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15日（星期二）下午2時
地　　點：台大醫院國際會議中心402A/B
出席領域：資訊學界及專家

【記錄開始】
主席行政院資安處徐副處長：

因為時間關係我們就先開始了，首先非常感謝各位專家學者來到我們這邊，就資通安全管理法草案座談會所要談的內容提供我們一些寶貴的意見。今天我們這個會議主要針對資通安全管理法草案目前送立法院的進度跟現在內容大概跟各位做一個說明。

另外一個比較大的重點是針對資通安全管理法草案後續會訂五個子法，這五個子法內容我們現在持續在蒐集各界意見當中，我們也透過這個會議，請各位專家學者給與一些指導跟指教。

第三點，我要特別提的是，今天的會議會做逐字稿，這個逐字稿未來是要公開的，提醒一下各位。

在今天的會議之前…親民黨黨團還沒有到，他希望我們能夠拿資通安全管理法的子法來做討論，所以我們今天的簡報重點也會針對目前資通安全管理法子法裡面的內容來跟各位做一個簡報，各位後續就針對未來在子法上可以再調整跟建議的地方，多多給我們意見，大概先這樣子。

等一下會議的進行方式，我會請我們同事先就資通安全管理法目前的進度還有子法跟各位做個報告，報告完之後我們就開始開放各位提問跟討論，請問各位對於這樣的議程有沒有問題？如果沒有的話，我們就請我們同仁開始，謝謝。

賴世榮分析師：

謝謝主席，各位與會的先進、代表大家好，首先由我來跟各位說明資通安全管理法草案的內容，大綱我們稍微做一個調整，原則上我們今天會把比較多的時間放在後面相關子法的介紹，前面主要是推動歷程及推動對象，因為前幾次座談會有受邀公司行號可能還不清楚我們目前整個資通安全管理法的規範對象、規範範圍到哪邊，所以我會針對規範對象、範圍再

做一次說明；第二個部分是針對草案的架構跟內容；第三個部分是針對一些國外的立法例跟各界的關心議題；最後一個部分我會花比較多的時間在子法的說明。

首先針對推動歷程跟規範對象，這個是我們推動歷程，資安管理法在去年8月底的時候就已經完成整個草案的修訂，在9月就陸續辦各個不同的座談會，同時我們在國發會公共政策網路參與平台徵詢各界的意見。這個草案是我們在今年4月28日的時候函送立法院，目前是交由司法及法制委員會審查，已經完成一讀的程序，我們會在下個會期繼續由立法院做審查。

這個是資通安全管理法的規範對象，目前原則上分成兩塊，一個是公務機關，另外一個是非公務機關，這邊的公務機關指的是中央與地方機關（構），這邊的機構指的是公立醫療機構或者是公立教育機構，都算是我們的公立機關，還有一個是公法人，包含行政法人。在非公務機關的部分，主要分成關鍵基礎設施提供者、公營事業、政府捐助之財團法人。在關鍵基礎設施提供者的部分，我們這邊會透過中央目的事業主管機關或直轄市、縣(市)政府指定，函報給行政院核定。在財團法人部分，原則上我們是以政府捐助超過50%為納管對象。這些規範對我們都是以對人民生活、經濟活動或對國家社會安全有重大影響主要考量因素為納管對象。有關關鍵基礎設施的範圍，我們雖然沒有在法裡面講這個領域在哪，其實我們在草案第2條的說明裡面，我們有把關鍵基礎設施涉及的領域講出來，其實跟國土辦的領域是大致一致的，包含能源、水資源等八類，這個是我們資通安全管理法規範的範圍。

接下來說明草案的架構跟內容，資通安全管理法草案的架構圍繞這五個核心，最終目的就是為了維護國家安全跟社會公共利益。在外圍黑體字的部分，我們有在相關的母法裡面內容有做一個表述，在藍字的部分我們會特別用子法規定，後續我們會針對子法的內容做一個報告。這個部分是我們針對各國資安法的義務內容做一個比較，主要分成美國、歐盟跟新加坡，新加坡網安法草案目前跟我們資通安全管理法一樣，都是草案的版本，還沒有完成立法，大概是以資通安全維護計畫、報告繳交、通報應變、稽核、資安檢查、罰則，資安檢查基本上指的行政檢查，這邊做一個比較，後續我們會針對稽核、資安檢查跟罰則還有一些規範對象，這四個來做

一個詳細的比較，這個表就請各位參閱。

國外立法的比較跟各界關心議題，首先說明一下規範對象，我們國家的資通安全管理法草案目前規範對象除了公務機關以外，還有關鍵基礎設施提供者、公營事業、政府捐助財團法人；美國FISMA主要是針對聯邦機關，就是公務機關，雖然沒有針對非公務機關規範，但是有各州的州法還有其他的法規，有針對特定的對象做一個規範；在歐盟NIS的部分，規範對象是針對CI關鍵基礎設施提供者跟數位服務提供者；新加坡的部分主要是針對關鍵資訊基礎設施提供者跟資安服務廠商。

整個法案推動的歷程，我們有分階段推動，原則上資安管理法我們希望三讀通過後半年，公務機關優先適用；再隔半年，關鍵基礎設施提供者再納入；再隔半年公營事業跟財團法人最後納入，我們希望整個法在立法院三讀通過後2年來做一個整體的檢討。之前外界有一些聲音，像刑事警察局一直要求我們像電商業者應該要納入，不過現階段電商業者沒有在這個範圍裡面，這個是各國規範對象的比較。

在稽核的部分，我們國家資通安全管理法草案跟美國FISMA稽核內容都是針對資安維護計畫的執行情形；在歐盟跟新加坡的部分，主要針對資安相關文件還有一些必要事項做一個稽核。在行政檢查（資安檢查）的部分，資通安全管理法主要是針對資安維護相關的實務做一個檢討；美國FISMA是針對公務機關，其他州法還有相關規定；歐盟跟新加坡主要可能會去檢查資安相關文件還有受影響的相關資料，這個是行政檢查的部分。

最後一個，罰則，在罰則的部分，目前我們資安管理法雖然有訂10～100萬不等的罰鍰，目前是針對非公務機關，公務機關是從相關的公務人員考績法、公務員懲戒法的相關規定，所以這個部分沒有在管理法裡面做一個著墨，這也是人事總處的意見，這個東西回歸到公務人員相關的法規，不需要在資通安全管理法裡面訂定，所以目前的罰則是針對非公務機關的部分。原則上我們這個資通安全管理法不是以處罰為目的，我們希望以輔導、協助的立場，原則上我們不會直接罰款，會有一個限期改正的措施，只有兩個情形會直接罰：資安事件應通報未通報時、無正當理由拒絕行政檢查，這兩個情形如果違反的話就直接開罰，這兩個情況以外，我們都會有一個限期改正，如果逾期不改正，我們才會處以罰鍰，這個是我們國家的部分；美國FISMA主要是針對聯邦政府的公務機關，所以沒有訂相關

的罰則，當然還有其他州法跟其他的規定，也針對特定的領域訂相關的罰則，我們這邊就沒有列出來；歐盟NIS是要求會員國自己去訂定有效的罰則，這個比較不一樣；新加坡網安法的部分有比較嚴格的規定，如果有違相關的義務，這邊有有期徒刑的罰則，他也有訂換算成新臺幣約200萬以下不等的罰金，這個部分請參考。

這個部分是我們過去幾場座談會整理一些大家提出來的問題，首先我們這邊分成六個部分，第一個部分是針對規範對象，過去有人認為為什麼規範對象要包含非公務機關？有的國家沒有包括非公務機關，為什麼我們資通安全管理法一定要把非公務機關納進去？那些納管對象有涉及一些公共利益、人民生活財產比較重大相關利益的部分，我們才把它納管。也有人提出來，目前政府捐助財團法人的定義，應該再考慮不同的因素，例如捐助的總額，因為我們目前是以政府資金累計超過50%為納管，有些法人有可能他的整個基金的分母政府捐助不到100萬，可是政府捐助超過50%，他也要納管，可是政府捐助的金額可能幾10萬，不到100萬，這樣還要受納管，他不能配合到我們相關義務的規定，有推動上的困難，也有人提出這樣的看法。

第二個，在母法相關的內容部分，有人提到目前資通安全管理法裡面，資安長是用兼任，也有部分的代表覺得這個資安長應該獨立設置，不應該用兼任的方式，不過目前資通安全管理法母法裡面是用兼任，機關首長指派副首長來兼任。關鍵基礎設施領域是否應明訂於母法？目前領域別我們沒有在母法條文裡面去做規範，可是我們有針對關鍵基礎設施跟關鍵基礎設施提供者的定義在母法第2條有做一個說明，有關它的領域就是能源、水資源等八大行業，我們有在母法條文第2條的說明有講領域的部分。也有代表認為資通安全管理法應該要取消罰則，不要有罰則、也不要有稽核跟行政檢查的規定，可能國外的立法例有些沒有罰則，為什麼資通安全管理法要有罰則，可能有一些不同的聲音。

第三個，在委外監督的部分，因為我們資通安全管理法除了規範對象必須要遵守資通安全維護的相關規定之外，我們會要求受規範對象也要加強他的委外監督，也有代表提出來，可能一些委外事務不熟悉，行政院可不可以提供合格廠商的名單給他們參考？他們就找這些合格廠商名單，去做一些資安業務，就可以很安心了，就可以不用顧慮到那麼多，希望我們

可以提供一個合格廠商名單給他們參考。

第四個，在資安責任等級分級的部分，有人提出來核心系統之認定是否應予明訂？這個部分我特別說明，我們在資通安全責任等級子法裡面，我們有針對資通系統的分級原則去做一個訂定，我們依照機密性、完整性、可用性跟法遵四個面向，只要有一個面向列為高風險，就算核心系統，這個部分我們有在資安責任等級分級子法裡面做一個訂定。還有一個是應辦事項內容之可行性，有些單位提出來，我被列為B級，可是那些應辦事項我不一定可以做得到，怎麼辦？那應辦事項的內容、項目可不以做一個調整？就像剛剛主席先跟各位報告，目前我們子法都還是草案的階段，我們希望這段時間蒐集各方意見之後，都還有調修的空間。

第五個，關於資安事件通報的部分，也有代表提出來，目前有關資安事件的等級，有關資料遭輕微或嚴重竄改的認定，是否應於子法裡面特別明訂清楚？這個部分，目前有關嚴重、輕微的認定原則上由通報的機關、通報的單位來做一個認定，當然他有他的上級跟監督機關做一個協助的認定，如果要在法裡面針對什麼是輕微、什麼是嚴重去做一個明確定義，可能比較會有困難。資安事件通報的時間是否可以有一個彈性？目前公務機關我們是有規範知悉資安事件1小時內要通報，非公務機關其實是沒有的，在我們之前開會的過程，因為有公務機關提出來有關資安事件通報是不是可以不要1小時內通報？他們也有表達這個意見。

主席徐副處長：

我先在這邊補充說明一下，針對這幾個關鍵的議題，等一下有些會在子法裡面做討論，包括資安責任等級裡面核心系統的認定問題，我們現在其實有一個初步的規劃，等一下請世榮在簡報的時候適當的說明一下，核心系統認定方式我們有一些初步規劃，後續等一下專家學者可以給一些意見。

另外一個是一般事項的內容，我們現在規劃的整個架構，適用資通安全管理法不管公務機關或非公務機關，都會透過資安責任等級的方式，依你不同的資安責任分成四個等級，就是A、B、C、D，但是對到每個等級有應該辦的一些資通安全管理事項，這些事項當然是可以討論的，我們目前公務機關有運作過一個模式，這個模式未來是不是適用到非公務機關都可以再討論，等一下我們會做一個簡單的報告。

