資通安全管理法草案座談會逐字會議紀錄

時　　間：中華民國106年8月11日（星期五）上午9時30分
地　　點：臺大醫院國際會議中心402C/D
出席領域：政府捐助之財團法人

【記錄開始】
主持人：
　　我們今天資通安全管理法草案正式開始，我們有請行政院資通安全處徐嘉臨徐副處長為我們致詞，謝謝。
主席徐副處長：
　　各位與會的貴賓大家早安，今天非常歡迎各位可以來參加我們這一場資通安全管理法草案的座談會，今天主要的對象是政府捐補助的財團法人，首先將開這個會的目的跟各位說明一下，針對我們現在送到立法院版本草案的內容跟各位會比較關心的議題，各位等一下可以就你們關心的議題再做深度的意見交換。
　　第二個，我們現在針對母法草案的內容也有需要去訂定相關的子法，今天所做的回饋意見都可以作為我們後續訂子法裡面的參考。
　　第三個跟各位說明，我們這個會議會做逐字稿，等一下各位的發言意見都會逐字記錄下來，這個逐字稿後續都會公開在網站上，所以這個部分也先提醒一下各位。
　　等一下我們的議程，會先請我們同事先就資通安全管理法草案的內容說明，不會逐條說明，主要還是針對截至到目前為止大家所關心的議題來跟各位做一個說明，說明完之後我們就開放各位可以來做一些討論，我想今天議程安排就是這樣，我不知道各位針對這樣的議程有沒有特別的問題？如果沒有的話，我們就先請我們的同事就針對資通安全管理法草案做一個簡報，謝謝。
賴分析師：
　　謝謝主席，各位與會的代表、先進大家好，首先就資安處這邊就整個資通安全管理法草案做一個報告。這個報告跟以往比較不一樣，之前的報告比較針對法條的內容做一個說明，這次是針對立法草案過程中外界比較

關心的議題，以及跟國外的案例做一個說明，大綱就請參閱。

首先針對整個推動歷程做一個說明，這個資通安全管理法草案我們在去年8月底完成整個法案版本的修訂，也在去年的9月到11月召開7場說明會，這7場座談會大概有一些議題，我們後面會給大家做一個說明，也在12月的時候做一個策略會議的檢視，我們這個草案是在今年4月28日函送立法院，立法院是在5月底的時候交付委員會審查，目前第九屆第三會期是沒有審查到，只有完成一讀，會在下個會期繼續審。這個資通安全管理法草案除了我們在座談會上面說明外，也在去年9月到11月，有在國發會的平臺徵詢各位的意見。

這個是我們之前辦一些座談會還有一些平臺上的大家的聲音，在政府機關主要是針對人力跟預算的不足部分做一個反映；在民間團體的部分比較擔心重複稽核，所謂重複稽核就是行政院也去稽核、中央目的事業主管機關也去稽核，當然也有提出一個投資抵稅的建議，不過這個部分有困難，目前沒有辦法。

在之前草案的版本其實我們有一條是指定電商業者，授權由中央目的事業主管機關來指定，這一條因為有一些專家學者還有一些外面的反應，覺得這一條可能會造成法的不確定性，也怕政府會擴權，所以這個部分已經拿掉了，所以目前電商業者沒有在整個納管的範圍。在學者專家部分，有部分學者覺得這個罰則有些過重、有些過輕。

緊接著就整個草案架構做一個說明，主要是這五個核心，針對整個資通安全組織推動、公務機關跟非公務機關的資安管理、資安環境與產業發展以及資通委外服務管理，我們最重要目的是為了維護國家安全跟社會公共利益。這五個環有一些相關的規範跟外圍的相關規定範圍，我們會在相關的子法，甚至在母法裡面就會規範到。藍字的部分，我們未來會朝子法訂定去做一個規範，基本上我們現在有一個草案的版本，只是目前因為覺得這個內容可能還不是很成熟，所以沒有提供給各位，我們今天還是希望針對母法這邊做一個討論。

這個是我們整個草案架構跟國外主要國家法規做一個比較，主要是美國、歐盟跟新加坡，各位可以看到，我們資安管理法跟其他三個部分都是針對各公務機關；美國是針對聯邦政府，沒有針對非公務機關規範；在NIS的部分是關鍵基礎設施提供者跟數位服務提供者；新加坡網安法草案

跟我們資通管理法一樣，目前都還是草案的階段，還沒立法，不過他是針對關鍵資訊基礎設施提供者跟資安服務廠商去做一個規範。我們資安管理法草案非公務機關關鍵基礎設施提供者的部分，我們昨天已經開了座談會，昨天也有公營事業，還有一個部分第三類對象是政府捐助的財團法人，就是今天在座的各位。

政府捐助的財團法人目前有兩類，一個是中央政府捐助的，還有一個是地方政府捐助的，今天早上的場次是中央政府捐助的，地方政府捐助我們會在月底召開一場，原則上政府捐助的財團法人，我們會比照法務部財團法人法草案內容一致的規範，政府捐補助達50％以上就納管。目前FISMA沒有針對罰則等做一個定義以外，其他大概都一樣，因為美國FISMA是針對他們的聯邦政府，所以沒有對非公務機關的資安檢查，資安檢查就是行政檢查，所以也沒有相對的罰則。

針對各界關心的議題，我們大概臚列這些，後面做一個說明。第一個部分主要是規範對象，目前就剛剛報告的，除了公務機關之外，就是CI提供者、公營事業跟政府捐助財團法人，未來我們的立法推動，我們的規劃在施行的期程有做三階段的適用。原則上第一階段我們希望立法通過後半年，由公務機關優先適用，第二階段是立法通過後半年再半年，就是CI提供者，再隔半年是公營事業跟政府捐助的財團法人，大概有這三階段的推動。

第二個部分是針對稽核的部分，稽核可以看到比較表，我們國家跟美國FISMA都是針對資通安全維護計畫去做稽核；歐盟跟新加坡主要是針對資安相關的措施、必要的事項做一個稽核。特別要說明有關美國FISMA的部分有內外部的獨立稽核人員進行；在歐盟NIS的部分是有由各會員國自己去訂定；新加坡可由指派的人稽核人員辦理。

第三個部分是資安行政檢查，各位就是手上的第18條，這個部分也是各位非常關心的，我們行政檢查有兩個發動要件：第一個就是當發生重大資安事件的時候，什麼叫做重大事件？第3、4級就是重大資安事件，我們就可以發動行政檢查；另外一個是當發現資安維護情形有重大缺失，原則上是資通安全計畫被發現有重大缺失的時候，就可以發動行政檢查。美國FISMA沒有這種資安檢查，因為他是針對政府機關，所以針對非公務機關當然沒有相關的檢查；歐盟NIS跟新加坡網安法目前都有。

