處長：

不只是 IT，特別是 OT 的部分，是這一次要納管的範圍，因此這個部分還是要再作一次說明。為什麼要把它管理？其實有很多的資安事件，很多的電廠在過去國外發生的紀錄當中都有遭受過資安的攻擊，造成大量停電的事，這個是曾經發生過的，這個是看國際上發生資安事件的情況，但是回到這個法裡面，它還是包含 OT。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

它是包含 OT 沒有錯，剛剛自來水反映的問題，控制器電的部分出問題，但對資安其實沒有關係的，我的問題是這個。

主席徐嘉臨副處長：

這個就如同仁剛剛的回答，也就是他的服務有沒有中斷，如果因為控制，而導致服務功能失效，那就是資安事件，因為已經不符合可用性了。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

這個而言基本上 ISO 9000放在速報，那個是速報下去做通報。

主席徐嘉臨副處長：

你們原本的程序怎麼走，我們不用管，但是回到這個法裡面就是要通報，符合資安事件的範圍，他就是要通報，這個是在這邊必須跟各位說明的。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

我請問一下，如果溫度點異常，難道我們就要通報嗎？

主席徐嘉臨副處長：

所以剛剛同仁講的是，溫度點會不會影響到整個系統的運作，如果1萬個點其中的一個，其他還有很多白的點在旁邊，其中一個小點失效不會影響整體，那就不是，但如果已經大規模異常，比如90%全部偵測問題失效，那可能就會造成整個功能運作上是有問題的。

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

基本上以影響範圍來作認定，是嗎？

主席徐嘉臨副處長：

我覺得機關未來在做這件事情的時候，還是要從整個業務是否符合，我們剛剛特別有提到資訊安全是所謂的機密性、可用性及完整性，如果在任何的性質去做功能失效，就是一個要通報的時機點，這樣 ok 嗎？

台灣中油股份有限公司天然氣事業部台中液化天然氣廠：

（點頭）

主席徐嘉臨副處長：

先作這樣主要的說明。

各位還有沒有其他的建議？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，就到下一個子法。「特定非公務機關資通安全維護計畫實施情形稽核辦法草案」，各位對這個子法有建議嗎？請說。

農糧署：

農糧署發言，第3條有規定「主管機關應每年擇定當年度受稽核的特定機關」，這個是每一年。

第7條規定主管機關應每季所定受稽核機關，這兩個條款所定的這件事是不是有相關聯的關係？一個是每一年、一個是每一季，這邊請教的是，因為每一年要做稽核作業，對特定非公務機關，這樣是每年要做或是每季要做？以上指教。

主席徐嘉臨副處長：

接下來還有沒有第二個問題？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有問題的話，先請同仁就剛剛的問題說明。

王詠萱分析師：

我們說明一下，第3條主管機關應該每年擇定當年度受稽核之特定非公務機關，主管機關現行的做法是每一年年初的時候，我們會挑選比較多的機關，通知你說今年有可能會對你進行資通安全的稽核。

等到每一季實際稽核的時候，每一季都會從年初通知的機關，會挑選一些真的稽核機關，在一個月之前會對他通知並進行稽核。

第7條是每季稽核完成之後的一個月內會發稽核報告，所以兩者是沒有衝突的，我們每一年初會擇定一定的機關，作為今年稽核候選機關，在每季稽核之前，我們會針對選定出要受稽的機關來稽核，以上說明。

農糧署：

如果受稽的機關不是很多，我可能一次就稽核完了，不用分到每一季去，每一季比如有二十個人，你分四次稽核，每一次稽核五個，如果你要稽核的對象其實沒幾個，可能一年裡面我覺得排定一次就稽完成。

主席徐嘉臨副處長：

這個主管機關是指行政院，不是各公務機關。

農糧署：

因為是「特定非公務機關」，如果以我們農糧署的角度來看，如果是以中央目的事業主管機關的話，跟我們署的業務有關有三個單位，「特定非公務機關」可能是香蕉研究所，還有兩個，我忘記了，所以總共有三個。

個資法裡面相關的規定，中央目的事業主管機關是農委會，但是那一些業務是農糧署管的，一個是計畫市場有關的，一個是別的之類的。我們管非特定公務機關有三個，不用累積，我就一次稽完，對不對？