接下來關於遭受輕微或嚴重，我們目前是文字上的規定，在前幾場確實有人反映，什麼叫嚴重？什麼叫輕微？在這樣的文字上不明確，我們後續希望在這個子法上透過一個比較明確的方式把這個定義清楚，至少未來在通報的事件上能夠依循，我大概先就這個部分先補充，世榮等一下就直接針對子法的部分簡報，麻煩，謝謝。

賴分析師：

最後一個有機關跟非公務機關提出，目前經費和人力都很欠缺，這個部分是各界的一些議題。緊接著進入我們的重點，就是相關的子法，目前這個子法都還是草案的階段，所以我們沒有提供給各位子法明確的條文，我們是用簡報的方式來說明，特別補充。

第一個是針對資通安全管理法施行細則的部分，有關資通安全管理法施行細則，這個是由資通安全管理法母法第22條授權訂定，整個裡面的架構主要是針對適用對象的補充、改善報告，資通系統、資通服務委外的注意事項、資通安全維護計畫、行政檢查等這邊做一個規範，後續針對這幾個部分來做一個說明。針對適用對象補充的規定，目前我們資通安全管理法排除了兩類機關，一個是軍事機關、一個是情報機關，什麼是軍事機關？指的就是國防部及所屬機關（構）、部隊、學校，國防大學也算我們的軍事機關；情報機關我們參考國家情報工作法第3條去規定的，所以原則上我們資安管理法排除了軍事機關跟情報機關這兩個部分。施行細則我們也特別針對政府捐助的財團法人這邊做一個定義，有一條針對法人的捐助累計的總額還有不同情況的一些判斷的條件，我們在施行細則也有做一個明確的定義，當然這個內容我們目前是參考財團法人法草案的內容，可是不全然是整個抄過來，雖然目前財團法人法草案目前在立法院審查階段，我們在施行細則裡面會針對目前財團法人捐助的方式做一個定義。

在施行細則我們會針對改善報告的部分做一個規範，第一個，這邊改善報告一個叫稽核後的改善報告，還有一個是通報應變後的改善報告。什麼是稽核後的改善報告？這邊有針對待改善的項目、影響的範圍、發生的原因，改善的措施、預定完成的時程有做一個規範；這個是稽核改善報告的部分；在通報應變改善報告的部分，我們主要針對資安事件的發生、結案登錄的時間、事件影響的範圍、損害的評估、復原的歷程、事件調查的歷程有做一個規範，這個是改善報告的部分，原則上改善報告，資通安全

管理法裡面是針對稽核後跟通報應變後的我們都叫改善報告。

目前我們資通安全管理法除了我們的規範對象要依照資通安全管理法提出資通安全維護計畫跟通報應變機制外，我們特別強調委外的監督管理，施行細則也針對委外監督管理要求受規範對象要做一個事前評估跟事中監督。什麼是事前評估？針對受託者的作業程序、是否經過第三方驗證、受託者是不是有足夠的人員配置來承接受託業務、確認他是不是有相關類似業務的經驗還有一些佐證的證明；事中評估的部分，我們特別跟受託者約定相關的事項，包括受託者資安維護的措施等等，這個部分我們也會在施行細則裡面去做特別的規範。

資通安全維護計畫，目前是我們整個資通安全管理法的重點之一，我們要求受規範對象要提出資通安全維護計畫。什麼是資通安全維護計畫？其實我們在母法有做一個說明，主要是針對公務跟非公務機關為防止資通系統或資訊遭受未經授權之存取、使用、控制…等等所採取的措施。資通安全維護計畫的項目包括哪些？包含資安政策推動、目標訂定、資安組織、人員的配置、相關的演練、通報、委外管理的程序、獎勵的標準，都會在資通安全維護計畫裡面訂定。目前資通安全維護計畫在過去辦理的過程中，一直有人提出來，什麼是資通安全維護計畫？提出來這個問題基本上都是公務機關，會問我們這個部分行政院會不會提供一個版本讓我們參考？不然我們不曉得怎麼去寫這個內容，原則上我們會提出一個範本給機關參考。除了安全維護計畫的項目裡面，我們也針對實施情形有做一個規範，包含計畫各個項目的執行、成果跟相關的說明，也會在這個地方做一個論述。

在行政檢查的部分，我們施行細則有補充，針對發動要件，中央目的事業主管機關、地方政府對於非公務機關的稽核有發現重大缺失或有重大資安事件的時候，我們才可以發動行政檢查。在職務證明文件的部分，我們執行行政檢查的時候，我們要求參與者攜帶相關的證明，我們在施行細則也特別為了保障執行行政檢查過程中，不要導致一些機敏資料、商業機密遭外洩，我們也會跟參與人員以書面約定保密義務，而且在檢查後也要作成記錄。之前也有人提出來，如果檢查人員在執行行政檢查之前有跟機關簽訂保密義務，事後有把一些商業機密洩漏出去的話，基本上就涉及了刑法，以上做一個補充。

在施行細則我們會針對什麼是重大資安事件做一個定義，原則上我們講的重大資安事件就是3、4級資安事件。針對資安事件各個等級的分級原則，我們會在另外一個子法，並不是在施行細則裡面去做定義，我們是在資安事件通報及應變辦法那個子法去做一個規範，我們在施行細則有針對什麼是重大資安事件做一個說明，指的就是3、4級是重大資安事件。我們有針對重大資安事件公告的補充規定做一個論述，公告項目就是指發生的原因、影響程度還有一些控制的情形，這個部分是施行細則的部分。

第二個部分跟各位介紹是資安責任等級分級辦法的子法，這個是第二個子法，資安責任等級分級辦法這個是由母法第6條授權訂定的，目前這個子法會針對資安責任等級分級、分級方式、分級原則、應辦事項等等做一個說明、規範。首先它的分級方式，目前我們規範的分級方式是由行政院直屬機關、省政府、直轄市、縣（市）政府、縣（市）議會，每年針對他自身的資安責任等級以及所屬機關跟所管非公務機關的資安責任等級向行政院提出來，彙整函送行政院來核定，這個是行政院直屬機關、省政府、直轄市、縣（市）政府跟議會的部分。在這些機關以外的部分，包括總統府、國安會以及其他四院，一樣是每年提出自身資安責任等級跟所屬、所管非公務機關，他們自己去核定，可是彙送行政院備查，這個是跟上面比較不一樣的，因為行政院不會去管到總統府、國安會或其他四院，他跟我們不一樣，由他們自己去核定，函送、彙送行政院備查，這個跟我們行政院的體系比較不一樣的部分。

分級原則及例外因素的部分我這邊說明一下，目前的資安責任等級大概分成A、B、C、D級以及不分級。什麼是A級？總統府、國安會、五院還有直屬這些機關的公務機關原則上都是A級，有直轄市政府，像台北市政府、桃園市政府；公立醫學中心，像台大醫院；還有業務涉及外交、國防、國土安全、全國性之財政、經濟等等這些，也會列為A級別。B級有哪些？縣（市）政府、公立大學、公立區域醫院，這個原則上是在B級。什麼是C級？所列機關如果有自行或委外開發資通系統且設置有伺服器者，才會列為C級，如果其中有一個要件不存在的話，就會在D級。也就是說，這些所列機關沒有自行或委託開發系統，也沒有設置伺服器的情況，都會在D級。我們還有列一個不分級，為什麼會有不分級？現行的確有一些不分級的情況，例如像果菜市場，他也沒有這樣的情形，所以他會被列在不分

級，目前我們原則上分成四個等級，A～D級。臚列這些機關、機構，我們是按照現行資安責任等級分級，目前還是一個規則，我們是參考現行做一個表列，原則上目前大概規劃的方向是這樣，這個也還是一個草案的階段，當然還有一些調整，我們在8月1日邀集所有的政府機關來對資安責任等級的應辦事項做一個檢討、意見交換，原則上這個表實際上的細部的內容當然還有調整的空間。除了分級的原則之外，我們還有一個例外考慮因素獨立一條，針對涉及外交國防、涉及關鍵基礎設施，也就是說依照前面的分級原則，他是列到B級的話，他可以針對這些例外考慮因素調整到A級，或者調降到C級等，不一定，這個是一個另外考慮因素。這個是比較細節的，有關資安責任等級應辦事項的部分，給各位參考。

第三個子法是有關資安事件通報及應變辦理，這個部分是由資通安全管理法母法第13跟17條授權訂定的，這裡面有針對資安事件的分級、通報流程、應變流程、通報及應變流程訂定、檢討機制、注意規範。什麼是資安事件1、2、3、4級？我們這邊簡單用這個表跟各位說明，各位如果看到子法的條文，會比較不清楚，可以看到分別一些敘述，所以我們用這個表列來做一個說明。什麼是1級？只要涉及非核心業務的資訊都是1級；什麼是2級？只要涉及核心業務或關鍵基礎設施業務的資訊洩漏的話，都會在2級；什麼是3級？只要是一般公務機密、敏感資訊的資訊洩漏都會在3級；什麼是4級呢？只要是國家機密洩漏，一律都是4級，這個是在資訊洩漏部分。我們在完整性的部分，只要涉及非核心系統，它的資訊遭輕微竄改，這也是會在1級；如果是在一般公務機密或者敏感資訊的資訊，不管遭什麼程度的竄改，都會在3級；如果以關鍵基礎設施的資通系統沒有辦法在可容許的時間內回復的話，就會在4級，這個表大概是這樣看。

這個部分是有關公務機關的通報應變流程，當公務機關知悉資安事件的時候，必須1小時內向他的上級或監督機關以及行政院通報，他的上級或監督機關，收到事件通報的時候，就會進行事件的審核，而且要在審核完成後將結果於1小時內通知行政院，他同時要判斷他的所屬機關，也就是通報的機關是否需要支援以及判斷是否需要行政院的協助，事件處理完畢之後，由公務機關完成結案登錄的動作，這個是公務機關的部分。在非公務機關的部分，原則上通報整個流程跟公務機關是類似的，有兩個地方比較不一樣，在非公務機關知悉資安事件的時候，我們公務機關有規範1

小時內要向他的上級或監督機關及行政院通報，非公務機關是沒有的，你只要知道是資安事件，就趕快跟你的中央目的事業主管機關或地方政府做通報；還有第二個部分不一樣，在處理完資安事件的時候，有關結案登錄動作是由非公務機關的目的事業主管機關協助他去登錄，在公務機關當A機關發生資安事件，是由A機關自己去登錄，在非公務機關是由他的目的事業主管機關或地方政府協助登錄，這兩個不一樣，這個是非公務機關的部分。

針對資安事件的補充規定，通報時有哪些項目？包含發生機關、發生時間、等級的評估有做一個規範。我們也有針對他的通報方式，這個目前是我們現行的通報方式，至國家資通安全通報應變網站填報，我們希望這個資通安全管理法立法通過之後，是由中央目的事業主管機關或地方政府指定任何的方式通報，如果因為網路中斷或停電等事故，無法辦理這些通報的話，可以採取其他的方式，例如紙本或傳真來填寫，可是當事故排除之後，他還是要按照原本指定的方式去補通報。

