資通安全管理法子法草案座談會逐字會議紀錄

時　　間：107年4月19日（星期四）下午3時

地　　點：金融研訓院501會議室

出席領域：財團法人及公營事業

【記錄開始】

主席（徐嘉臨副處長）：

好，謝謝那個周科長的報告，那接下來我們就開始開放各位的提問或者是建議。那因為我們剛剛這個發言規則裡面也有特別提到是提5個問題，我們這邊再開始做一個說明這樣子。但是我想說，可能每個單位要發言的問題數比較難控制，我們是不是就2個單位提完問題之後，那我們就開始做一些詢答，這樣子好不好。好，那就開始，那有沒有哪一位，哪個單位願意先提問。

司儀：

不好意思，司儀這邊補充，每一位發言人發言前，請幫忙報上您的單位跟姓名，那以發言2分鐘為限。

主席：

好，那我們其實剛剛司儀在會前有說，因為有6個子法，所以我們是分2部分討論，所以第1個部分各位可以看到投影，我們現在是針對前面3個子法就是資通安全管理法的施行細則，還有資通安全責任等級的分級辦法，以及公務機關的人員獎懲辦法來去做討論，那我想子法因為各位在隨這個開會通知，各位應該都有收到，所以我想子法內容大家應該有些熟悉，那就請各位提問這樣子。好，有沒有人要先，有沒有哪一個單位要先發言的？

財團法人法律扶助基金會代表：

大家好，我是財團法人法律扶助基金會的代表。然後我主要有6個子問題想請教一下，我主要針對的是責任等級第7頁的部分來作探討。

主席：

對不起，等我一下，請問一下我們這邊有子法的內容嗎?如果我們等一下需要的話，我就把它投影在上面好不好。好，請繼續，不好意思。

財團法人法律扶助基金會代表：

好，不會，謝謝。然後第1項就是防護基準嘛，因為它是後面寫說1年內要依照附表5跟6來改善，因為我們預算是今年提明年的，是否它可以放寬說2年以上?然後第2項的話是，它要通過第三方的驗證，之前我參加的會議之前都是至少1項或2項，然後它現在好像改成全部的核心，不知道它可不可以就是有機會改回之前的。然後，第6項的話是因為我第1次看到資安治理成熟度評估，然後我上網搜尋了一下簡報，然後想說是資通安全處這邊來發網站，然後我們填寫，不知道是不是我理解有沒有問題?想說這個應該是不是從上面來要求下面，而不是機關自己主辦的。然後倒數第2項，教育訓練的話，是否像我們財團法人可以一起參加公務機關的教育訓練，然後，再來第8頁的話就是，職能評量證書，不知道我理解的是不是就是說，我們參加資訊人員參加訓練之後，他就有一個證書的意思。然後最後一個問題就是說，在第15頁有1個完整性驗證工具，然後想說，它是否能放寬說，不一定要工具才能檢驗完整性。好，謝謝。

主席：

好，因為這問題還蠻多的，所以我們就先回答，能夠回答我們先做說明好了。針對提問的部分，如果是建議的部分，我們可能就納入參考這樣子。那我們在第2輪的時候，把一些修正的結果再跟各位做說明。那智禾是不是可以先就你所知的部分說明。

資通安全處周智禾：

剛剛講的第1個是在第7，主要是針對我們附表2的部分。第1個是資通安全資通系統及防護機制。我們要在核定之後1年內要完成相關的一些控制措施，是這個問題嗎？那希望可以放寬到2年？