第四個部分是罰則，其實我們在管理法草案目前的版本，罰則我們訂一個期限改正的措施，我們不會因為不符合這個規定就直接開罰。原則上我們只有兩個情形會直接罰鍰，一個是拒絕行政檢查。資安管理法目前沒有針對公務機關人員做一個懲戒、懲處的規範，因為之前我們在過程當中人事總處有提出來，說不需要在資安管理法草案針對公務機關去做一些懲處、懲戒的相關的規定，因為公務人員有相關的法規，像公務人員懲戒法，就依其規定，不用在母法草案這邊去做一個規範；在非公務機關的部分，各位可以看到罰則，大概有10到100萬不等的罰鍰。我剛剛提到，拒絕行政檢查會直接開罰；另外一個是發生資安事件應報而未報者，我們就直接開罰，其他的基本上都有限期改正的規定，不會直接開罰。FISMA的部分沒有規定，因為他只針對政府機關；歐盟NIS的部分，是由會員國各自去訂定有效法則；在新加坡網安法比較嚴一點，因為還有有期徒刑的規定，以及換算達220萬台幣以下不等的罰金這些規範，以上簡要說明。

主席徐副處長：

我們就開始開放各位討論，有沒有哪一位先詢問？發言？

科技部：

我是科技部，因為我手上有兩個法人，一個是捐助50%，一個是未足50%，可是你們訂標準好像沒有確定，到底是不是未達50%要納入？剛剛簡報看起來是排除了，是不是確定了？

主席徐副處長：

我剛剛忘了說，我們大概先搜集三個問題之後，統問統答，剛剛是科技部，還有沒有下一個問題？

法律扶助基金會：

主席、各位先進大家好，我是財團法人法律扶助基金會的代表，我有幾個問題想請教一下，第一個是草案第14條，裡面敘述「非公務機關應訂立資通安全事件之通報及應變機制」，看到簡報第35頁附件3-4是非公務機關的通報流程，下一頁附件3-5左下角，這邊有敘述「現況通報方式為至國家資通安全通報應變網站填報」，請教一下，像我們這種非公務機關的話，之後也是去這個網站嗎？還是還有統一的平臺讓我們做填寫？

第二個問題，簡報附件2-5的部分，這邊有規範各個責任等級的分級的辦法，因為我有參加今年1月跟去年10月的會議，像B級，事實上裡面的

內容跟這次所提供的內容好像也有所差距，不知道這個地方是否還有轉圜或是修改的地方嗎？

接下來的問題比較細一點，因為今年我有開始做教育訓練的事情，像我們基金會在各縣市都有一個分會，我們這邊只能採取北、中、南各辦一場教育訓練，但是這樣還是有同仁沒有辦法參加教育訓練，教育訓練是否可以透過線上的方式？或是我錄影，他之後來觀看這樣的方式？之前有說教育訓練完要通過評量，我這邊又遇到兩個問題：第一個，評量他的方式可以用線上還是紙本的方式？考卷內容是我們單位自己出嗎？還是我跟主管機關討論？通過評量方式它有一個分數嗎？

主席徐副處長：

我可不可以確定你剛剛說的教育訓練是指什麼樣的教育訓練？你們要對誰辦？為什麼要辦教育訓練？

法律扶助基金會：

附件2-5有一個教育訓練，一般使用者/主管（宣導）每年要3小時的教育訓練。

主席徐副處長：

你是指應辦事項裡面的教育訓練是不是？

法律扶助基金會：

是的。

主席徐副處長：

所以你們現在原本就有在辦？

法律扶助基金會：

沒有，是去年我參加會議的時候，所以我們今年才會試辦一下，提早因應。

主席徐副處長：

了解，你剛剛特別提到的評量方式，也是應辦事項裡面的評量方式？

法律扶助基金會：

對，因為今年1月的B級有評量，可是這次的已經沒有了，確定一下，如果之後沒有評量的話，這個問題就不存在，謝謝。

主席徐副處長：

我們再蒐集一個與會者的意見。

中央廣播電臺：

我是中央廣播電臺，剛剛那位先生提到教育訓練，我們也是有辦，不過隔1、2年會付費請外面一些專家，既然行政院也有辦這樣的訓練課程，是不是可以仿照我們上的環境教育宣導課程？這些政府單位的課程也可以釋出，讓各單位用影片觀賞的方式，這樣統一，不管要做評量或是宣達政令，也可以達到它的目標，以上報告。

主席徐副處長：

有關教育訓練我想請敏慧這邊回答；有關現在政府捐助的財團法人它的那條線畫在哪裡，等一下會請婉萍幫忙回答；接下來還有一個法扶剛剛提的，第14條通報應變的流程到底怎麼做，請世榮說明一下。先請婉萍回應今天大家比較關心的，到底政府捐補助的財團法人那個線要畫在哪裡？這個部分我先請婉萍說明一下。

李科長：

關於政府捐補助的財團法人到底佔基金份額比例多少？我們目前規劃的文字是寫「超過50%」，目前是參考行政法人法草案的規定，當然行政法人草案它還有很多其他特殊要納入該法規範法人的形態，但是在資安管理法這邊我們只看政府的資金在財團法人的基金所佔的份額，我們現在規劃的文字是超過50%，用法律的觀念來看，超過就是不包含，目前規劃是這樣，後續跟各位開會之後，資安處這邊有沒有可能做調整？可能是之後才會有定案。

主席徐副處長：

原則上我們現在規劃就是超過50%，接下來請世榮說明一下現在通報的流程跟怎麼通報。

賴分析師：

我補充一下，剛剛婉萍口誤，剛剛說成「行政法人法草案」是「財團法人法草案」。

各位可以看到投影片這邊，我就先講公務機關，因為在座其實也有公務機關，雖然公務機關有一些…我直接講非公務機關，因為我怕時間受到影響，因為公務機關都清楚。

各位在座幾乎都是中央政府捐助的財團法人，所以原則上我們會依通報應變流程來做說明，我們未來也是會以資通安全事件通報及應變辦法這

個子法去做規範，那個規範裡面有針對公務機關跟非公務機關，這個是非公務機關，從這個流程圖一開始知悉資安事件，並不是發生，所以在座各位只要知道有資安事件趕快通報、疑似也趕快通報。向誰通報呢？當然向中央目的事業主管機關或者是地方政府通報，在目的事業主管機關跟地方政府收到這個通報的時候，他會判斷這個是不是屬於3、4級重大資安事件，如果是的話，他一樣會通知行政院；如果不是的話，會進行事件的審核，也會判斷是否需要其他機關的協助，包含行政院的協助，大概是這樣子。