第四個子法是資通安全維護計畫實施情形稽核辦法的規劃內容，資通安全維護計畫實施情形稽核辦法主要是由母法第6條授權訂定，主要內容包含稽核內容、配合事項、稽核後的辦理事項有做一個規範。這個資通安全維護計畫實施情形稽核辦法主要是規範由行政院對非公務機關去稽核時所做的規範。我一樣用一個流程圖做一些說明，針對非公務機關接受行政院稽核資安維護計畫實施情形之流程，首先行政院必須在每年提出一個年度稽核計畫，而且在1個月前就要通知目的事業主管機關或地方政府，在1個月前也要通知受稽機關，在目的事業主管機關收到這個通知之後，必須要協助派人一同來稽核，受稽的部分要提供相關的說明跟證明文件。行政院在稽核結束之後，我們會提出一個稽核結果報告，我們會把這個報告提供給受稽單位，受稽單位也要針對我們這個稽核報告提出改善報告，後續會有行政院跟中央目的事業主管機關持續去追蹤他的改善報告，這是一個簡單的流程。

最後一個子法是針對資通安全資訊分享辦法做一個說明，一樣是由資通安全管理法母法第7條授權訂定，裡面主要是針對資訊分享的對象、平台還有注意事項去做一個規範。這個部分我們目前是規劃由行政院建置一個資訊分享的平台，當然我們也會由行政院指定中央目的事業主管機關去

建置這個平台。我們目前的現行狀況是有針對關鍵基礎設施八大領域要求他們的目的事業主管機關去建一個平台，來做一個情資的交換。我們在做這個情資分享，我們這張投影片是表達其實不是所有的資訊都可以放到那個平台去做一個分享，我們必須考量到一些個資保護，如果有涉及一些商業機密、機密資料，我們都不可以在上面分享，原則都會做一個過濾的機制，這個是資訊分享的子法，以上說明，謝謝。

主席徐副處長：

謝謝，我還是必須要先強調一下，剛剛報告是子法內容，但是所有東西還是會尊重立法院母法通過以後，我們還是依據母法內容再做子法的訂定，目前這個階段純粹是就子法做意見蒐集，現在開放發言，請吳顧問。

吳國維顧問：

主席，我必須說不管是母法或子法都是一個災難，第一個部分，今天叫做學者專家的座談會，不知道為什麼我們沒有找公法的學者或專家進來？因為你要訂定法律，找的都是資訊專業的人。譬如上個禮拜在業界的部分，就來了兩個公法的學者還有公法的律師，他就會告訴你這部法律有問題的地方，太多不確定因素在裡頭，不確定因素會造成兩個問題，第一個部分是子法上的困難；第二個部分是政府行政可能會擴權的問題，所謂擴權甚至會侵犯到人權的問題。

第二個部分，假設去讀個資法，都還有比例原則，法律的比例原則目的在哪裡？就是當我的資源人力不足的時候，在判決的過程裡頭，相對的法官會給他從輕量刑，我人就不夠，只有兩個人，你要我做什麼？

接下來幾個比較大的問題，好幾年我一直在講這個問題，我我們過去在講資通安全的時候，很顯然你今天還把CIP跟CIIP混為一談，但是你偏偏都叫「資通安全管理法」，但是資通安全管理法要用在CIP就會有問題，因為在國外CIP在美國是歸國土安全部來管的，CIIP是由國家資通安全管理中心來負責的，所以這兩個是切開來的，你現在把它混在一起，這裡頭就會造成一個很大的困擾。

從過去資安處這次辦的四次的座談會，我這是第三次，我所聽到幾乎所有人都會困擾的一個地方，你用了一個名詞在母法裡面，叫「非公務機關」，非公務機關在法律上本身就會有一個特殊的意義存在，就是不執行公權力的機關叫非公務機關，你偏偏在第2條解釋條文裡頭自己創一個「

非公務機關」叫做關鍵基礎設施提供者、公營事業及政府捐助之財團法人，也就是你的非公務機關跟法律的非公務機關的名詞基本上是不一樣的。

另外一個部分，剛剛雖然列了前面幾次座談會有人對你們的東西有意見，我看到的偏偏就把公法學者、律師所提的問題把它漏掉，我不知道是有意還是無意？你在前面幾次座談會有機會跟大家解釋，大家不要擔心，非公務機關指的叫做關鍵基礎設施提供者、公營事業或政府捐助的財團法人，你剛剛所訂出來的子法或者是在母法裡面的分級，有A、B、C、D級，什麼意思呢？假設在座的都知道，你們的關鍵基礎設施理論上講叫做A級，但是你偏偏又在你的子法跟母法又把分級B、C、D都拉進來了，然後你到處跟人家說B、C、D我們不會管，對不起，以後在子法的時候是按你通過的法律在走，不是用你的嘴巴在走，你嘴巴跟人家說不會，你的法條是怎麼寫的？你的B、C、D都訂下去了，你說不會管，不通報也沒有什麼。所以邏輯上有誤差，而且有問題的。

接下來我覺得比較重要，你們可能要去釐清的幾個地方，我建議你在子法或者假設在子法有立法委員提出修正的時候，你們應該謙虛的接受，譬如第5條：行政院得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。我們都知道這個第5條怎麼來的，因為在上一屆的政府，希望把技服中心變成公法人，現在沒有了，所以就把第5條塞進來了。第5條會出現什麼問題我簡單說明，你只說明行政院的委任或委託其他公務機關法人跟團體去辦理相關的事情，你從來沒有說什麼東西不能委託、不能委任的，我大概從林逢慶當政務委員開始，歷屆科技政委我都跟他講過這個問題，我們公務機關的資訊單位已經外包到根本就是一個外包單位，只會寫外包文件而已，根本沒有operation，也就是說，什麼叫關鍵？你已經都委託出去、外包出去了，沒有一個關鍵核心業務在你手上，因為你都外包光了，有什麼東西是不該外包、不該委任的，從來不講清楚，這只有讓公務機關的資訊單位越來越弱化，然後你說要把資通安全做好，緣木求魚，根本做不到。

我舉一個最簡單的例子，國發會以前的研考會，我們的GSN根本就外包光光了，有誰知道那個operation是什麼operation，根本就不知道，只等著廠商告訴你怎麼做而已，廠商給你什麼資料，你只知道那些資料。我高度的建議，為了中華民國的資通安全要提升，應該在子法講清楚什麼

東西不能委託也不能委任，而不是只講說我要委託、我要委任。我當然同意，以目前政府的資源跟人力是不足的，但是講難聽一點，也很多部會的資訊單位幾10個人，我們都委外到沒有核心業務在自己手上，真正的核心關鍵是可以委託委任的嗎？而且委託、委任有經過classify嗎？譬如我以前在美國上班的時候，當我們要承接這個業務的時候，要被classify的，你沒有，根本就是委託出去，也沒有經過classify，甚至是一個核心業務也把它委託出去，很可能你都委託給外商在operation。所以光看到第5條，老是在想把事情推出去，從來沒有說什麼東西我不推出去，我要自己好好把它做好，至少你現階段做不到，總要在子法裡頭分年，應該要在第2年、第3年、第4年什麼東西不能委託出去，我要自己operation，不要告訴我什麼東西都要委任、委託。

另外一個部分，這部法律最糟糕的問題在哪裡？你把中央目的事業主管機關、直轄市、縣（市）政府都拉進來，講難聽一點，個資法還只講到中央目的事業主管機關，你現在把直轄市、縣（市）政府都拉進來。我隨便舉一個例子就可以想像未來紛爭、爭議、困擾會產生在哪裡，你剛剛通報講了一大堆有的沒的，譬如台機電、中華電信，任何一個非公務機關被你列在關鍵基礎設施，他很可能在台灣每一個縣（市）都有辦公室，按照你的通報，你告訴我，我到底要通報給誰？還是每一個都要通報？假設可能，我倒是高度建議你在子法講清楚，就一個通報窗口就好了，搞這麼多的通報窗口，這個叫做擾民。中國石油公司全台灣都有，每一個縣（市）政府都可以叫他通報，你有幫他解決問題嗎？沒有，只是製造他問題而已，本來就應該說行政院指定一個主管機關，大家跟他通報，單一窗口。你搞到中央目的事業主管機關一直到直轄市、縣（市）政府都進來了，講難聽一點，在座每一個都是資訊的專家學者，有多少縣（市）政府的資訊單位是很弱的你知道嗎？你還要叫他們去做有的、沒的，搞A、B、C、D級，還要負責蒐集通報、去檢查、稽核，這個根本是自己找自己麻煩。

接下來可以看到好幾個地方都有問題，我相信大家都知道，所有的單位，特別是非公務機關，最擔憂的議題在哪裡？除了罰則以外，其實最擔憂的條文是在你第17、18條的地方，你在第18條怎麼說的？你在第18條說：中央目的事業主管機關或直轄市、縣（市）政府因稽核資通安全維護情形發現重大缺失，或遇到重大資通安全事件，而認有必要時，得派員攜帶

執行職務證明文件，進入非公務機關場所檢查。上次的公法學者跟律師都告訴你，這個第18條犯了多少問題，第一個，你的「重大」這個名詞不明確；第二個，什麼叫做「認有必要」？食品安全相關的都會跟你說，有犯罪嫌疑或影響公共衛生安全的條件底下才能夠派員進去，你沒有，只要「重大缺失」，誰知道你的「重大缺失」怎麼定義的？你的「必要」是怎麼定義的？是你說的算嗎？或者按照18條中央目的事業主管機關、直轄市、縣（市）政府都可以認為這是重大、必要我就進去了，請問要是牽涉到商業機密的時候或是牽涉到其他部分的時候，甚至講難聽一點，你們只想到方便，都沒有想到假設進去的時候發現牽涉到國家機密的時候怎麼辦？隨便縣（市）政府的人跑進去，結果發現這是一個國家機密，他連碰都不應該碰的東西，他竟然進去了，帶著所謂的執行職務證明文件。所以你是不是應該把子法裡頭把這些東西都講清楚什麼叫「必要」、什麼樣的人才能夠進去、什麼樣的職務證明文件才叫做有效。坦白說，假設你是關鍵，我們認為關鍵是牽涉到國家資通安全重要事情的時候，這些要不要被classify？還是可以隨便跑來跑去？他甚至跑到關鍵基礎設施進去，他還可以到處亂跑，雖然後面你說有保密義務，保密義務連寫都不要寫，因為我們有保密法，這些一大堆空白的條件，我覺得今天開這個會，你把公法學者跟專家漏掉是一個非常糟糕的問題，因為我們今天在談法律，不是在談資通安全技術問題。

再說，整部法律20幾條讀下來，你只在做兩件事情，雖然講了一大堆，只是在做稽核跟通報，整個資通安全要把它做好，真的只靠稽核跟通報就可以做好嗎？而且可以看到不管在歐盟或是在美國，都不是叫稽核，叫Compliance，Compliance如果會翻譯成稽核我也滿服了你，Compliance跟稽核差很遠。所以我覺得剛剛把子法的部分精神拿出來，不管A、B、C、D或是通報的相關認定，一定要認真的把它做好，隨便寫一個「輕微」、「重大」那個是不能被執行的東西，到底輕微、重大是誰認定？你認定、我認定、他認定？一定要非常明確告訴人家什麼叫輕微、什麼叫重大，否則光在通報就會製造一堆困擾，尤其對非公務機關的時候，你又把中央目的事業主管機關、直轄市、縣（市）政府都納進來，那個通報真的要規劃好，高度的建議你單一窗口，這種方式的通報叫莫名其妙、擾民。

主席徐副處長：

謝謝吳顧問，其實我覺得剛剛聽了吳顧問的說明，滿多是我們現在訂子法裡面可以再進一步考慮的地方，我滿贊成吳顧問其中幾個論點，第一個，我先說明一下，我們有安排公法人的學者場次，應該是在8月底的時候。

吳國維顧問：

為什麼不在一起呢？

主席徐副處長：

其實顧問這個問題上一場已經有對你說明過，我們當時開這種不同group座談會，會有的不同聲音，其實是因為能夠一起對他們關心的事情做說明，後續要安排混在一起都沒有問題，我們都可以來安排。