財團法人法律扶助基金會代表：

對。

資通安全處周智禾：

因為預算的問題嗎？

財團法人法律扶助基金會代表：

對。因為我們主管單位是司法院，然後基本上我們是今年編明年的預算，而且它現在是草案的階段，比較難強而有力。

資通安全處周智禾：

我知道，因為我們的法其實並不是通過之後馬上施行，我們大概會有一段緩衝期，然後目前規劃是6個月。那6個月之後是不是一次全部施行，我們目前還在內部做討論。所以其實這個時間點還是會比一年再更長一點，那到時候如果有這一些執行上的困難，其實是可以提報到你的中央目的事業主管機關來做一個核定，如果您在針對我們後面附表1到附表6所列的一些應辦事項跟防護基準，如果有執行上的困難的話，其實可以跟你的中央目的事業主管機關來做一個說明，然後給大家來核定，是不是OK。那，接下來是核心系統部分。那因為以前我們有發現是說有些機關因為在導入ISMS，常常是以直接找1項導入，然後就認為它已經通過了ISO的驗證。那後來我們是認為說。應該要依照後面我們附表5裡面所列的這個資通系統的一個分級。那評估出我們資通安全，系統的一個安全等級。把中高系統列入到我們的核心系統，那這些核心系統，應該要納入到你們的ISMS驗證範圍。那資安治理的話。我們這邊是有設計資安治理成熟度的一些問項。那是交由機關自評它的一個能力的成熟度等級。所以這個是由機關來做自評，目前作法是這樣，那現在的問項其實是會非常多，所以我們今年大概下半年會做這個問項的檢討，然後會把整個問項再精簡，精簡之後會再找機關試行導入，然後預計會在年底或明年初會公布新的一些問項，希望用更精簡且更客觀的方式來評定整個機關的一個資安治理成熟度的一個能力基準。那教育訓練的部分的話，以往都是由技服中心，就是由行政院資安會報，我們會舉辦一些教育訓練，那教育訓練對象的話一般是公務機關。所以，我們的能量其實有限。那其實從去年開始，我們就把教育訓練變成說我們來訂課綱，然後委託給學校。去年是有4所大學在北中南，那由他們指派，就是配置相關的場地。然後指派適當講師，依照我們所訂的課綱，然後，因為其實北中南，也會比較符合我們現在需求，因為如果以我們辦，我們就辦在北部其實就照顧不到中南部的每個人，所以我們是委託給北中南4所學校，然後開辦這樣的資安的課程。那它可以找當地地理比較相近的一些人員來參與上課。那，所以到時候應該這些學校我們可以要求說它所開放的對象不限於政府機關，應該會開放到所有我們資安管理法所納管的對象。那職能證書的部分的話，則是參加過職能教育訓練的話要做考試，考試通過才會拿到證書，目前我們狀況是這樣，那最後一個是有關於完整性的部分，我們其實並不會限制是說一定要用工具，你用其他

方式可以達到一樣的效果都可以，以上說明。

主席：

好，那接著我們就來看。這樣有回答到你剛剛的問題嗎？

財團法人法律扶助基金會代表：

有。

主席：

好，接著我們再看第2個。

財團法人中央畜產會代表：

大家好，也感謝行政院能夠來辦理這一場的座談會。那我想延續前一位的這個問題。那本人是財團法人中央畜產會做發言。因為剛剛提到教育訓練可能就是我們這一些財團法人比較關心的。因為也牽連到一些預算的關係，那我們所要知道的就是說第1個，因為在簡報第7頁有個時程，它到底在什麼時間點的時候，我們這一些財團法人就要就位，因為這牽涉到未來我們在於專業人力，根據剛剛簡報可能在25頁有提到，這一個。因為我們專業人力跟經營，零方向，就是說我們目前可能在一些軟硬體設備各方面是並沒有達到這個位置的。那延續剛剛這個第3個問題，就是做教育訓練的部分，那雖然現在是有4所學校來做教育訓練，但是我們所知道的就是說如果本身在一些財團法人它並沒一些屬於這種專業所謂的技術的這個比如說像ISMS的導入的這些執行的話，那是不是也會有相關的輔導單位來協助。那我印象中在103年或102年的時候，資策會也曾經做過一些學術輔導，那也希望行政院去做一個未來的規劃方向，謝謝。