我們在非公務機關的部分，沒有說在知悉資安事件要1小時內通報，原則上目前沒有這樣規範，原則上各位只要發現或知道資安事件，疑似這些情形，就趕快向你的目的事業主管機關通報。目前通報方式原則上就是向那個平臺，那個平臺是建置在我們技服中心一個網站去通報，未來這個子法裡面我們也會在附件說明跟各位要在哪邊通報，基本上這只是一個通報流程，各位要在哪邊通報，我們之後會有一個統一的平臺，以上。

主席徐副處長：

我再補充一下，非公務機關要向中央目的主管機關通報是一個程序，中央目的事業主管機關到行政院是一個程序，剛剛世榮講那個平臺，是通報到行政院這邊的時候有一個技服中心的通報平臺，但是非公務機關到中央政府這一段，這個通報的方式可以由中央目的事業主管機關來訂定，通報的方式像是電子、傳真類似這樣的方式都可以，目前我們在子法裡面有這個規劃，跟各位做一個補充。

接下來有關教育訓練跟人員評量的部分我請敏慧說明一下。

劉組長：

有關應辦事項裡面資安教育訓練的部分，它有A、B、C、D不同等級，但是基本上我們把同仁分為四個部分，一個是一般的主管、資訊人員、資安人員跟一般的使用者，資安跟資訊可能需要接受12個小時的訓練，一般的使用者跟主管需要3個小時，其實這個課程只要機關自己自辦，你們可以自己找老師、自己出題，一定要有評量，因為有人可能會簽個到就走了，我們是希望這個訓練是可以落實、對大家有幫助，所以原則上是授權給機關自己出題，只要你們做的評量通過就可以了。

另外在課程分享部分，其實我們在這幾年來也做了非常多的數位課程

，已經放在人事總處的平臺上，大家都可以登錄去申請帳號分享，所以目前我印象裡頭還有3、40個小時有關資安的教育訓練，大家可以上去使用。

主席徐副處長：

接下來還有沒有人要提問的？

農委會：

長官好，我這邊農委會，幾個問題想要請教一下，因為在財團法人法的草案規劃裡面，如果他的業務涉及兩個縣市以上的話，他就是屬於全國性的財團法人，他的目的事業主管機關就是各個中央目的事業主管機關；如果他只單獨在一個縣裡面的話，他就是地方性財團法人，他的主管機關就是地方政府，不是以捐助的人是誰來做這個區分，這是第一點。所以在通報的部分，假設我們有一個財團法人他是位在臺北市，請問他的主管機關如果是全國性的，可是他人在臺北市的話，他是要向中央政府和地方政府都要有通報的機制嗎？這是第一個問題。

第二個問題，因為財團法人法的草案裡面也有一個規定，好像這些政府捐助的財團法人，有所謂的公轉民、民轉公的相關規定，假設今天政府捐助財團法人超過50％，他因為接受民間的財產又納入基金，他低於50％的時候，是不是這個時候就不納管了？以上兩個問題，謝謝。

主席徐副處長：

第一個問題我先釐清一下，你剛剛說的財團法人，我們前提是他一定是要政府捐補助超過50％，你剛剛說跨縣市，如果他不是政府捐補助超過50％，基本上就不納管。

農委會：

應該這樣說，財團法人法草案把財團法人從基金的部分分成政府跟民間，從他的業務範圍分成全國性跟地方性的，全國性的財團法人他的主管機關就是中央目的事業主管機關，如果農業跨2、3縣市的話，就是我們農委會；如果他只在單一個縣市的話，他的主管機關當然就是那個縣市的地方政府。這些都要有一個通報機制，財團法人跟主管機關報相關資通安全管理的措施，請問他的申報機關到底是跟著財團法人法，所謂全國性的財團法人就跟中央目的事業主管機關？還是今天我在臺北市，除了中央目的事業主管機關外，我還要跟臺北市政府來申報？

主席徐副處長：

你剛剛前面講的是，他現在分成是從政府捐助的基金面去看跟業務面去看，我們這個資安法裡面規定是從基金面去看，不是從業務面去看，我看的就是你的基金是不是政府捐補助超過50%以上的，我們才會比較關心，政府捐補助如果影響一些國家安全或者是民眾生活，是我們關心的財團法人範圍，至於他的業務不是在我們現在認定的主要範圍裡面，這樣可以回答到你的問題嗎？

農委會：

我的意思是，今天我是財團法人的時候，請問我這些文件交給的主管機關，假設今天這個財團法人業務是全國性的，我人在臺北市，只要跟農委會講？還是跟臺北市政府？

主席徐副處長：

不管是全國性還是地方性，我只認定農委會捐助超過50%或地方政府捐助超過50%，才是這個法的規範，我是看你捐補助的規模，不是你前面說他的業務範圍。

科技部：

我上次有跟資安處同仁提過這個事，後來因為跟我沒關係，我就不來亂了，我想可能有一個名詞上要定義，是「設立基金超過50%」？還是「累計捐助超過50%」？這個裡面有差別，他每年還是會接受外地的捐助，加總起來有沒有超過50%？一種是設立的時候這一塊，成立的時候那個基金有沒有50%？差別在這裡，因為我們沒有這個問題，所以後來我就沒有繼續這個問題。

主席徐副處長：

目前規劃的是累計超過50%。

親民黨立法院黨團：

不好意思我建議一下資安處要回去好好思考，預算法本身…我是親民黨立法院黨團，我很誠心的建議，第一個我要說明我的立場，我是反對行政院版；第二，我們就法論法，我們完全從技術層面來看這個問題，你們應該參考的是預算法裡面有關於財團法人，裡面是規定捐助50%以上，預算的部分主管機關就要送給立法院來審議，你們用這個法條的話，不是就輕鬆解決很多人的問題嗎？他的資安計畫要誰去管？他有多少範圍要納進

去？你們為什麼不用已經現成有的法條？因為現在所有財團法人的預算都送來立法院，其實立法院也沒有能力審，你的主管機關也解決了、範疇也解決了，財團法人法哪時候會通過還未定之天，可能還要吵一陣子，你現在就要一個草案來規定另一個草案的範疇，這不是很奇怪嗎？你們再跟你們自己的法規部門研究一下這個妥適性，我是這樣建議，就會有一個很清楚的範疇，謝謝。

主席徐副處長：

我先回答一下剛剛農委會提的問題，你剛剛的前提是這個財團法人已經是政府捐助超過50%，至於未來誰來當他的主管機關？這個我們可以納到未來的細則去看，原則上他一定是找一個主管機關就好了，不會通報兩個，這個是原則，這個部分再跟你做一個說明。

有關財團法人的認定，我們知道按照預算有那個規定，我還是請法務部的人針對我們當時在思考的方式幫忙說明一下，目前財團法人法在考慮財團法人納管的範圍主要的線到底在哪裡？