吳國維顧問：

我解釋理由，尤其在今天這一場，公法人不知道我們的資通安全技術問題，但是我們資通安全的專家學者不知道公法的基本條件是什麼，所以為什麼要把他放在一起的理由在這裡，互相知道，讓法律人知道我們在資通安全顧慮問題的是什麼，他可以怎麼幫我們的忙；我們從資通安全的技術進去的時候，公法人可以告訴我們怎麼寫，那個法律才不會有漏洞。你把它拆開來，講難聽一點，我們講了半天，很可能在公法人學者認為這個有問題；但是公法的學者在講的時候，他根本不知道資通安全技術上我們擔心的問題是什麼，所以我是覺得來不及了，不過假設有機會，我建議你真的應該把他放在一起，這是不應該切割開來的事情。

主席徐副處長：

這個意見我們可以考慮，因為我們陸陸續續還是會針對子法的部分開其他的場次，這個意見我們就記下來，下次我們可以安排一個有關不同領域的人在一起討論的機會跟場合，我們可以來配合。

接下來有幾個我特別強調說明一下，剛剛顧問有特別提到，現在其實在資安責任等級裡面是用A、B、C、D級來做規範，我們現在公務機關是用這樣的方式，但是未來對於關鍵基礎設施提供者這些非公務機關，是不是採用這樣的方式？我們現在沒有決定的定案，我們還是會持續來聽各界的意見，這個部分目前可以後續再討論，我們內部後續也有一些想法，希望他能夠跟公務機關的做法是切開管理，不要套用同樣的模式去做管理，這個我們可以同意來做一些調整，這個沒有問題。

剛剛吳顧問有提到，現在政府的委外，到底哪些可以委外、不能委外，希望在子法裡面做訂定，我們可以來思考一下，其實目前有一些政府機關有些業務可以委外跟不可以委外要去做一些區隔，這個部分我們可以在子法後續訂定，或者是透過其他的方式把這樣的東西規範下來，讓政府機關可以依循，我們可以參考這樣的意見。

接下來有特別提到通報的部分，大概是對一個機關還是多個機關，其實我們現在的規畫就是對一個機關，譬如剛剛特別提到中華電信，以目前現在的機制，中華電信是通報NCC，NCC再通報給行政院，所以是對一個機關，現在的子法裡面可能讓大家以為是通報多個機關，可能我們後續在文字上再去做更明確的調整，這個我們都可以來配合做修正。

剛剛有特別提到行政檢查，什麼樣的職務證明文件才有效？假設去執行行政檢查的時候，只要是重大或者是得視必要這樣就可以進去？是不是再有一些限縮上的條件？我們後續可以針對下面公法學者的場次請教他們，或者他們有一些其他的意見，我們都可以把它納入，再做一些調整，到時候顧問也可以再來參考，多給我們一些意見，這個我們都可以配合做調整，沒有問題，我先就吳顧問的部分先回應到這邊，接下來各位還有沒有要給我們一些建議的？蔡老師。

蔡志宏教授：

我想就幾件事情建議在母法文字的說明欄或者是在子法裡面能夠儘量釐清。第一個，我想在座對於了解政府現在委外的狀況以及關鍵基礎設施現在各式各樣提供的樣態，會發現一點，不管是所謂關鍵基礎設施提供者，或者是許多承接政府委外業務的財團法人，或者一些民間的單位，他們常常有多重角色。

多重角色的例子很簡單，比方今天有一家關鍵基礎設施提供者，他本身是因為通訊、提供電信網路被納入，可是他又去接受政府委託其他的IT業務，這時候他就有兩種以上的角色；財團法人也可以，他說不定被納進去是因為政府捐助超過50%，這個主要原因被納入非公務機關，可是他說不定承接的是政府委託另外一個有點敏感性的業務，可能在這樣的單位裡面，他是分屬於不同單位，他裡面可能不是所有東西都很敏感，可能有8個單位，有2個是很敏感。這個牽涉到我們實施的強度、母法訂到一些用詞，比方資安的維護計畫、遇到事件的時候去做檢查等等，我們在這裡面

的適用範圍是指針對他被列管的業務？還是那個非公務機關他的所有？如果按照比例原則的話，我們在某些地方的說明或文字或子法裡面要去處理這一段，避免無限上綱的問題。

可是如果是承接政府業務委外的這些人員，事實上這個牽涉到政府服務的範圍，政府有些IT系統不在政府地方裡，是在他所委託對象的機房裡，所謂機關對民眾提供服務的範圍，那台server算不算？雲端的系統算不算？以及雲端系統很核心的技術人員算不算？這些我會建議在說明或子法裡面釐清，要不然會有比例原則或者是強弱的問題，我舉例來說，譬如有一個政府捐助的財團法人比例不到50%，他出的業務就是很敏感，那一段要怎麼算？所以我還是認為以實務來看，我們要就他的資安敏感度、跟他的範圍來做事實認定，不管是在母法的說明或者在子法真正要實施的範圍上，這一部分是回應吳顧問剛剛的疑慮，那個部分如果有所處理，可以釐清不少，這個是第一大的建議。

第二部分，因為我在看資通安全責任等級分級辦法裡面，你們列了一個學校，特別是列了大學跟學院以下的一些公立學校，因為我們好多教授都在這裡，問題就來了，大學是一個很複雜的體系，第一個，有公立大學跟私立大學，私立大學為什麼就沒有關係？第二個，如果大學有敏感，是什麼地方很敏感？公立大學如果是學生成績很敏感、學生的學習資料很敏感，那私立大學也是一樣；如果公立大學有些研究計畫很敏感，私立也有些承接政府很敏感的研究計畫。

資安藉由實務的認定來看，不是隨便一個單位，學校通常還有2、3種單位，學校有附屬單位，比方學校有宿舍，這個條文出去，你要不要管學校的所有宿舍？宿舍的網路常常也是麻煩的來源，因為學生隨便就在架網路、server，會造成一些麻煩，可是那也是創意的來源，很多時候他們很多厲害的高手是這樣養出來的，因為我看過我的同仁去管我們學校的宿舍網路，我只能說那是一個特殊區塊。學校附屬單位裡面也有另外一種特殊區塊叫附設醫院，台大就有台大附屬醫院，大家都忘了台大醫院跟台大是有關係的。我是舉這樣的例子，大學不是一個簡單的分類區塊，我建議還是從業務的實際範圍來認定，我建議在母法說明或者子法裡面的一些條文做比較細緻的處理，朝向跟業務有關的、必要性的部分加以等級上面的區隔，以上。

主席徐副處長：

我覺得這兩個意見都非常好，因為我們現在訂子法，這個其實可以在子法裡面再去做明確的規定，各位現在看到其實都是暫定的，我們也在討論大學以下的學校要不要去做管理，還是回到剛剛蔡老師特別說，他業務的重要性是不是這麼重要，這個部分我們會納進去，這個都沒有問題。

第一個，剛剛前面提到，假設一個組織有雙重角色的部分，他到底應該適用哪一個？是非公務機關還是公務機關？還是政府捐助的財團法人？因為這個規範強度確實是不一樣的，這個部分我們會在施行細則裡面再把它做一個明確的說明，各位還有沒有其他的建議？

親民黨立法院黨團：

不好意思我真的忍不住了，我覺得不是這樣子的，對不起，我是親民黨立法院黨團的法案助理，副座你這樣的法律觀念完全錯誤，因為我覺得那個教授的意見很好，他點出一個很重要的問題，你們所提的母法是以機關為單位，你們管理的範疇、直接限制的對象是以機關為單位，你用一個公務機關以及非公務機關去作為你管理的範疇，請問一下怎麼可以說子法的時候就翻盤？以他牽涉的機密程度或他承接的業務作為…這些東西你的母法文字沒有寫到，子法可以這樣訂嗎？你可以告訴我你的母法是以機關為切割單位，結果你子法去訂定管理的層級核心範圍是以…

主席徐副處長：

我們現在的設計邏輯是這樣…

親民黨立法院黨團：

我現在在講立法技術的問題，我就是要呼應吳顧問，你不能把公法學者跟資訊專家學者把它切開，你要知道立一個法要規範…我先說明我們的立場，我們親民黨團的版本非常簡單，我們只會拘束行政機關，不會拘束所謂非公務機關的部分，我們先表明我們的立場，我們參加這個會議也不是要幫你政策和版本去背書，我要特別強調。

我跟你們講話都覺得很痛苦，因為你們都不會回答問題，我都跟你講了，你母法明訂是你要規範哪些機關要受到你們的管制，你們的單位是機關，不是他的核心業務，你們自己訂的很清楚，自己的定義就是這樣寫的，本法用詞，定義如下：關鍵基礎設施提供者、公務機關、非公務機關，你們都是以一個實體的存在作為你們規範和管制的對象，然後你告訴我子

法要變成要看核心業務有沒有涉及國家，我們認定有沒有危害到我們社會公眾利益的時候，也要把他規範進來，可以這樣子嗎？母法沒有明訂有這種東西，你的子法有出現這種東西，可以嗎？這是一個很簡單法學緒論的概念，不需要什麼公法學者在裡面，我們都知道不可以這樣訂，你覺得這樣可以嗎？

我們現在就一條一條來跟你算帳：第一個，我想請問一下，資通安全管理法第1條，你們到底是要推動這個資安產業？還是要做資安管理政策的訂定？你可以告訴我一件事情，食安法有說我們要促進食品工業嗎？沒有，就是要管理食品的安全及衛生。

主席徐副處長：

我想這個問題我們在前幾次會議有人提到…

親民黨立法院黨團：

我跟你講，這個接下來我會談到，你放心好了，我不會放過你的，第2條有關於公務機關、非公務機關、關鍵基礎設施、關鍵基礎設施提供者，這部分我已經講很多遍，我們就是希望能夠正面表列，你要管制哪些行業，就是要把它列進去，為什麼？很簡單，就是為了法律保留原則及法律明確性，我們真的不能空白授權，讓你們到時候覺得什麼是關鍵基礎設施、什麼是關鍵基礎設施提供者，你想要列進去就列進去。

我只問一個很簡單的問題，其實公務機關不應該外包核心業務，但問題是民間機關想要外包核心業務，那他們家的事情，對不起那就是民間，他愛怎麼樣自由去外包業務。我請問一個很簡單的問題，如果有一個民間公司列為關鍵基礎設施，也是關鍵基礎設施提供者，可是他把他的核心業務外包給另外一個公司了，請問這個公司算不算是關鍵基礎設施？A公司是關鍵基礎設施，他把他的核心業務一部分委外外包給一個B公司，請問B公司要不要提資安計畫、稽核？這個你們要去思考。

我們看第3條，第3條的問題其實就跟第1條問題是一樣的，今天到底是一個政策推動授權給你們做資安政策的法？還是你們要搞產業？我也不用講太多，反正立法院的報告大家都可以拿得到，我們資安基礎建設推動及經費執行之探討，我看了報告，我完全懂了，這個法的目的完全就是把現在所有的行政機關、委外的科專、計畫全部把它合法化，因為你們列了這四個項目，現在行政機關全部都有在做，成效好不好？不知道，委託給

哪些法人？我也不知道，我們會去查，這個是第3條已經把現在行政機關委外或委託辦理或委外研究的那些科專、那些計畫全部把它合法化了，簡單來說一言以蔽之，這樣會不會有什麼商業利益的糾葛？我不知道，這個我們要去查。