主席徐嘉臨副處長：

我說明一下，這個「稽」是指行政院要去稽特定非公務機關。

農糧署：

所以不是我們要去稽，對不對？

主席徐嘉臨副處長：

對，但是你們自己要另訂辦法。這個子法是行政院要去稽特定非公務機關的稽核辦法，因為我們現在實務上的做法，目前對公務機關，我們每一年會挑選公務機關來稽核，會分在每一個季裡面，每一季會分配不同的公務機關來稽核，每一季完成之後就會產生一個稽核報告，目前的做法是這樣子。

農糧署：

所以不是我們要做的嗎？

主席徐嘉臨副處長：

這個子法不是。

各位還有其他問題嗎？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我們就進入下一個資通安全情資分享辦法，有沒有哪一位要先發言？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我就要到下一個子法了。

接著到第六個子法，「公務機關所屬人員資通安全事項獎懲辦法」有沒有哪一位要先發言的？

農糧署：

獎懲辦法是要給各機關去參考，然後自己訂定自己的獎懲基準，如果參考我們公務人員，都會有一個所謂平時獎懲標準。各個機關，像縣（市）政府會訂自己的、各部會也會訂自己的，其實是參考公務人員考績法施行細則去訂的，也就是說，比如部會或者是縣（市）政府可能會去訂一個標準表，什麼情況下記嘉獎、什麼情況下記功，這樣子各單位在執行時就會比較有標準。

以這一種情況來講，對應到資通安全事件獎懲辦法的話，這個部分是比較上位的，這個獎懲辦法訂了之後再往下，有沒有比較明確的獎懲標準表？有那個東西的話，各機關才比較好參考。不然給各機關適用，要訂哪一種情況是用嘉獎、哪一種情況是記功的話，過去每一個機關或者部會或者是縣（市）政府，可能訂出來的標準不太一樣，有的獎勵比較大、有的獎勵或許會比較小。

因此我要問的是，這個辦法出來之後，未來所謂的獎懲標準表是各部會、各縣（市）政府要去訂給他的下屬機關去參用嗎？以上。

主席徐嘉臨副處長：

接下來有沒有第二個問題？

苗栗縣政府稅務局：

有關分類獎懲的部分，不管 A、B 級部分，有一個 CNS 27001的導入或驗證的部分，有的部分實際上是要錢的，但我們在訂定實施時，我們可能會碰到經費的問題，如果因為經費的部分，我們沒辦法真的很完整實施時，我不知道這算不算情節重大？如果這樣的話，我們沒錢，還是可能會被處以警告或是處分，我不知道會不會有這一種情形，謝謝。

主席徐嘉臨副處長：

還有沒有其他的問題？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，我們針對這個問題說明一下。

王詠萱分析師：

首先我說明一下，獎懲辦法當中我們指定標準、原則，沒有訂額度的原因是，我們有問過銓敘部的意見，參考考績法施行細則第13條的規定，嘉獎、記功、申誡、記過的標準，由各機關視業務情形自行訂定報請上級機關備查，銓敘部認為額度的部分是各機關的權責，如果統一訂定額度的話，有點違反考績法第13條的規定，所以額度的部分還是要請各機關自行視自身資安業務的重要性來訂定，原則上不會再提供標準表。

有一些資通安全維護計畫的實施情形，像要求要導入27001，又因經費不能實施的話，算不算情節重大？這個法施行之後導入27001會變成法遵的義務，公務機關必須要依法行政，所以還是要請各機關儘量編足夠的預算來推行這一些業務。是不是情節重大還是要回歸到機關的權限，請各機關自行判斷。

農糧署：

對不起，剛剛回答的我想要再說明一下，不是由你們來訂定，是要求各部會或者是直轄市縣（市）政府來訂，為什麼？地方的地政事務所或者是戶政事務所要自己訂嗎？他們沒有人訂。

A 戶政事務所跟 B 戶政事務所訂出來不一樣，誰要訂？內政部來訂，也就是這個部會訂一套自己部會的特性，而內政部所屬機關，這個業務性質是類似、相同的，所以內政部來訂。

直轄市、縣（市）政府可以來訂，像目前公務人員平時獎懲標準表也是這樣做，我的意思並不是由行政院資安處或行政院來訂，並不是，是要求部會或縣（市）政府訂一個給他們所屬機關去採擬的，不然各機關訂成五花八門，這樣都訂不出來。