法務部柯專員：

主席、各位先進，法務部發言，有關於財團法人法就像剛剛先進講的，其實現在還是草案，照資安法的規範裡面，其實政府捐助財團法人的範圍原則上是依據財團法人法的範圍去訂定的，因為現在財團法人法也還是草案，所以現在兩個範圍是不是一定會一致也還沒有完全確定，不過以現行來看資安法的規範，應該不會擴增到變成準用財團法人法的情形，應該是很明確，他的財產來自於公部門的部分是合計超過50%的情形。

至於剛剛有先進提到，可能財團法人之後來自公家部分的財產比例上變少了，當然這個部分有牽涉到財團法人認定的時候，還是要回歸到財團法人法，如果這個立法通過之後，以主管機關對這個部分的認定為主。

主席徐副處長：

原則上我們還是把那條線先畫在哪裡，就是政府捐助超過50%以上，當然後續有調整，可以照後續的程序去做，譬如你的基金母數可能突然變多了，你可能就不是在50%之內，後續有程序做這樣的作業。

親民黨立法院黨團：

首先我還是強調我是反對行政院版的，以下都是技術性的討論，我不太了解你們是學資訊的，為什麼你的做事情或回答答案不能1就是1、2就

是2呢？我真的很疑惑，你們為什麼要用一個那麼模糊的答案？因為以後財團法人法通過，我們可能會改成從捐助50%變成累計母數。我可不可以請教你們，你們這種變動、跳動立場的原因是什麼？你們會覺得改成母數累計超過一定數額才要納管所持的立法理由是什麼？能不能說明你們為什麼要變動的理由？

如果不能說明的話，為什麼不能按照現行的程序去做呢？因為預算法這個規定已經運作一段時間了，所有的財團法人捐助50%以上的，他們都把預算書送到立法院，所有主管機關都很清楚，他的財團法人在什麼地方、哪些人要納管，那個那麼簡潔、大家都已經有運作習慣的程序你們不採用，還要跟你們不確定哪時候會通過的另外一個草案，你要跟它連動，我不曉得你們的邏輯思維是什麼？你們應該是最有邏輯思維的一群人。

主席徐副處長：

預算法裡面規定是50%沒有問題，他的50%一定有母數跟分子…

親民黨立法院黨團：

因為我不是主計處的人，我只能告訴你那條法規已經修正很久、運作很久，哪些財團法人是屬於主管機關要送來立法院都很清楚了，如果你們為了求行政簡便，大家做事情很方便的話，我建議採取這樣的判斷基礎就好了，你不用去跟隨一個你不確定哪時候會通過、哪時候會修成怎麼樣的法去走，我不懂你的目的跟邏輯為何？我質疑的是這個，你為什麼要去跟隨一個不確定的變數去決定哪些人要納入你的管理？事實上我根本不需要幫你提出這個質問，因為我根本就反對你的版本。

主席徐副處長：

他們的概念其實很像，因為我們現在已經是50%，你剛剛有提到預算法既有的規定。

親民黨立法院黨團：

我真的覺得行政的法規部門自己要去做協調，不要用不確定的法律概念去做你的決策，我真的很誠心建議你們，你們自己去找主計總處的人去看看，到底這樣做會比較簡便，還是你們那個不確定的法律概念會比較簡便？

主席徐副處長：

這個沒有問題，但是剛剛他們關心的問題是，50%(政府捐助財團法

人之比例)不會永遠不變的…。

親民黨立法院黨團：

他們會有這個疑惑就是因為你提出一個新的東西，如果還是按照原本舊的標準，現在這個東西已經有在運作，你自己去問各主管機關負責主計處的人，他都非常清楚，他底下有多少財團法人的預算書是要送到立法院的，就是以這個範疇作為你納入資安管理法管理的範疇，這不是很簡便嗎？只要資訊長或是資訊人員去會同他自己部裡面的主計機關，他就可以知道他底下有多少的財團法人、他要去管多少的資安計畫，這個不是很清楚嗎？這麼簡單的邏輯，我不太了解有什麼困難懂的？當然你們覺得你們要管理的範圍要極大化，大家都把清單算出來，你們公式化會把你們要納入管理的範疇極大化，大家都把那個清單提出來，看看哪一個清單比較多，如果到時候立法完全偏向於行政院版的話，大家再來決定到底要採取哪個計算公式。

主席徐副處長：

我想你的意見跟我們現在的概念是一樣，我要再說明的是，剛剛大家講到，那個母數會變動，可能現在是50%以上，未來可能會不是，立法院未來也是會遇到這樣的問題，他一定有一個程序來做調適，這個關鍵問題在於，假設我未來的母數變大，我可能就不是在那個範圍的時候，那個程序可以怎麼做，我們在解釋是這個議題。

你剛剛那個議題跟我們現在所要做的範圍概念是一致，因為大家都是捐助50%以上為目標，但是他一定會有一些名單上的落差跟變動，所以我必須對這個部分再做一個說明。

我再徵求下面各位的意見，各位沒有特別的意見要表達嗎？

中央廣播電臺：

有另外的問題，我們把這個有問題的事件通報上來，但是我們要自己解決，還是行政院要派人協助？因為很多東西可能牽涉到技術的、有可能牽涉到你的設備的，這個問題有時候不好解決。我建議如果比較嚴重的，不管是任何單位可能會在這個上面卡住，建議行政院動用他自己的資源主動協助，比如這些財團法人或者這些相關的單位，能夠幫助他們，開這個會議作草案的規範說明，它的目的也是這樣子，所以行政院盡可能幫忙單位、協助他們資安問題的解決，以上報告。

主席徐副處長：

接下來有沒有第二個問題？

財團法人農業科技研究院：

長官好，我這邊是財團法人農業科技研究院，有關於簡報附件2-3，資通安全責任等級分級辦法規劃內容，我們這邊的問題是，在C級跟D級的部分有點模糊，C級是「下列機關具自行或委外開發資通系統，並設置伺服器者」，第一個想請教的是，資通系統部分是指對外有提供服務系統的部分嗎？如果我們對內使用的員工系統算不算資通系統？第二個，如果我的系統建置在虛擬主機空間上面，是不是就不用納管了？這個部分再麻煩，謝謝。

主席徐副處長：

接下來還有沒有問題提問的？

工研院資通所：

主席，我是工研院資通所，我想要請問簡報附件2-5，比較技術性的問題，那些認定，管理面所謂的「核心系統」是怎麼定義的？因為我們看到弱點不見得是在server上，很多可能是從員工的機器開始發生，慢慢進去，所以我想要定義所謂核心系統，到底這個滲透測試或者是弱點掃描涵蓋面要到多大才符合？每年2次或1次的網路弱點掃描、滲透測試有一個規範嗎？做到多少規模有沒有一個認定標準？還是只要有做就算可以？我到底要做到涵蓋多少標準才算完成？有沒有這些相關規範的說明？