第4條沒有什麼問題，因為本來這個就是你們在做。第5條，你們訂了這一條，又要第三方驗證，就要委外稽查，從我們這種立法院委員的助理來講我覺得很不可思議，副座您知道勞動檢查也是有勞動檢查專法，不是資安法訂了一條，所以我們就可以去稽核第三方驗證別的私人機構，沒有，我們要做勞動檢查，我們還有一個勞動檢查專法，而且他有明訂勞工檢查員本身的權利義務，以及他如何不去侵犯這些被檢查民間公司的權益，還有明訂他的資格。這一條我根本認為不應該存在，如果到時候真的有要這一條的話，一定要訂一個資安檢查專法，我認為才會合乎保護人民權益。

第6條:行政機關應衡酌公務機關及非公務機關業務之重要性與機敏性…我不太知道你們要怎麼樣衡量，你可不可以告訴我你們用什麼樣的行政程序去衡量所謂的機關業務之重要性、機敏性？因為大家關心的是非公務機關，你們只是規定我們可以做這個事情，但是程序呢？你不要又告訴我說子法、又尊重立法院之類的。「行政機關得稽核非公務機關資通安全維護計畫實施情形」，這個其實就是牽涉到前面第5條的部分。「非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向行政院提出改善報告，並送中央目的事業主管機關或直轄市、縣（市）政府。」你們這個設計是不是會有問題？為什麼一個這樣的缺失同時要跟三方報告：行政院、目的事業主管機關、縣（市）政府？可不可以告訴我？因為你後面指定基礎關鍵設施是中央目的事業主管機關或直轄縣（市），結果你現在這一條裡面第6條第3項規定這個同時要送兩個地方，一個要送行政院，一個要送縣（市）政府，這樣行政院來統管就好，為什麼要做這種設計？你可不可以告訴我你的原理是什麼？

第7條：行政院應建立資通安全情資分享機制。你都沒有一個中央資安的防護機構，請問你要怎麼樣分享？能不能說明一下，你們要怎麼樣讓所有人去分享這個資安的資訊？我們來看第8條，這個就很詭異了，你們是在綁樁嗎？「公務機關或非公務機關，於本法適用範圍內，委外辦理資

通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目、性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。」請問你們要推什麼公司認證嗎？你可以告訴我嗎？如果今天一個非公務機關，我委託一個你不認可的廠商，你要罰我嗎？還是你要加重稽核？從檢查一次到變成檢查三次，這條的目的設計是要做什麼？公務機關為什麼寫這一條？自己按照採購法就可以去處理這個問題了，對非公務機關還要去限制他的採購廠商，請問你們侵權行為的依據在哪邊？請問你們要訂定一個認證標準去訂什麼是適格的廠商嗎？所以你們要公然綁標嗎？目前先這樣。

主席徐副處長：

謝謝親民黨黨團給的意見，你昨天有發文給我們，希望我們今天能夠討論子法，所以我們當然…

親民黨立法院黨團：

因為你們子法不拿出來的話，我們都討論抽象的原則沒有意義。

主席徐副處長：

所以其實今天剛剛報告的內容…

親民黨立法院黨團：

因為你們的內容之前我們已經看過三次了。

主席徐副處長：

所以我們今天主要目的是希望能夠對於我們現在子法內容可以給一些比較具體的意見。

親民黨立法院黨團：

我給你就是子法的意見，因為我完全不認同你這個法，所以你這樣訂我根本覺得不OK，你沒有回答我的問題，因為你們這個子法設計完全是按照你們自己的邏輯去設計的，我只問一個很簡單的問題，譬如第5條部分，我就不認同你們這樣的設計，就算按照你們版本過了，你們的資安稽核以及資安檢查就要訂一個專法，所以你們按照子法訂這個東西我完全不認同，很簡單，因為勞動檢查法也有明訂資安人員要考什麼證照，如何不去侵害到受稽核、被檢查單位的權益。

主席徐副處長：

這個沒有問題。

親民黨立法院黨團：

這個不是沒有問題的問題，全世界的人都知道，立法委員最不關心就是子法訂定。

主席徐副處長：

你剛剛提的部分我們會參考。

親民黨立法院黨團：

這不是參考，這是應該的，你自己想想看看勞動檢查這樣對於民間公司權益的侵害這麼輕微的情況底下，都要訂一個專法，資安搞不好都會碰到人家的核心業務，你還跟我說這不用專法？

主席徐副處長：

所以你的具體建議？

親民黨立法院黨團：

第5條應該刪掉，而且應該訂專法。

主席徐副處長：

因為母法就還是到立法院去做最後的決定，這個我們尊重。

親民黨立法院黨團：

為什麼我昨天會發文一併要把子法拿出來，因為只有看你們子法有多麼的荒謬才知道母法應該要怎麼立，第5條應該寫，如果按照行政院版本，基本上我要再次說明的立場，我今天對於這些立法技術提出缺失的建議，不是代表我認同行政院版，我只是看到行政院版就一個很普通念完法學緒論的人，就可以看到一個很明確法學的缺點，第5條如果真的要訂資安稽核或是資安檢查，後來那句話應該「另以專法訂之」，不能用子法，為什麼？因為你要侵害人民的權益，萬一他洩漏怎麼辦？勞動檢查專法裡面對於這個都有規定，謝謝。

萬幼筠營運長：

這樣的話可能個資法也要修，個資法的行政檢查列在子法裡面的細則，我建議助理可以回到黨團…

親民黨立法院黨團：

我講就是代表我們的立場，我們認為就要訂專法。

萬幼筠營運長：

這個我理解，我沒有問題，可能一致性，可是你一直強調勞檢，因為

我希望立專法，跟個資法一併討論，不要只看這個，反正個資法也有資訊安全規範細則在裡面，把它綁在一起談，可能一次解決，不然就好像我們勞檢或這個專法，結果個資法變成是一個漏洞，他還是只是在細則裡面擬定，這樣在衡平上可能會比較…

不過我解釋一下，大家一直說沒有法律學者，在座有林宜隆老師，我是政治大學法律研究所，我在東吳大學教法律基礎法學，所以我先講我簡單的意見。

第一個是第8條的本法，我有一個實務上的建議，因為這邊一直談到委託，可是因為我知道行政程序法第15、16條授予行政機關以及民間機構委託的法源依據，所以我要回答助理的問題，我們政府機關說不能委誰或可以委誰，它有法律依據，請大家回到行政程序法去看，但是這個委託裡面有一個現實的狀況，是因為通訊安全的專業複雜性很高，所以委託出去可能會很多重，第一個他會再委託，我們在個資法裡面有談到再委託的事情，因為當時寫細則的時候我有跟法務部法律事務司談過，這一點一定要寫，可是在這一次的專法裡面，我不知道第8條裡面的委託含不含再委託，舉例，我委託一個民間公司，或是誰做了一個A項的資訊業務，他又再次往下捆綁，我從本法看第8條，我發現我只能對委託機關有監察的權利，對再委託機關沒有監察的權利，而且所有的權利義務要回歸委託機關跟再委託機關的民事契約，如果他的契約訂定的是不完整了，那政府喪失監督的權利，這一點是有風險的。

第二個部分，又link到剛才系爭頁數的第27頁，裡面對於安全責任的分級劃分第C點，他規定一件事，我有重要系統運用開發、有伺服器主機者，我套用一個例子，他如果放到雲端呢？他沒有主機，系統開用到雲端上，他完全規避A、B、C，到D了，可是他的應用系統可能很重要，可是因為現在所有的委任，在契約行為上放到雲端，政府不可能自己建立一個電信機房，所以政府的電信機房概念上看，都是可能用中華電信，所有沒有一個政府的，你所有行為就是委託，甚至是再委託了，我們沒有辦法把它跟第8條的精神做link，我認為這裡面是一個風險，所以建請不是條文母法的第8條可能要調整，不然就要在細則詳述，或是請兩位黨團的長官們可以針對這一點稍微補強，否則的話我們會出現一個很大洞，一直往下委，委的可能是中國的公司，甚至其他國家的公司，這個風險系數太高，這

個是我建議的。

第三個部分，因為剛才吳顧問提到委託他人的資格，我完全贊成，可是套美國經驗，要稍微澄清一下，因為我在美國工作過，人一定是Security clearence，他的身份背景是不是安全關係？有沒有驗尿、有沒有Speeding，對於安全的訊息，這些資訊、這些標的物是classify，他到底是什麼等級，所以他的安全等級會因為牽涉到的人等級不同，安全等級會調整，所以就會有一個律定，你單看一件事，這個標的物對不對？可能牽涉到的人很重要。我舉個例子，總統府的長官行程表看來不重要，可是他是總統，當然很重要，如果移做他用，也很重要，所以他的人跟標的性這個部分我是建議未來可能要像吳顧問建議的，委託他人資格的規範上，可能要特別考量技術性的要素，這樣會比較容易繼續去施作。

最後一個我要特別解釋，剛剛一直講歐盟的法律，那個是我鑽研的主題，歐盟稽核跟Compliance，它的概念是很像，可是適用標的是不一樣，譬如稽核是指我們企業或組織自行降低風險的方式，遵行是把這個東西都查核，變成法律規範的要件，才叫Compliance，所以要看我們符合的目的是誰，當然你沒有訂的話，我自己因為你的法律責任，律定我自己的內部規範，我可以說是稽核，可是這個稽核的結果不能代表我已經遵守法律，如果有公法學者在，可以講得更清楚，是更好，因為我覺得這個東西需要一起來描述，以上是我幾個簡單的建議。

主席徐副處長：

謝謝萬總的建議，我覺得這裡面有剛才綜合幾個吳顧問的意見，我們就一併納入思考，其實這個Security clearence部分我們也有注意到美國一直有這樣的措施，這個意見其實非常重要，我可以帶回去跟我們行政院法規會做一些研究，如何在人員的規範上，至少在資格上的一個限制來去做一些規範，我覺得我們可以考慮來做這件事情。

其他的部分有關稽核、compliance這個部分，我們會再請教公法學者，你剛剛有特別提到，他們在這個方面可能會一些比較明確的意見，或者在歐盟一些相關法律上的做法，這個部分我們可以再去做請教，或許在下次的場次裡面，我們會找幾個，請他們針對這個部分提供我們一些經驗的分享，我先回應到這邊，我想再聽一些其他專家學者的建議。還有沒有要對這個施行細則的部分？

親民黨立法院黨團：

我要補充一下，行政程序法的規定是說「得」，不是說一定要，而且要注意，行政程序法是一般法，今天資安這樣一個關係這麼多公司權利的部分，我個人認為他的這個比例原則的強度應該夠到立專法，不能視為一般普通的行為為之。我記得法務部對於有關於行政程序法上面委託的部分有提到，有關於個別立法面行政委託的部分，要視立法者的意思來去訂定比例原則。換言之，今天這個資安法裡面，有關於委託的部分我們是不是要提升到一個專法的位階？當然這個就是我們立法院的責任，在審母法的時候我們對這一條到底要採取到什麼樣的態度？要提升到母法呢？還是要怎麼樣？還是視為一般的行政程序法規定委託的層級？我覺得這個就是立法院自己要去考慮一件事情，謝謝。

主席徐副處長：

這個部分就尊重立法院的意見，還有沒有其他的建議？

黃明達教授：

我覺得資安法很重要，所以我和幾個朋友來聊一聊，我大概有幾個看法，我們看這個條文第2條，麻煩切母法第2條切一下。

主席徐副處長：

我們今天沒有準備母法條文，老師你可以講，因為我們手上都有。

黃明達教授：

第一點，第18條裡面有提到所謂重大資通安全事件，什麼叫做「重大」？我聽起來大概是偏向於這邊定義的第3、4級，所以在條文裡面要注意一下，但是教育部是第一層5級，0到4，是教育部要發文還是什麼？要請教一下。按照第2條裡面要不要增加資安事件的定義？因為在學界裡面資安事件是比較廣泛，比較重大一般就是資安事故Incident，所以這邊說的重大資安事件可能把它定義一下，這個是第一點建議。