主席徐嘉臨副處長：

我想請問一下，這個機制目前在地方政府是這樣運作的嗎？你剛剛講很多事情是由上級的地方政府在訂，然後給所屬機關。

農糧署：

我不是很瞭解，但我查了一下，像上級機關是農委會，農委會有訂農委會及所屬機關公務人員平時獎懲的標準表，這當然是依據公務人員考績法施行細則所訂的，內政部有內政部訂好的，縣（市）政府好像也有自己訂好的，但差異性我想應該不大。

主席徐嘉臨副處長：

我的建議是，如果現在已經有這樣機制運作的話，這部分就回到那部分去訂就好了，如果沒有的話，我覺得權責還是回歸到目前現在機關自己人事考評的機制上，像剛剛講農委會已經有訂所屬的，未來是不是可以把資安這一塊納入，就是在人事運作底下運作；如果沒有的話，我倒不建議一定要另外為了這個，再跑出另外一套特定的機制出來。當時訂這個目的希望能夠回到現在人事考評機制裡面去運作就可以了，不需要再大費周章跑出另外一個機制。

農糧署：

瞭解。來參加北、中、南三場（機關同仁）有可能有四級機關或者是三級機關或者是二級機關，所以有可能是部會的資訊單位來參加這個會，應該要針對這個獎懲標準去修改一個類似範本之類的，納入原來的標準表；也就是說，依我們來講，農委會暨所屬機關公務人員的獎懲標準在這裡（好比四十項），農委會的資訊人員應該根據這個把資通安全的項目加入進去，應該有部會的資訊人員來做，因為部會的資訊人員比較多、縣（市）政府的人也比較多，而不是由這些所屬機關的人說這個要加入、那個也要加入，行政上的工作就會比較多，因此有上面的部會跟縣（市）政府來做。

如果以院的高度，是可以有一個文或是什麼方式，請部會的資訊人員針對這一塊就現有公務人員獎懲標準表考量，把資通安全的標準納入進去，底下的單位就適用，才不會覺得很麻煩。

主席徐嘉臨副處長：

這個獎懲辦法如果聽了之後，機關本來就要配合做這一件事，我個人覺得並不是資訊人員在做這一件事，因為機關內部人事的獎懲標準，一般是人事單位在訂的，所以資訊單位如果知道這一件事，應該要告訴你或你的資安長告訴你這一件事要訂，資安長就應該出來主持跨單位的協調，把這一件事納入到機關，甚至現在有函所屬的話，就把規定納入，倒不是一定要資訊人員啟動這一件事。

我再強調一次：是要回到你們現在內部的人事管理制度裡面，人事管理制度通常是人事單位在主政的。

農糧署：

實務上資通訊的工作，人事人員絕對不會主動來說：「你們有這個東西。」發動權一定是在資訊單位。

主席徐嘉臨副處長：

資訊單位一定可以發動。

農糧署：

我的意思是，這個東西不用每個機關都去做，就有部會跟縣（市）政府來做，不然一件事，大家都要做的時候，沒有什麼人要去做，如果指定部會，就要考量所屬機關，將來要適用給所屬機關用的時候，請你要去做，然後指定給他，他就比較有責任是要訂一個給大家所屬來參考，這樣可能比較有效率一點，我是這樣子建議。

主席徐嘉臨副處長：

謝謝。後來在資通安全維護計畫有把這個放進去，所以我們未來在看各部會或各機關資通安全維護計畫時，原則上就可以看到這部分的機制如何在各機關裡面運作，所以你剛剛的建議，我們會納入參考，這一件事讓大家都知道，謝謝。

還有沒有其他的建議？

（與會者皆無意見）

主席徐嘉臨副處長：

如果沒有的話，那我們今天六個子法都討論完畢了。各位有沒有臨時動議要提出的？

苗栗縣政府頭份市公所：

可以再讓我們看一下時程表嗎？

王詠萱分析師：

我們說明一下，今天的簡報已經放在國家資通安全會報的網站上，有一個「資安法專區」，各位可以到那邊下載今天的簡報。

主席徐嘉臨副處長：

各位其實可以不用抄，回去下載簡報就知道裡面的內容。

如果沒有（其他意見）的話，今天會議到此，謝謝各位。

（會議結束）

1