主席徐副處長：

第一個我先回答，剛剛問到通報的時候行政院可不可以提供協助？其實通報有兩個目的，一個是用來做損害管制；第二個希望能夠提供需要的協助。以我們現在大概的做法是這樣，當你遇到一些資安事件，你能夠處理的話，就自己先處理；但是如果你不能處理的話，在通報流程上面有一個菱形的部分「是否需要行政院協助？」這個目的就是你在網上通報的過程中，就可以請求協助了，如果這個資安事件真的很嚴重，到行政院這邊，行政院一樣是可以看今天受發生的資安事件需不需要提供協助，通報的目的也是希望如果真的需要我們協助的話，是可以提供這樣協助的服務，這個就是通報的目的，這個可以先回答到你的問題。

第二個是有關農業科技研究院，他問有關C、D級的部分，目前的規劃

是你要有自行委外開發的系統，並設置伺服器，原則上目前是這樣，現在目前你只要有建置就是納管。但是剛剛有特別提到雲端服務算不算？其實雲端服務也算是一種委外服務的形態，所以它應該基本上是，因為不可能你的服務放在雲端，你就不管他，因為他畢竟還是你自己在維運的一個系統。但是我們必須先說明，目前訂的A、B、C、D級，先這樣訂，今天也可以來聽聽各位的意見，針對你們實際在執行業務上，譬如政府捐補助財團法人裡面你們針對這樣的東西，未來在適用上有一些問題或者是需要建議調整的部分，這個都歡迎各位提出意見，這個只是現在目前先暫定的規劃。

剛剛後面還有一個問題，何謂核心系統？這部分我請婉萍先說明一下，現在所謂的核心系統是什麼？其實是有一段話在定義，但是沒有在這個簡報上面做呈現，我請他補充說明一下。

李科長：

我們現在規劃中的分級辦法面有一個附件，請機關針對自己系統的機密、完整跟可用性風險等級做區分，如果照那個表做完區分之後，機密、完整、可用性裡頭的風險有任何一項為高風險的話，那一項系統應該要被機關定義為他的核心系統。另外一個，如果依照這個方式都沒有任何高風險的系統，凡是支援核心業務必要的系統，就會請機關定義為自己的核心系統。如果是共用系統的部分，機關才有這個問題，財團法人應該沒有共用系統的問題，這個是我們對核心系統的定義。

主席徐副處長：　　另外一個問題，剛剛有一個先進請問，如果做滲透測試等等，應該做到什麼程度？我們請敏慧說明。

劉組長：

其實關於應辦事項裡頭的一些要求，包括像做資安健診、滲透測試、弱掃，我們在102年已經有把這些SOC這些服務納入共契，過去是在臺銀的平臺，今年開始彙整到共契，目前有五項，包括資安健診所、SOC有分高、中、低三個流量、弱掃、滲透測試跟資料風險這一塊，到底要做到什麼程度？我們在共契裡頭都有一些基本的要求跟服務，廠商一定要做到這些東西。當然如果你們不想買共契，想要另外開RFP，其實可以參考這個內容，再外加上你們的需求，以上參考。

主席徐副處長：

我再補充一下，剛剛其實你應該特別關心到底滲透測試的範圍要做到哪裡，我們現在的說法是，其實你只要核心系統做就好了，如果經過你的風險評估出來，它不是非常重要的系統，倒不一定要做。但是也必須提醒一下，雖然那個系統有核心、非核心，但實務上會相互影響的，講到技術面，如果在機關那個網段、或組織那個網段沒有切得很乾淨，在資安事件會受跳板式的逐一擴散，這個部分還是會先提醒一下各個組織注意這個資安事件，但是原則上我們還是以核心系統為主。

各位還有沒有其他的建議？

法律扶助基金會：

我是法扶的代表，因為上一位問的問題，我想細部延伸一下，他有講到滲透測試跟網頁的弱點掃描，因為我有研究共契，事實上有分黑箱跟灰箱，我有問過，他1年只能做一次黑箱或是灰箱，我們每年要交付測試嗎？還是我們只要做其中一個箱子就好了？

第二個是附件2-5簡報，一般事項，像系統分級跟防護基準符合的話，這邊寫1年內完成，不知道有沒有修改的或是放寬的餘地？謝謝。

主席徐副處長：

你剛剛說的是資通系統分級1年內完成那個嗎？

法律扶助基金會：

對。

主席徐副處長：

跟防護基準符合1年內完成嗎？

法律扶助基金會：

可能第一次我發言的時候有點緊張，沒有說清楚，舉例來說，現在B級的規劃跟今年年初1月的B級好像有點落差，當然修改一定有他的背景跟原因在，主要劃分A、B、C、D級，由主管機關所畫定的，從1月到現在，B級好像變得更嚴苛一點，不知道有沒有可以轉圜的餘地？謝謝。

主席徐副處長：

接下來還有沒有其他的問題？目前這幾個問題都比較關心資安責任等級應辦事項，你剛剛特別提到共契裡面有黑箱跟灰箱，我覺得他有不同的目的，如果你從駭客在外面攻擊的角度來講的話，當然原則上一定是黑箱要先做到，因為灰箱可能是內部再去做滲透測試，基本上就是看你的資源

，這個部分倒沒有一定要的規範，一定要做到黑箱或灰箱，就是看你的資源跟優先順序去做調配就可以了，沒有強制的規定。

接下來有提到資安責任等級的事項跟你去年看有調整的地方，確實是沒錯，因為我們行政院還在持續蒐集各界意見，所以還是在調整當中，也就是說就今天的版本，不管是會後或者是等一下，你們有一些需要可以建議的事項，都歡迎你們提出來，尤其是像資通安全系統分級還有防護基準的符合度，假設這個立法通過之後多久時間內完成，而不是要求你立法一通過就要完成，這個在各個受管機關施行上一定會有所難處，所以像在B級裡面就有特別強調，是在1年內完成，所以未來在A、B、C、D各個等級的設立上，應該都會加上這樣一個條件，不會一通過就馬上完成，大概不會有這樣的做法，這也是你從過去看到現在有調整的原因，這也是一個調整的重點。