第二點，有關第10條資安長，到底我們國家的最高資安長，一般各個公務機關都訂資安長，這邊的角色、職責應該把它定義好，這個是在子法裡面應該要注意的。

第三點，第16條，CI的提供者，關鍵基礎設施提供者，以外的非公務機關，這邊看起來是有公營事業還有法人之類的，因為公營事業牽涉範圍滿大的，各行各業都有，所以要規範一點，例如公營事業還有可能做土木

建築，和知悉都無關，那個要不要計入？這個也請教一下

第四點，有關第16條「得」，這個得就很有彈性，可以有也可以沒有，所以也可以思考一下，這個「得」是不是要改成「應」。

第五點，第5條剛剛吳兄有提到這個觀念，中央目的事業主管機關有關稽核這方面認為有必要，什麼叫做「有必要」，這個也要訂定清楚，不然這個長官權限就很大，他認為有必要，要去就去，事實上就沒有事，擾民也是一大堆。

第六點，我們幾個在聊的時候也提到有關資安工作項目，是不是要定義清楚，行政院資安處只負責政策，機關是負責稽核，現在目前主計處是負責稽核一些政府機關。

第七點，這點是我剛才和總監有稍微聊一下，我們這邊的CI有點怪怪，是不是應該叫CII才對？剛剛吳兄有提到CIIP，是不是CII會比較對一點，CI太大了，我舉例，像高速公路應該算CI，但是高速公路裡面有很多控制系統，那個可能就CII，你不把它定義清楚，國土安全在裡面會打架，整個牽涉方面會弄不清楚，到底是CI還是CII？這個大概要思考一下。

第八點，如果CI定義清楚，這邊有一個服務對象，在簡報第27頁，我請教一下，這邊有兩個問題，剛剛蔡教授有提到B級公立大學，私立大學事實上比公立大學還多，我們統計是這樣，私立大學是6，公立大學大概是4，事實上很重要的資訊大概都在私立大學，公立大學比較少，這方面在教育部裡面B級是包含什麼？是包含所有大學都算B級裡面，C級就像學院之類的，這個也可以參考一下教育部。

第九點，有關於第29頁，這是個小問題，資安防護應該都是APT的防護，當然是為防火牆，人家是蓋一個防護之類的，這小問題。

第十點，簡報第29頁ISMS，管理面這邊是2年內完全ISMS導入全部核心系統，根據我去查一個ISO規定，認證範圍大概偏向於product或service或system，我一直聽到這個system感覺不是那麼漂亮，可以加一個什麼？應該是全部核心系統或服務，產品就不用了，至少兩項核心的資通系統或資通服務，可以參考一下，這個我們討論很久，給各位做參考，謝謝。

主席徐副處長：

謝謝，很多對我們文字上的調整，母法的部分因為這個版本已經送立

法院，所以不管是「得」或是「應」，基本上行政院立場其實之前都有考慮過，到底是「應」還是「得」，現在目前有些就是「得」，並沒有很多規定成「應」，大概都是有考慮過，在這邊做一個說明。其他有一些比較細部的意見，我們基本上都在細則或其他子法裡面可以考慮做一個修正。接下來還沒有其他的專家要給我們一些建議？

蔡敦仁教授：

不好意思，因為我法律方面不是很懂，所以有一些疑義不是很周延，跟大家抱歉一下，因為我們今天要討論子法，可是我在想我們這個母法的目的，可能是要讓我們資通安全做得更好，尤其裡面提到要帶動產業發展等等。我們這裡面規範的主要就是公務機關跟非公務機關還有一個是行政院，就這三個角色。因為剛剛簡報也有看到，有一些國外除了罰錢以外，還有一些刑事責任，是不是有可能在未來對這部分也做一些規範？如果機關你去罰他錢，其實不會處罰到個人，所以他也許會做某一些奇怪的事情，譬如有惡意或重大影響的行為，如果在那個單位裡面，公務機關應該沒問題，可是如果是非公務機關的話，是不是有辦法去罰到一些人？另外一個就是反面的，如果那些駭客、惡意入侵的人，我們有沒有辦法去規範他，我要做資訊安全，不是有人說「資安即國安」嗎？對於這個是不是也有一些規範？也許這個可以考慮。

在很多政府機關或者是業界在討論個資法的時候，其實大家都反應一個問題，我們要保守的有時候不是個資而已，我們要營業的機密或其他的，公務機關沒問題，可是那一些非公務機關他的營業機密那些資料，怎麼樣去規範他？如果我們的子法可以把這個部分也納入，也許會解決部分的問題，因為上次行政院有說，請法務部去討論這件事情，可是後來就不了了之，因為沒人知道適用什麼樣的法律，這個可能是一個問題。

我們這邊的非公務機關的定義跟個資法非公務機關的定義是不一樣，我建議既然都是法律，也許應該定成一樣，我們只是講第一階段先適用於資訊基礎設施的行業或者是國營企業，而不是自己發明另外的定義，跟我們一般的法律見解不太一樣。就像個資法當初在施行的時候，也有幾條是暫時先不適用，也許可以這樣去思考。而且非公務機關如果以個資法的做法，其實是由目的事業主管機關去監督他，所以大家都逃不掉，只要是一個公司都適用個資法。我想資通安全管理法是不是也應該階段性的？有一

天所有的公司應該都適用，而不是我現在的做法是有人攻擊的話，我就少一點，所以就有人說八大行業，可是我們的目的在前言裡面有說明，就是要促進國家整體的資訊安全，我們的願景滿大的，可是我們現在又把它限縮到很小，其實以目前這個階段，我們的資通安全管理法也沒有迫切性，為什麼？因為這些事情都有相關的辦法，而且資安處也正在做，如果我們要想到一個未來性的話，應該是把這個法律訂得比較周延一點，而不是把它變得限縮。

當然這個問題會跟當初個資法施行的時候一樣，因為很多反對意見，認為我們還沒有準備好，所以我們應該發展資訊，不應該綁手綁腳，當然都有它的理由。個資法管理已經到現在這個階段，大家都能夠接受；可是資訊安全管理實際上更應該去規範，因為資訊安全濫用或者誤用的情況是滿嚴重的，我們訂出這個法律大概解決部分的問題，可是實際上我們沒有解決的問題搞不好是更多，我滿期望在我們在那些子法裡面怎麼樣去做一些加強。

我們在過去做相關稽核的時候發現，有一些也許可以思考的問題，剛剛有一位先進提到，像伺服器如果放在雲端，另外一個，我們現在分A、B、C、D，出發點就是他的資料很重要或者他的業務很敏感，可是有些單位根本沒有足夠的資源跟人力。譬如他只有1、2個人在管資訊或者是資安，這個單位不可能額外再配置額外的人力或者是資源，也緩不濟急，而且也沒有必要，因為本來單位就很小。對於這樣一個單位把它分到A、B、C，其實是造成一個負擔跟困擾。應該有一些方式，如果處於這種資源有限的情況，我們應該有一個規範強迫他這些資訊、資源應該向上集中，在單位裡面基本上只是一個取得service而已。

向上集中到哪裡去？現在是到部會，可是有一些到部會也沒有能力接受的時候，我們是不是要有一個方式由國發會或行政院來收容這些，因為真的有很多單位他東西很敏感，可是他根本沒有能力，你叫他放到哪裡？像這樣的問題也許是應該要來適度的解決，不是我們A、B、C、D一定要檢查哪些東西，他本來就沒有什麼資源，你又叫他做這些事情，可能他也沒有能力。

我們這邊另外有一個，我們希望能夠去帶動產業發展，跟我們有一些相關法律一樣，會有促參條例或中小企業發展，這裡面找不到東西去獎勵

，或者是做什麼事情，讓我們的資安產業能夠發展，因為我們只是間接講因為有這麼多服務委外，也許會發展，可是他的發展只是在部分的人而已，應該我們會有一些子法，我來促進他發展，你做什麼事情我獎勵你，或甚至政府相關的資金會投注到這方面，要有一些相關的鼓勵，也許是辦法或者是其他的。

另外，我們在做很多事情，剛剛有先進講，行政院有很多事情可以委外，在稽核的時候我一直在想，我們的稽核跟ISMS、ISO 27001的稽核大致重複，除了技服中心有另外做技術稽核以外，是不是像這個東西就可以委外？即使行政院去稽核的話，如果我們認可了這些稽核單位，他就可以來扮演這個角色？而不要又重做一次？這個也算是擾民，因為同樣的東西檢查兩遍，基本上也沒有什麼太大意思。或者甚至由行政院授權另外做一個稽核的規範，而不要僅限於ISO 27001，因為ISO 27001大概大家都有發現他只有做管理面的，所以在技術面可能是有所不足。

另外我不知道在母法裡面有沒有可能去增加資源跟人力配置的規範？我們不一定要給他百分比，只是他的上級機關應該適度去提供資源跟人力的資源，也許有一些子法裡面或是施行細則再來解釋什麼樣的措施來做這些事情，謝謝。

主席徐副處長：

謝謝蔡老師的建議，我大概簡單回應的一下，剛剛有關政府機關人力的這個問題，透過這個法裡面讓機關可以有一點依據在內部去爭取人力之外，其實在前幾個場次我有大概說明過，我們政委也有召集我們相關機關來討論，未來資通安全管理法一旦通過之後，政府機關應該會支援，其實這個問題都有在處理當中。

另外一方面是透過資訊資源的向上集中，往部會去集中的方式，讓部會統籌所屬機關去提供資訊服務，3、4級機關原則是不設資安人力，除非他有提供全國性的業務，目前在過去的組改過程都是這樣的原則在處理。其他有關到底現在法的規範範圍要不要再擴大，不限關鍵基礎設施提供者？因為我們目前就是以關鍵基礎設施等為應該規範的對象，目的是以國家安全跟公共利益的角度來看這件事情，我先補充這兩點。好像還有吳老師。

吳宗成教授：

不管公法、民法，萬法歸宗，剛剛講這個法律，不是訂給這個法律的人能夠了解，法律是要你在執行的人能夠依這個法執行，要讓民眾知這個法、守這個法。我不是法律專家、法律學者，但是如果訂這個法，我要知道這個法要幹嘛、未來我怎麼去遵循這個法要幹嘛，這應該才是立法院兩個黨團的代表回去要督促立法院把這個事做好，訂一個法律出來是要能夠去做、能夠落實，這個是我第一個呼籲。

第二個，我們來談資訊科技是沒有界限，沒有國界，看也看不著、摸也摸不到，管理是有範圍的，沒有範圍怎麼去管？所以看我們把這兩個名詞放在一起，可想而知，一定會有很多的爭端、爭論、很多不確定的因素，一個是摸不著，一個是要有範圍，管理就是要有範圍，不能訂一個法說要來管理，管哪裡？管上天，管下海，管那麼大？這不可能，所以管理一定要把這個範圍訂定很清楚。有些管理是可以透過一般的行政程序、行政手段，所以有人說這個人很會管理，管理這個事到他手上就做得很好，另外一些人可能就做不出來，管理方式不一樣，有些的管理就不是，大家都要去依循，代表這種管理是必須很清楚的、很明確的。你的程序剛剛幾個先進都講到一個名詞「compliance」，compliance就是依據這個程序、這個法律，我可以去達到，相關的細節的條文我就不再去做說明，或者再提供建議，因為剛剛幾位先進都講得非常清楚。