主席：

好，這個我簡單回答一下。這個立法時程的部分，就是先跟各位大概說一下，我們這個立法案一旦通過的話，因為規範對象其實還蠻多的，所以它並不是一下子統一全部就開始適用。那我們剛剛同仁在簡報的時候有特別提到它會是分階段適用，也就是說假設今天立法今天這個會議通過。我們就可能暫訂年底開始實施的話，公務機關是優先適用，接下來每半年可能接下來是特定非公務機關的關鍵基礎設施接下來適用，那再半年可能其他的公營事業跟財團法人，原則上會有分階段。所以，這樣子的目的也就是讓各位可以有時間去做準備。所以大概會有這樣子，換句話說，可能財團法人或者是公營事業在立法通過之後，到你們真的適用，可能是1年

以上的時間了。所以在這個期間裡面，你們就可以趕快做一些準備，原則上是這樣子。那教育訓練的部分，其實現在坊間在做資安教育訓練的課程已經非常多了，各位我不知道你們是不是資訊這個領域或資安這個領域，其實非常的多，像恆逸、資策會，還有現在交大開的這個資安駭客學院，其實他們都有提供非常多的教育訓練課程，那各位其實都可以多多去，去送、選人員去做這樣子的一個訓練。大概是做這樣子的一個回應。

主席：

好，那接下來還有沒有第2個單位要做提問。或者是給我們建議，其實我們今天的會議，比較希望是各位可以針對我們現在子法內容做一個提問，不過因為從剛剛到現在為止好像大部分都是在詢問這個內容，不過沒有問題，可能大家對這個法案的內容還不是太熟悉。那都歡迎各位可以提出。好，麥克風。

臺灣土地銀行股份有限公司代表：

這裡是臺灣土地銀行，那我有一個疑問，就是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這一份子法，那子法的第2條講到，第2條第1項，主管機關就是行政院應每年以現場實地查核之方式，稽核特定非公務機關之資通安全維護計畫實施情形。這樣感覺起來好像行政院是每年一定會實際查核所有特定非公務機關的那種一網打盡的感覺，但事實上實務上並不是這樣，因為在第2條的最後那一項，就是第4項，主管機關，有一個決定的過程，它是決定到底要去檢查哪一個受稽核機關。所以這個部分，有關第1項和第4項，我是覺得有一點點不太明確。

主席：

針對關鍵基礎設施，我們現在的實際運作方式，我們先跟各位做一個說明，那至於文字怎麼調，我們就回去納入一個參考，好不好。就1點嗎，還是還有其他？

臺灣土地銀行股份有限公司代表：

就一個。

資通安全處周智禾：

那我們目前如果辦理資安稽核的話，我們其實在1年，每年一開始我們會先公布計畫，那現在做法是先公布一群候選機關，就是讓大家知道說你接下來可能會被稽核，但是不確定，然後在每一季我們會從每一季的開

始前一個月，會再用發函的方式通知當季的受稽機關。所以，其實我們因為量也不可能那麼大，全部都去。所以，我們目前是1年，至現在為止，以今年跟去年的狀況來講，我們是挑30個。所以以現在這個條文，剛剛所提的意見我們後續納入參考，那至於對象的話其實我們在這個計畫裡面我們去評估說我們會訂出一些準則，然後再依照我們這個準則，挑選出今年的受稽機關，然後再去做實際的稽核，大概會是這樣。

主席：

好，那還有沒有其他的單位要提出來的。各位這麼客氣，那我就開始點名。因為今天其實人不多。如果人多的話我大概就不會一一點名了。所以，我想請問一下，財團法人國家文化藝術基金會今天有到嗎？有，OK嗎？我覺得如果各位有問題就儘量提。那像我今天早上在參加一場座談會的時候，那大家其實就是我點名之後再問，那我想大家不用這樣子，就是有問題就儘量提出來都沒有問題。有嗎，好，麻煩那個麥克風。

財團法人中央廣播電臺代表：

主席好，各位好，我這裡是財團法人中央電台，剛剛有提到那個罰則的問題，因為你依照這個資安的等級程度來訂定罰則的時候，有沒有考慮到說各單位它們能夠應變到什麼程度？剛剛有一個，前一位有提到說，那我在我的設備上，我的軟硬體設備，我的這個資安防護的能力欠缺的狀況之下來稽核我，然後我沒辦法在你這個（時間內）提出改善。所以改善方案我也提不出來，因為沒這個設備去改善它。那你在訂這罰則的時候，我不知道這個罰則的範圍怎麼訂定說，它如果有設備，你罰到多少，那它如果沒有這個能力的話，你要去罰到多少。所以這個地方比較有疑問性，以上說明。