各位有沒有特別的建議？

中央廣播電臺：

我是中央廣播臺電，第三次發言，因為相關這些都是要花錢，像很多財團法人包括我們自己單位，每年都被砍預算，你訂了那些，我也沒有設備、也沒有東西，我怎麼去執行？不管是核心、非核心的業務那個都是要花錢的，如果在資安要達到你要求的，不管是A、B、C、D等級這些所有的檢測問題，如果真的要做到比較完美、完善，行政院應該針對這個計畫案做一個統一、統合的統辦預算，固定撥補各單位到底是什麼等級的，自己也沒有錢，不可能去做這個事情，我怎麼去達到符合你這個要求？最嚴重的問題就是出在這裡，請上級機關了解我們財團法人這個單位自己本身困難的問題在這裡，謝謝。

主席徐副處長：

還有沒有其他的問題？

工研院資通所：

我是工研院資通所，現在再補充一個技術問題，現在看到資安的防護範圍我覺得還是在網路的安全、核心資訊系統為主，但是到現在很多的攻擊已經很少是從Internet他看到的就可以打進來，大部分是社交攻擊，或者是一些關鍵的人員，從他的手機或他用這些電腦系統成為一個跳板，我們幾乎沒有對行動安全的管理，或者是對於那些掌握核心資安情報的人，

有些主管本身就有比較高的權限，對於他使用的那些系統或這些行動裝置或IOT設備，有比較必須特殊的機制去管理，不然的話，會覺得對外防得很嚴，但是裡面這些關鍵每個都是漏洞，不知道現在立法有沒有考慮到這個層次？因為這種行動資安或IOT的管理在國外已經蠻多公司都有自動Solution，但是我們現在似乎是沒有考慮這一塊。

主席徐副處長：

接下來還有沒有其他的？

營建研究院：

各位好，我這邊是營建研究院，我們雖然在成立的時候是受政府的捐助，可是因為之後我們每年都沒有受政府的補助或捐助的狀況，所以我們所有的經費或人力其實都是自給自足的，如果要依照政府現在資安法去做的話，那些設備可能要像剛剛先進所說，需要一些昂貴的設備，我們要考量的就是經費的問題。

第二點，因為我們每年均不受政府捐補助的狀況，所以我們也沒有辦法去下共契單，我們光這一點的狀況就屬於比較弱勢的狀況，不知道這樣是不是可以爭取到一些補助？謝謝。

主席徐副處長：

自給自足是說政府捐補助的部分你們還超過50%？

營建研究院：

我們雖然是超過50%，可是因為我們每年都沒有受到任何的捐補助的狀況，每年的補助的經費之類的，每年的費用其實是我們自給自足來的，加上我們同仁曾經有去反映我們可不可以下共契單，他們給我們的回應，因為之後我們沒有再收過政府的捐補助，所以就沒有這個資格去下共契單，相對的，我們要採買任何東西的費用都比較高。

主席徐副處長：

大家有反應經費的問題，經費問題在公務機關也都是有這樣的問題，因為政府的經費也是逐年都一直再被遞減，這是同樣問題，但是我們的原則基本上就是資源花在刀口上，假設你是一個政府捐助超過50%的財團法人，一定是把資安資源放在非常核心的系統裡面，所謂的核心會從CIA的角度，服務中斷以後影響到的效益是非常嚴重的角度去看。這裡面所列不管是管理面、技術面跟教育面，一定是從核心的業務去做著手，所以第一

個，資源絕對不會是無限上綱不斷的投入可能不是非常重要的系統。既使是這樣，可能還是有一些資源不足的問題，我覺得這個問題我們可能會納入思考，看後續怎麼跟主管機關討論，因為這個問題假設它是一個需要做防護的系統，當然就必須做到一定的防護，這個部分可能容我們再去跟相關的機關做一些研議，先跟各位回答這樣的問題。

第二個，有關工研院資通所有提到行動安全，因為資安責任等級是一個原則性的規範，不可能會規範到非常細的東西，其實資訊的科技發展一直不斷的在演變，現在有行動、未來有雲端、甚至有大數據、AI，這種東西慢慢陸陸續續一定會延伸到公務機關或非公務機關裡面去做運用，一樣秉持這個原則，你還是從管理面、技術面跟認知教育訓練的部分去做著手，我舉例來說，譬如你在技術面做評估的時候，就發覺你有一個AI的技術需要去做防護，你就是在這個資源去做適當的調配，我們這邊不會規範到非常細的技術上細節。

以公務機關來說，特別容易遭駭的，使用者端一定是一個很容易遭駭，因為駭客其實很喜歡用竊取資料的攻擊，就是寄一封假冒郵件給你，你可能點了，這個病毒或木馬程式就開始在組織內擴散，所以為什麼有針對人員做教育訓練的原因是在這邊。以我們公務機關做法，我們還會要求各機關要做社交工程的演練，行政院也還會再對各機關做一次大規模的演練，目前我們公務機關是這樣做的。

回到非公務機關、組織面或者是財團法人，倒沒有這樣強制規定，這個部分目前還是先用教育訓練的方式，來去提升同仁的資安意識，當然各個組織裡面有需要精進的做法都是可以的，這個部分我們沒有提高到非常高的資安要求，這邊再跟各位做一個說明。

經濟部資訊中心：

主席好，這邊是經濟部資訊中心，之前其實我們在討論財團法人分級我們所屬有提到，有一種狀況，財團法人的行政人員可能都是由我們機構內部人員去兼辦的，他們所有的作業也在機構裡面，這樣的狀況到底要不要納入？因為我看了一下，我們就有一個捐補助100%的財團法人，它的人員只有3個，捐助金額只有40幾萬，這樣的狀況下還要他們再去做這些事情？剛剛提到錢花到刀口上，可是他們最主要的任務不是資安，他們大概也不會有多餘的經費再去做這件事情。其實這個問題在我們之前討論有

關財團法人的時候，就曾經提到過，可是在現在的版本來看，是完全沒有考量到這個部分，謝謝。

主席徐副處長：

接下來還有沒有其他的問題？

文化部：

主席、各位與會的先進大家好，我這邊是文化部第一次發言，承接剛剛經濟部所提，剛才中央廣播電臺也提到，今天一開始就提到，到底財團法人的納管標準那線到底在哪裡？剛才主席跟相關的先進也提到，是以政府機關累計捐助的佔比達50%以上，原則上現在是寫這樣子。剛剛經濟部也提到，事實上我們之前在談財團法人納管的標準時，曾經有很多的先進都提到，即便政府機關累計捐助的金額是達50%以上，但像一些文化部補助的財團法人，可能他捐助金額的總額不到100萬，可能才4、5、60萬，並不像一些比較大的基金可能達千萬或上億，如果我們捐助的總額未達百萬，但是這個捐助的金額卻佔基金總額的100%，事實上依照現在的標準、那條線，他就是納管，將來要投入做一些資安防護經費，事實上都已經超出我們捐助的額度，是不是不成比例？