我就從這個法的本身來看怎麼去訂這個法，我在很久以前這個草案剛開始有一個draft，那是在前年的時候，我就說這種法定出來不要定成像一個資安的稽核守則，這個法訂出來是要讓大家心理有一個依循、遵從，有一個目標很明確在那裡，我們怎麼去做，也不能講得很細節，講到很細節，就變成大家每個人讀了以後各自表述，不知道怎麼去依循就違反我剛剛前面講這個法，要訂一個管理的原則。

法裡面我看也看不太懂，但是以前我也提過很多次的建議，這裡我忍不住還是再說一下，第一個什麼叫做立法的目的？第一個，越簡單越好，大家的解讀要很清楚，不會覺得我這個法要規範出來，管到天、管到地、管到海、管到山，而要很清楚，而且後面所有相關的條文，都是要滿足或是達到立法的目的。剛剛兩位蔡教授都講到。我們訂這個法要推動國家資通安全政策，這是我們政府該做的事。第二個，要加快建構國家資通安全的環境，這也是所有的企業都要去做的，因為沒有做，像你是一個資通公

司，你沒有一個好的資安環境，你根本就接不到生意。企業好、民眾好，當然整個國家法令都好，所以這個不需要特別用這個法來訂。第三個，大家批判最多的，帶動這個產業的發達，大家能夠遵法、知法、守法，本來資安就很重要，沒有人說資安不重要，很自然這個產業就會帶動起來，我們很多科技的運用、創新的模式都認為這個很重要，自然就會帶動起來，也不需要訂定這個法。

所以要達到的目的是國家安全跟社會公共利益，就涉及到對象，我們這個法要規範的對象以我普遍的認知，雖然我不是讀法律的，但是我們看很多法的認知，這個對象有一種是規範自然人，簡單來說，一個就是規範人、一個就是規範一個機關或者一個公司或者一個全體或者一個組織。就規範一個人，人當然就是跟個人所謂的利益有關，譬如個資法，你會不會因為你的企業濫用我的資訊，這個法會規範濫用資訊；或者你這個機關有沒有盡到你的責任，讓個人的權利受到損失。這個是人，你要規範的是人。第二個，是規範機關，機關影響層面就很大，一個組織跟一個人能夠造成的影響不一樣，一個組織能夠造成的影響很大，絕對比一個個人能夠造成的影響要更大。

假設我們今天界定的不是這個人，是對於這個機關有一個約束力，我今天不管公務的機關、非公務的機關都要受到這個法的約束，你要很清楚的告訴我，我有沒有違反這個機關的作為，讓民眾、讓這個機關裡面國家達到利益的損失，才用這個法去約束他。最後的問題就來了，誰能夠認定你違反這個法？什麼叫違反這個法？剛剛就說檢查，我就舉個例子，剛剛也有先進提到檢查員，是不是每個人都可以在大樓裡面牽水電、架設水電？不行，為什麼不能？因為這個涉及到公共利益，涉及到公共的安全，所以我要有執照、證照，我們來做檢查的人執照、證照是什麼？那個水電是歐盟發的水電執照，可不可以在台灣架設大樓的水電？是美國發的執照，可不可以在台灣架設水電？我們就用這個來做比喻，我們後來發現當我定這個法以後，缺了一個這樣的東西，你說通過拿到ISO 27001證照的都可以來，那就落到我剛剛講的事實，拿美國的水電執照在台灣的大樓牽水電、架設水電。

所以我們這個法裡面也要有相關證照的能力，以後什麼人能夠來去判定這個機關是不是沒有落實、依據這個法來進行。剛剛我看到1天要幾個

小時做什麼，看到這個我就想到這個比喻，這不對的，我們有太多資安的證照在國內都不是我們自己政府訂定相關的資安證照。我們在這個法裡面就開始要建立這個制度，讓這個法能夠實行，要去把那個環境建立起來，所以你光談每年要稽核幾次，就落入那種迷思了，這個其實是不需要的，那個是你的作為。剛剛談到，Web security、APT，我看搞不好過幾年連Web這三個英文字母就不見了，哪有人還在用Web，APT搞不好以後新的名字不叫APT，我也不知道叫什麼，反正總之就會有一個T，attack、威脅，threat，你把這個弄在這個法、弄在這個程序裡面，我認為不太妥，可以再思考。

最後一個簡單的結論，這個法寫出來，不管你寫的專業也好、不管你寫的廣度也好、不管你寫的所謂的範圍很小也好，一定要能夠執行，這個執行一定要讓民眾知道這個法在幹什麼，第一個要能夠執行，當你沒有爭議、糾紛。像剛剛提了幾個檢查，對於關鍵基礎設施的認定，在幾次的公聽會也看過很多的訊息，這個都有很多的討論、爭執，就代表原先的定義並不是那麼周詳、周全，可以再把範圍再縮小一點，我們現在談的個資法，還不是一樣經過好幾個法修過來，原先從我規範你政府機關、原先我規範你幾種行業、原先我規範你幾種資料的模式跟格式，到最後慢慢擴大，現在民眾你問他什麼叫個資法他都知道，之前你問他什麼叫個資法，他會說我不懂電腦。什麼叫做個人資料保護法到最後他很自然而然就會成為一個大家都能夠知法、守法，所以一般人沒有法學素養他可以講，你侵犯了我的個資、權益，以前只有講八大行業，大家還搞不太清楚，因為那個太專業、太專門、範圍太狹隘了，但是畢竟那個範圍是明確的。

最後還是希望幾個條文的一些文句「應」、「得」、「適當」，這種字一定都要講清楚，可不可以這樣？反過來，如果不能這樣，未來我怎麼去認定？難怪人家對你現在這個草案裡面會覺得好像簽一堆支票給你們，適不適宜、可不可以，都是你們自己說了算，執法的人不能這樣。第二個，你要大家遵循很清楚，你要告訴他這個應該是怎麼樣才叫做違法，所以你訂了那麼多子法，我的感覺好像是把，ISMS或者把ISO相關的document再分成好幾個相關的section，我個人是不太贊同這樣。除非這個程序是依據我們自己訂立的程序，我們訂立一個檢查程序、我們訂立對於關鍵基礎設施的定義是什麼。看過去好幾個國家在發展的過程，Information

provider是一個對於資訊安全裡面很重要的因素，現在規範台電該遵循什麼法、中油要遵循什麼法，我覺得離現在在釐清的階段還有點遠，最好這個文字上看能不能做一些比較限縮或者明確的說明，否則以現在這種草案條文我是認為還是存在很多各說各話，或是沒有辦法聚焦的條文，以上。

主席徐副處長：

謝謝吳老師，剛剛聽了滿多各位對於有些部分可能需要再做更明確的規定的部分，其實母法的部分還是維持一個原則性的架構，子法的部分其實就是在補充現在母法不足的部分，我們會再做細部的規定，剛剛其實也聽了滿多的，我想我們大概會針對今天的意見，逐條再就子法的內容，包括各位非常關心的行政檢查、CI跟CII是不是再做一個比較明確的訂定，包含什麼叫做重大資安事件，資訊如何分享，我們都會在子法裡面做規定。

李盛安教授：

我這邊簡單，其實我不太懂法律制定流程，我長年在TWNIC做一些地方政府業務推廣，實際上看到前幾次討論會提到的一些事情，一個是沒有經費升級，服務本身有很多的漏洞，應該是升級的時程，因為像TWNIC在推IPV6這10年中間，我們都問地方政府說你們推動的時程是什麼，你們寫一個升級計畫給我們，那我們會知道什麼時候是升級硬體，什麼時候是升級軟體，如果他們升級的防火牆不會設定，到了去年我們變成開始輔導地方政府怎麼去設定防火牆，發現那個部分是非常專業，專業到有些廠商沒有辦法提供相關的服務。

我好奇的情況是說，其實這幾年發現資安事件實際上都是比較像是web網站，或者是一些真正data service的形式被發現、被發生，才爆出來的，今天早上又有銀行發生被DDoS攻擊，那個消息很新，我今天早上看到的，實際上資安事件本身牽涉到技術層次的範圍非常的高，今天不是像實體的資安事件，譬如說異地備援、資料竄改或資料認證這樣的形式的話，一般自動化的資安事件我覺得資安處常年有在做，是不是有可能變成自動通報的形式？整個事情已經被發現說流量非常異常，或者是服務已經完全中斷的時候，那通常已經算是非常嚴重，這樣的情況也許列在專法或是子法裡面。我們之前也發現一件事情，沒有法令確實地方政府在施行的時候會覺得很模糊，因為他們會覺得我不做這個沒有罰則，可是我要做的時

候沒有經費，所以多年來我們發現訂成要真正的升級計畫，不然的話是沒有任何依循的準則，雖然已經有一個法令，可是實際上還是會有年度的完成時間，大概這幾次開會的時候有這樣的感覺出來。

主席徐副處長：

好。

林宜隆教授：

立法的基本原則，立法是要解決問題，首先我表明我贊成立法，但是立法會涉及很多層面，最重要比例原則，影響最大的，這裡面有一個原則，有法比無法好，這邊的原則是規範資通安全首重風險評估，在這個社會上得到更多利益的人他付出代價，舉例某個行業對於社會在cyber space影響很大，當然要規範阿，否則譬如公路上卡車亂撞誰負責，環顧全世界現在有沒有法律，大陸有沒有法律，大陸的網路法6月1日通過了，美國的FIMAS，它的M原來是Mangerment，到2014年叫Modernization，我當初在15年前就提出說要立這個法，這裡面有爭議，但爭議沒關係，downsize，把它縮小一下。剛剛吳兄說的，他講的也很對啦，再拖下去就不會過。

第二個，這個法律規則怎麼樣來縮小比例原則，我在TWNIC的cert開過一個會，有一個駭客他講一個方向，如果我們遵守假設risk等於AVT這個公式，假設大家都認同27005的話，他說我們鼓勵做法都是A跟V沒有T，所以我們現在來思考一下，所以余宛如那個立法草案，這兩個的概念都不一樣，我現在有支持，國家我還是支持，但是余宛如那個我也滿喜歡的，整個立法機制，那T的問題，我們立法是不是要檢討，立法院的第一次原則，立法漏洞就是說網際空間是大家跟生活結合，既有法律不足，還有影響到大多數人利益所以我們現在要箝制它。這是立法漏洞。

第二個技巧是立法的精神，配合我們國家，我是國民，因為政府已經喊了，資安就是國安，那方向政策action plan要出來，如果大家都認為資安不是國安，沒有共識，那今天大家不要再談這個了，如果有共識，這個action plan，行政單位就要負責任，提出大多數人可以接受的，我現在沒有說服每個人，現在保障員額已經去掉了，現在沒有什麼法律強勢，現在人多就是強，再來就是，一直有網際空間這個影響到人類的生活，這裡面有一個很重要的說防護機制義務，你們在上面得到很多的利益，誰來跟你評估責任，誰要稽核，非公務機關當然也要，這個是新的概念我認為

法律就是因人而存在的，非公務機關在網際空間得到很多利益，你沒有一個很好的control，你怎麼知道他的品質誰來負責，一個車子到現在再生輪胎，要確保他有沒有去弄，也是要靠警察去抓，一顆輪子1萬跟5萬差很多，我當然要用1萬的阿，但是風險移交給別人，所以要強力執行，所以稽核是很重要的。