主席：

你只有這個問題嗎？好。這個智禾可以先說明一下。

資通安全處周智禾：

剛剛你講的罰則指的應該是母法裡面的第20、21條這邊。其實這邊指的罰則指的是說，依據這個法要求各個納管對象應該做的事情，應做沒有做。而不是說你資安防護做的不好，然後導致駭客入侵，就會被罰，不是這個，沒有這種東西，我們主要是針對於說依照法裡面我們訂定的，你應該訂定實施資通安全維護計畫，然後要提出實施的情形，且要提出改善報

告等。你要做這一些事情，大概是這樣，如果沒有做才會有罰則。

主席：

原則上是應該先回歸到你的訂定及實施資通安全維護計畫這件事情，這是前提，就是針對你的組織裡面的資安風險，跟所要求對應的資安責任等級裡面，你應該去滿足到現在法裡面，或者是你自己的資安風險評估裡面所應該辦理的一些資通安全的防治措施，那這就是訂到你的資安計畫裡面。那未來不管是這個稽核，甚至內部的通報程序，其實就是依據你自己之前怎麼訂，那你未來就是要怎麼做，那除非你自己怎麼訂，但後來沒有怎麼做，才會衍生後續的可能因為你自己怎麼訂，但後來沒有怎麼做，而後來衍生一些資安的風險，那才會針對那個部分去做一些檢討，跟請你們提改善報告，倒不是說，無緣無故就是去罰。原則上是這樣，一定是你自己一定要先訂好你的資安計畫，那大家就是照表操課，那未來其實就是看你有沒有依照你自己所講的東西去做，原則上是這樣子。

主席：

好，那有沒有其他的要提，我們今天其實參加的單位有財團法人國家文化基金會、同步輻射中心，還有金融消費評議中心，中央畜產會剛剛有提了，那還有漁業發展基金會、電信中心、法扶、榮眷基金會，還有兩家這個公股銀行就是臺灣金控跟臺灣銀行、臺灣菸酒公司，還有交通部臺鐵，臺鐵今天有到嘛？那臺鐵未來是非常重要的關鍵基礎設施，那還有中央存保，還有桃捷，這也是未來的關鍵基礎設施。好，那我就再次問一下還有沒有真的要詢問的？沒有，如果沒有的話那我們會議就要結束了喔。

臺灣菸酒股份有限公司代表：

主席，各位先進。臺灣菸酒在這邊做第一次發言。這邊有2個問題請教，第1個是說在那個資通安全責任等級的部分，其實這邊都有，辦理內容都有提到說，初次受核定或等級變更後1年內，或是2年內這樣子的敘述。可是像我們很多單位其實早就已經定義自己的責任等級。所以它這邊的初次受核定的定義是什麼？是在法令通過以後我們納管之後，往後算1年，還是怎麼樣算？那第2個問題請教就是說，我們在一般使用者跟資訊人員，大部分都有提到資通安全專業課程跟一般的課程，那所謂的專業的課程的定義大概是怎樣，像資通安全職能的訓練這個我們知道，就是行政院定期都會開，那像資通安全專業課程的定義，是像我們如果去像恆逸這樣

子的專業機構上課就算嗎？還是？請教這2個問題，謝謝。

資通安全處周智禾：

剛剛講的資安責任等級初次核定指的是法過了之後，中央目的事業主管機關送行政院核定，這個才是真的初次核定。對，那接下來就是每2年要重新再核定，所以是等法過了之後。那至於資安的教育訓練的話，例如你剛剛講的像恆逸這種開設相關的EC-Council，或者是（ISC）2的那種課程的話，其實裡面touch到大部分都是跟資安有關的，這一類應該都算是資安相關的課程。