經濟部也提到，我們之前討論時有講過，有些我們的基金主辦業務的同仁都由機關內部的同仁兼辦，如果沒有符合獨立的辦公場所，或者主要業務均由機關同仁兼辦，就是不予納管，不曉得現在的標準是不是還有含括這點？以上兩個問題請教，謝謝。

主席徐副處長：

我再接受一個問題。

陳映竹助理研究員：

你好，我是臺經院陳映竹，其實我今天有一個疑問是比較好奇，今天我如果做了某個部會的網站，或者經營這個系統，第一個他的系統可能是在部會的資訊機房裡面，這樣我可以很安心我的系統是安全的，如果照這樣的標準來看的話。

第二個，如果我們今天是委外建置，可是系統在我們家的主機，你又說要參考核心業務，但是在整個計畫案的核心業務可能不是做這個網站或是這個系統，只是其中一個方法而已，它並不是我整個計畫案的核心業務。

第三個，如果我今天把這個系統的建置是委外給第三方的廠商來進行建置、規劃，甚至是放在國外雲端伺服器時，我要怎麼去評估怎麼樣做這樣的資安風險管理？同時，我在資安維護上我要付給檢測公司非常高的檢測費用，但是完全不是我整個計畫的核心業務，這樣不是在增加我的營運成本嗎？

主席徐副處長：

我先就我能說明的先說明，剛剛經濟部有提到，假設受歸管財團法人人員很少，行政業務都是由主管機關兼辦，如果這個規模很小，假設我們現在暫定的這個分級原則來看，他是不是有自己維運資訊系統？假設沒有的話，基本上他就落在D級，D級不會去管他；假設他有核心業務，而且有自己管的系統，他可能就是需要被管理的對象，就是在這張表裡面。你剛剛提的範圍，他有沒有自己自建或者是委外資訊系統？假設這個規模很小，我想他不一定有自建或委外系統，可能到時候他就被歸到D級去，D級就沒有剛剛前面說要做的這麼多的應辦事項。

剛剛文化部有特別提到，可能捐補助的金額很小，但是我們現在是拉到50%，這一點我們後續可以納入考慮，我們在訂要納入財團法人的標準，可以訂一個捐助的門檻，可能捐給他10、20萬，也要納入嗎？這個部分是我們可以再考慮的，容我們後續再做一些討論。

剛剛臺經院有提到，如果是委外放在雲端，雲端怎麼去做評估？今天不管是用雲端或自己建，以我們政府機關來說，都有一定的風險，你就必須去做評估，如何評估可能不是在我們這個法規裡面去說明的，但是其實現在很多的雲端服務透過一些認證機制，是可以讓你分出哪些雲端服務是好的、壞的，你其實是可以去學的，所以以我們政府機關來說，我們現在的原則是這樣，國發會訂有一個資料中心的管理作業原則，裡面有訂一個，在政府機關裡面原則上是使用國內的雲端服務，當然財團法人不在這個規範的範圍，但是我必須強調，當你在做一個系統的建置，你會考慮的風險是很多面的，不管是你的data是要放本地或是國外，都是可以的，但是你必須看它的風險在哪裡，如果你覺得你要放在國外的雲端資料中心，可能有一個風險，譬如未來發生資安事件，你要請他調閱紀錄是困難的，如果你認為這個風險是你必須要去正視的話，你就要思考要怎麼去做下面的，或許你可以考慮不要放在國外，或就是放在國內。假設你一定要放在國

外，你有哪些資安的配套措施去做，這個是我們一般在做資安管理上面所採行的做法，至少我在實務面的做法可以先回應你。

不管是A、B、C、D等級，還有資安責任等級，還是從風險跟核心系統的角度去做出發，不知道這樣沒有回答到你的問題？還是需要再進一步再跟你回應的地方？你剛剛說評估檢測這個部分都要付費，如果機關或者組織可以自己做的話就自己做，當然也有人在幫忙機關或者是組織做這樣的服務，你要不要委外或者自建都是可以由機關自己來評估的，大概做這樣的說明，不知道各位還有沒有其他的問題？

金管會：

我是金管會的代表，今天我們討論的問題有一個很根本的問題，到底財團法人是什麼樣的標準可以列入？剛剛聽到很多先進提到，其實財團法人有很多不同的態樣跟形態，先進提到的那些態樣，我這邊有一些建議，是不是我們訂一個標準？因為剛剛提到捐助50%，我覺得那個標準太簡單了，這個將來在執行上會有很多的問題，我們現在討論都知道，就現況來說就有這麼多的問題，所以我這邊建議，是不是那個標準可以再做一個通盤的檢討？現在這些態樣各部會可以蒐集一下，大概目前的態樣是長什麼樣。

像資安為什麼要管？是因為你有重要的資訊才要管，如果你沒有重要的資訊是不是就排除掉了？像這個也是可以納入一個考量的因素，你是不是要納管的一個很重要關鍵因素。像剛剛講，雖然捐助金額超過50%，可是他就是沒有什麼資訊，即使他的系統被駭了，也沒有什麼關係，因為我沒有有價值的資訊時，那個資安對我來說就不是那麼重要；反過來說，也許捐助的金額很小，但他掌握的資訊是機密性很高的，這個要不要管？這個無庸置疑是要管的。我建議在定義我們這些要納管的這些財團法人標準可以做一個通盤，因為今天大家已經提出來有這麼多不同的態樣，所以我建議資安處這邊可以做一個通盤的考量，再把它定義清楚一點，或者我們在子法保留一個彈性，或者子法上可以訂出來標準、範圍在哪裡。

主席徐副處長：

大家也知道其實它的態樣蠻多了，剛剛有人說，捐助的錢不是很多，我們現在的標準是50%，剛剛親民黨黨團代表有特別說，這個事情很簡單，就依照預算法去做，但事實上聽起來還是有一些不同的態樣。之前這個

會議有找各機關開會有關財團法人的部分，我們會把上次各位的意見整理一下，當然比較簡單的方式是拉50%，今天我們也加入，可能捐補助的金額不是很多，或許我們也是可以考慮再做一個界限上的劃分：

剛剛金管會提到，我不知道你們講的財團法人的樣式，或者你這邊有沒有特別建議，是要再拉出什麼樣的條件或者是界限？這個是你可以提出建議的地方，我們現在的做法是，我們拉出那個界限之後，我們會把納管的地方做分級，分成A、B、C、D等級，假設他真的不是核心業務，你就會落到D級，根本就不用去管他，但是這個A、B、C級現在的訂法，可能還是回歸到那些是重要的財團法人，我們應該納在A級、哪些是B級、哪些是C級，設計邏輯應該是這樣子。如果這樣是可以認同的邏輯的時候，我們後續就會依據這個方式，會針對財團法人部分在他的資安責任等級上去做一個定義。

我不知道各位還有沒有其他的建議？

農委會：

這邊農委會，我再就剛才金管會所說的再補充一個建議，因為我們主要是在管財團法人的業務單位，在財團法人法裡面，今天院內這邊提供的資料我們發現，世界其他各個參考國家裡面他們並沒有把財團法人納管。

第二個，在財團法人法第2條的說明，他有明寫政府捐助的財團法人本質上仍視為私法人，而且在整個草案送院的說明裡面，是強調「對政府捐助之財團法人採高密度監督、強化管理規定以杜絕弊端」，所以在財團法人法裡面是為了杜絕弊端才去特設一個政府捐助財團法人的專章。在這種情況之下，資安管理法對於政府捐助財團法人納管的說明部分，是不是還可以麻煩院內這邊在未來的時候去強化這個論述？因為我看我們的草案裡面只有寫非政府機關要納入政府捐助財團法人，可是為什麼納入這個並沒有相關的論述，可能導致各個財團法人它的性質不一樣，對於這個地方他們會認為要花我自己的錢，為什麼我要再花這筆錢？為什麼我要被納管？以上建議未來在法案說明的論述部分可不可以再強調一下，謝謝。

主席徐副處長：

還有沒有其他的建議？

電信技術中心：

各位先進，我是電信技術中心，因為我們也有一些政府資安專案的執

行，所以對於這個政策的部分我們也有一些涉獵，我想就剛剛各位先進以及主席所回答的問題裡面，我覺得有一個很簡單邏輯上的問題，未來政府資訊事務的資安事務的執行，到底是由資安處由上而下？還是分散到各個單位，由下而上？因為有時候這個法案裡面有一個很不一致的地方，有的時候他的責任是放在主管機關，或者是放在非公務機關裡面；但是有時候資安處往上又抓了非常嚴的一些範圍。

所以至少在範圍的部分，譬如我們參考美國經驗，他部會的成立非常重視跨部會，也就是說，資安處是不是有像美國的預算辦公室或國土安全部這樣的能力去統合各個單位，並且由上而下去執行，我今天跟各部分會溝通，各部會告訴我哪些很重要，來決定你的納管範圍，這個是依據資安的要求而去訂定納管的範圍，而不是按照財團法人的規距50%，我捐助超過50%就要管。你要按照事務性、按照各個機關他們自己認為他們底下的這些財團法人是不是很重要，這個協調過程是必須的，你可以擬出一份很具體的清單去做未來的管制，可能每1年一次，或者每2、3年一次，這樣的滾動，這個做法其實是比較有彈性的，也符合資安的要求，因為現在你的範圍畫下去是很死的，這個問題就非常的多。

所以我建議在執行或者法案在寫的時候，既然資安處參考了這麼多國外的立法例，國外的做法就是重要彈性、溝通協調、跨部會，這點在資安法草案裡面我是看不到，所以我在這邊提出一個比較高的政策方面建議，謝謝。

主席徐副處長：

應該有三個問題了，我先說明一下農委會的問題，未來可不可以在法案裡面針對財團法人部分納管的論述多做說明，當然沒有問題，把政府捐補助的財團法人納入範圍，主要考量是因為他是政府捐補助，而且超過一定的金額，所以才需要做納管，因為是國家納稅的錢所捐助的，也是基於這樣的理由去做納管的範圍，論述的部分我們後續可以再加強，這個沒有問題。

剛剛電信技術中心有特別提到，到底現在的法規是由上而下？還是由下而上？這個部分你剛剛主要論述的法規是指哪幾條？可不可以跟你請教一下，這個第一個。第二個，其實在行政院的層級做跨部會的協調是我們平常就一直在做的事情，就財團法人這件事情來說，你剛剛的建議是不要

訂紅線50%，或者是金額不要去訂，把這個責任回歸到各主管機關去，我想各主管機關會把問題再丟上來，請問你要叫我怎麼納管、怎麼訂？

電信技術中心：

這個就是我剛才提到，由上而下或是由下而上，因為由下而上是一個溝通的過程，各個主管機關會可能會問這些問題，但是我想資安處就要先做解決，因為美國也不是這樣畫紅線的。你如果沒有辦法去協助解決的話，財團法人你要納管，抓一個50%，你可能就必須拿掉一些，像捐助金額太小的、任務範圍不重的，這些你可能就要額外拿掉，可是你在草案裡面沒有反映出這些事情。所以如果由下而上的話，又都丟給資安處，那是因為其他部會哪有那麼高的資安能力去決定這件事情？你們就是一定要協助他，我想這個在國外的立法例完全可以看得出來，人家就是這樣做的，如果你不這樣做，你就說：「丟上來我也不知道怎麼辦？」我也不知道怎麼辦啊？因為我是你下面更下面的財團法人。

我想這個問題當然不是一朝一夕，但是如果像資安管理法剛才那個簡報所提出來的，你是跟美國的FISMA、日本、韓國的，跟一些高位階資安的法規去比較的話，那麼你在這個法規裡面就必須要去解決這樣的問題，這樣的問題美國、英國或者是各國他們怎麼樣解決？這個我覺得你們應該也看過了，這個協調過程真的就是很漫長，如果不這樣子，直接一條線畫下去，大家開始50%，這個機關有問題、那個機關有問題，你們不覺得在這場座談會大家問題非常的雜、細，我想這個法規由下而上或由上而下的問題，我只能請資安處參考國外立法例，你們應該也已經參考很多了，看人家的過程去解決，如果你要問我怎麼辦的話，要有一個問的過程。

主席徐副處長：

財團法人如何去納管，我們過去也跟機關開過幾次會，如果你要問我這個資安法如何納管這條線怎麼畫？後來怎麼管？我們現在就是一直在討論過程中，為什麼需要把那條線畫出來，是因為我們希望框定一定的範圍，接下來再透過分級的方式，確定這些是我需要納管的，不然各部會不知道我到底要納管什麼東西，當納管之後，再把這些納管的東西依據資安業務的優先等級，不同的風險去做分級，這個是我們現在思考的邏輯。

基本上他應該是一個由上而下，去跟現在財團法人主管機關協調出來的過程，我們現在做就是一個協調的過程跟蒐集各位的意見，目前處理方

式大概就是這樣子，可能每個國家的做法不一樣，為了產出誰應該要納管、在納管的同時要兼顧到納管的必要性跟影響國家安全風險的高低，這樣的過程當中，其實我們現在就是不斷在跟各位溝通，未來希望在過程中能夠由上而下，來把這樣的制度產生出來，這個大概就是我們現在的做法。

我不知道各位還有沒有其他的問題？沒有的話，我們今天的會議準備結束，就到這邊，謝謝。