臺灣菸酒股份有限公司代表：

謝謝。

主席：

好，請問還有要詢問或意見提出來的嗎？沒有，好。OK好，那這是我們親民黨的助理，陳先生。

親民黨立法院黨團代表：

那個副座以及各位先進大家好，我是親民黨團的助理陳治棋。其實我是比較想要求教於各位，因為其實前面各位綜合討論很抱歉，那個我沒有聽到，但其實我要先說明，其實我也不是資安出生的，其實我負責的是社會福利及衛生環境委員會的助理。我的專長應該是醫療法規才對，親民黨團的資安法是我寫的，那其實我比較想要請教各位的意見就是說，其實就是3月31號那天，就是我有聽那個政府機關的，他們其實發言還算蠻踴躍的，但是都集中在某些單位，比如說台北市政府他們就提出來就是說他們有上課的問題，就是公務人員指定的課程，資安訓練課程以及員額、預算，那現在也提出來就是說，他們的核心業務如果說他們要按照這個辦法裡面，就是說一年2次的話他們恐怕做不到，因為他們所有核心業務全部盤點完的話，要兩年的時間。那我不曉得前面的先進有沒有提到這些很執行面的問題，那我真的想請問各位就是說，這個子法這樣拼下來真的能執行嗎？而且我還看到就是桃園航空城事業處沒有來，雖然他們並不是一級的關鍵基礎設施，那我真的想請問各位就是說，各位財團法人，各位公營事業，公營事業可能比較有錢，他們可以委外去處理這個問題，但是財團法人，你們如果不吃飯你們有錢去委外去辦理這些？好，就算你們是三級好了，你們三年三級，你們有錢去辦這些東西嗎？我這個人是比較講求實際

層面的問題，我真的很懷疑，因為你們都不表示意見，那我們立法院也無可奈何，因為你們都覺得沒問題，執行沒問題，那你們好像錢都很多的樣子，你們都可以把業務委外去這樣辦理，所以就是我這邊想聽到各位真實的聲音這樣子，我是覺得它有很多執行面的問題，謝謝。

主席：

好，那我想我們還是回到法的本身，如果各位有任何建議，我們都非常歡迎可以提出來做一些建議上的修正。那我剛剛特別也提到就是說，各位提出來之後，我們在第二輪的部分還會找各位來，把我們的修正情形做一個說明，好，那各位還有沒有問題要提出來的？

親民黨立法院黨團代表：

不好意思，我這個人意見比較多，因為我不曉得，其實我沒有很仔細看子法裡面對於各位的懲處，那我還想請問各位，如果說你們委託辦理的機關違反了這些東西的話，你們要代為受過嗎？那如果說有觸犯到，就是違反了保密協定，或者就是說他有利害衝突的時候，那你們要怎麼辦？你們對於這種就是法根的事項你們沒有任何意見嗎？我真的很懷疑，尤其是公營事業，你們都沒有這方面的問題嗎？萬一你們的委外的這個事項有，萬一啦，真的發生了這些什麼違反保密協定，或者是說違反這個就是有利益迴避，或利益衝突的情況出現的時候，你們都沒有意見嗎？

主席：

好，各位歡迎提問，那因為我們還有第2輪，就是第2個3個子法的部分，那就還是我們就直接進到接下來的第2個部分就是3個子法的部分，那就看各位針對這3個子法有沒有意見要提出來。這3個子法主要是資通安全事件通報的應變辦法，還有特定非公務機關資通安全的稽核實施辦法，那還有資通安全情資分享辦法，有嗎？各位有要提出來的嗎？沒關係，我不知道各位對於這個子法的條文內容應該大概也有看過，我們今天承辦單位應該也有給各位一個書面的這個意見單，那各位如果會後真的又想到了，也都歡迎以書面的方式提供給我們。好，我再問最後一次，各位還有意見嗎？好，那如果沒有意見的話，我們今天會議就到這邊，謝謝各位參加，那再次重申各位如果後面有什麼意見，都歡迎用書面方式提供給我們，謝謝。

司儀：

非常感謝徐副處長及各位貴賓的蒞臨。那如果各位對於子法草案還有一些問題想要提問，歡迎寫發言單交給我們會場工作人員。我們會在會後做彙整。