我剛剛滿同意親民黨的助理，我剛才花了時間去看了一下勞動檢查法，其實我也以前也有提到稽查涉及到權利入侵，那應該要有一個相當的資安稽核法，法律不足的時候，現在國際上已經有通過ISO的標準，譬如27007是ISMS的auditing，大師在這邊可是誰有在做呢？沒有，剛好你在稽核的項目是什麼？ISO 27008 security control auditing，那誰在做呢？你們只是看27001驗證，27002導入，那個是narrow down，那個是很小的。你都沒有去弄，甚至於各單位在實施計畫，你要參考什麼？不是27001、27002而已，你們要看27003它是ISMS的implementation，你們有沒有遵守，沒有。現在大家都27001和2，但3、4、5、6、7、8都出來了，這邊我在講說資安防護的工作推動義務，你在網際空間你的流量最大你的客戶最多當然你要受控制，如果按照交通規則來說就是這樣的狀況，以上因為時間因素本來我要說法律規範配合ISO，我要留給我們三位健將，他們也是認同法律要通過，只是方向不太一樣。

李忠憲教授：

可能在座我參加最多次，歐洲有兩個資安的法律要實施了，一個是通用數據保護條例，這個跟我們個資法有點像，它的罰則2,000萬歐元或是年度營業額百分之四，那一般的資安事件，如果不是什麼特別災害一般就是個資外洩最嚴重，這個法如果可以好好的執行也可以遏止一些資安事件的問題，那我們可能個資法裁罰的部分好像不是特別理想，這個部分大家也不會特別害怕。歐洲的企業現在是害怕得不得了，因為要罰這麼重。

另外一個趨勢是說2005年德國實施的資訊安全法，它實施的時候是納入了2,000多家的關鍵基礎設施，那它現在要多納入900家，就以前沒納入的金融、保險、交通、健康，通通納入。那這個在德國被批評的非常慘，德國的資安年度預算是下降，但是要管卻是管更多，前一陣子我看到一篇批評的文章是說，德國一年已知的資安事件大概有6萬件，德國聯邦資訊安全局大概有600人，年度可處理的大概是2000件，然後這個事情在通報

裁罰的部分還是罰10萬歐元，那我一直對於通報裁罰的部分是比較有疑問，就是你這個是要怎麼通報？小的資安事件大家不知道怎麼通報，那中等的資安事件罰則是200萬台幣，德國處罰是10萬歐元，那跟我的商譽比起來這是小錢，我為什麼要去跟別人說我不可靠，另外如果是大的資安事件的話，發生了，然後我公司嚴重損失，媒體追著我走，甚至於我可能要倒閉，我還管你通不通報。

所以不管是小、中、大都有它一個邏輯上的問題，那如果我們要走這條路，真的是要好好想一想。另外德國人口是我們4倍，土地是我們10倍，關鍵基礎設施即使新的納進去大概是2000多家左右，那我不知道我們這樣的情形，我們關鍵基礎設施要納進去多少？就是說這個部分的話可能要好好考量一下，尤其是通報裁罰的部分我覺得是有很大的困難在實務上要做，那資安處現在有些方向我覺得值得嘉許，尤其是資安消防隊的部份的話，你這些稽核、你這些產業願意納進來，資安消防隊給你一些協助，這個是一個好的方向。這個法是進步的是好的，但是你要用促進要用鼓勵，而不是用裁罰的手段放在前面，這是我一些小小的看法。

主席徐副處長：

謝謝李老師，我想要請教你一些看法，尤其你對德國的一些他們現在的資通安全法律也有研究，你提到的CI與CII的那個範圍，應不應該把它明確下來？我想我們現在從關鍵基礎設施的定義裡面，大概就是分八大類，有主部門、次部門這樣去分類，那我不知道就德國的立法技術上，他們如何去確定每一個關鍵基礎設施到每一個組織，因為我想在立法技術上很難去規定誰是關鍵基礎設施。我只是想了解…

李忠憲教授：

當然它在法律上沒有明訂，但是它在立法的同時已經把那2000家左右通通公布出來了。就是說，資訊安全局他決定要納管哪幾家，它就先列出來了，然後就是跟法的同時，它不是列在法律裡，是同時在做的，這個是他們的作法。

吳國維先生：

這個部分其實好幾個地方可以去查，OECD裡面也講了，很多地方包含美國政府也談到了。那我剛剛在講其實CIP與CIIP要切割，我當然知道國土辦它沒資源，所以國土辦就把這八大行業就塞到你這個資通安全法裡面

去，其實這個是非常不恰當的行為，CIP要防護的與你CIIP要防護的非常不一樣的，我舉過N個例子，中油的油庫爆炸，當然是國家安全的問題，但是會影響到中華民國的資通安全的operation嗎?當然不會，我沒有說那個不重要但是你們要防護的東西是不一樣的，你硬要把CIP與CIIP混在一起，這個本身就給你自己製造很多困擾，所以你那個八大行業的來源，大家都知道是國土辦塞給你的，很多CIP列出來的國土辦塞給你的東西，從資訊安全角度來說它都不是關鍵，你假設要問關鍵，基本上只有3個東西，至少OECD是這樣說的。

OECD講的關鍵基礎設施，只有三樣東西第一個DNS、第二個是IRX，第三個是主要的ISP。其他都不會被放進來，當然google所牽涉到的是其他社會衝擊利益問題，那個是另外一回事，那你就會面臨到一個問題，你在立法過程中就要非常非常小心，譬如說在座很多是大學教授，大家都知道我們很多大學用的DNS是8.8.8.8，各位知道嗎?Google從來沒說這是個產品，是你要用我沒叫你用，那假設發生狀況的時候，我也沒說這個不好用，是台灣自己的DNS管不好，假設有一個backup 8.8.8.8，not bad。

舉個例子我們自己國內只有一兩家業者在run DNS服務，那請問你在資安法或相關的法定裡頭，要不要規定這些ISP業者要run DNS，你被駭客入侵，或者你中毒了，就是一個資安事件，我就要通報嗎？所以我就想你那個就要講得很清楚，什麼要通報，什麼不通報，譬如說wannacry你中毒的時候幾十萬台，每個人都通報給你，你也受不了，因為你可能是要抓核心，你也不是要抓每個人。或者了不起你知道說文化大學有幾台電腦中毒，你只要知道個數目，然後因為文化大學忘了通報或是因為什麼理由，中毒又不是文化大學資訊中心中毒的是學生還是老師，然後它都不通報，好我現在罰你100萬，你覺得我會心甘情願，會爽嗎？要記得一件事情安全和方便兩個是對沖的，你要安全就會不方便，你要方便就會不安全，這本身就有個拿捏點，那個拿捏點是不容易的，所以我才一直講你要訂那個罰則要非常非常小心，除非你能夠很明確去執行它，否則人家一定會…我真的有問題的時候你又不能來幫忙，真的有事件的時候你說你要罰我的時候，到底你是用哪一個明確的條文來罰我？

特別我剛才講的18條，你要派人進入一個非公務機關，要非常非常謹慎的，因為你自己的母法寫得很寬鬆，這幾個中央事業主管機關又可以提

報關鍵基礎設施，雖然你說行政院定之，然後它又可以去管，然後通報又要通報給它，所以你面臨的問題返回來就像是剛才李忠憲所講的一樣，在台灣我們有沒有做過最基本的assessment，第一個請問我們台灣在整個資訊安全裡頭最嚴重的問題在哪裡，第一個你知道嗎？你可不可告訴我台灣資訊安全裡最嚴重的問題出在哪裡？譬如說為什麼歐洲梅克爾要訂那個東西，因為她發現美國政府很壞，那個資料流到美國，美國就把它竊取啦，相關東西美國就把它拿走了，那我就問了好幾年。

我們知道今天台灣的網路的資訊在流通routing的過程裡有哪些東西是跑到國外去了，我們不知道耶。我隨便舉一個例子，蔡總統發個email給屏東縣縣長，你確定這個信沒跑去國外再回來嗎？我們不知道因為從來沒這個information，所以第一個你要做assessment，要去了解我們資訊安全漏洞在哪裡，第二個問題是你有多少的resoureces？你不要講其他的，光說稽核好了，台灣這些稽核單位你把它加起來，你一年給他稽核兩千家，當然他會很高興，因為他就hire人就是啦，但是至少短期之間是做不到的。

請問你這個法通過了以後，你這個相關的資源配置到了沒有？你assessment做了沒有？請問我們目前，我們一年在台灣我們要做稽核通報，我要多少資源人力?假設你這點都不知道，你這是空中樓閣，講給自己爽的嘛，然後我之前講的，所有人都跟你通報，然後所有的credit都是你的，你可以跟行政院說今年發生了多少資通安全問題，都是人家貢獻給你的，不是你發現的，是人家貢獻給你的，變成你的credit變成大家的痛苦，這個邏輯是有問題的。

所以我是比較鼓勵說，這個法應該是大家合作，大家認同資訊安全是重要的，我們逐步來達成，透過assessment知道我們的資源能力到底到哪裡?初期可能隨便舉一個例子我們關鍵基礎設施這一百家，我就是要把你做好，那這一百家假設你已經做好，其實你很多事情已經解決了，而不要把它散到2000家、2萬家、20萬家。李忠憲他剛剛講參加很多場，我絕對參加比你多，我參加3次。所有業者都在擔心我是不是關鍵基礎設施，所有電商都跑來問你這個問題，你真的有能力去管2000、3000家嗎?假設你做不到就不要去承諾這件事情，你等於是讓每個人在資通安全法上去做違章建築，你鼓勵大家去做違章建築，反正你做不到，我用很務實地去談幾

件事情，最快的、最基本的assessment一定要做。

主席徐副處長：

謝謝老師，跟各位說，這個我們沒有credit，通報沒有credit。

吳國維先生：

這是你唯一可以拿出來的KPI。

主席徐副處長：

通報的部分只是希望我們能夠去，能夠做損害控制。那當然我們在通報的部分，以現在行政機關的通報過程中，如果他們需要協助，我們行政院還是會提供協助。我想這個部分，顧問剛才有特別提到。

吳國維先生：

損害控制，中華電信那條海纜斷掉了，請問中華民國政府要不要買一個海纜的潛水艇，然後隨時在那待命，只要海纜斷掉你就幫他做處理？不要讓業者還要從日本調船過來，調船進來就要十天耶，對不對？你真的能夠幫人家解決問題嗎？我才不覺得呢，你自己覺得而已。

主席徐副處長：

我們其實看這幾次、幾個資安事件，我先講我們碰到的例子，譬如說剛剛前輩有談到前幾次應該是證券業者遭DDoS攻擊這件事情，其實我們還是在協調、協助，因為其實它們有做通報的，通報的同時，我們同時協助、協調NCC與金管會對這些業者看能不能提供什麼樣的協助，我覺得站在通報的角色不是說…我覺得還是要回到通報的目的，在行政院的角度看，不是說要給行政院什麼credit，這個我在說明一下。

吳國維先生：

你所有的罰款都是在通報阿。

主席徐副處長：

現在的版本送到立法院是這樣，你也表達過很多次你的立場。現在的這個我們在討論的會上，我也沒辦法跟你說是或不是，現在行政院的版本就這樣子。我剛才也特別提到，未來這個CI的或者CII的在指定的同時，譬如說剛這個德國在立法技術上，跟我們的做法沒有不同的，但是它們在做法上是在同步去公布那幾個清單，我覺得這幾個清單的公布的機制怎麼去設計上，讓很多的multi-stakeholders，怎麼去討論這個清單，我想那個機制的建立是重要的，後續經過國家安全等評估哪些是應該被納進來關

鍵基礎設施，那個機制怎麼去確立，我想那個是後續我們資安處可以去做到的，跟各位做一個說明。

林宜隆教授：

這個罰款裡面的制定，第19條的第1項第五款和第六款，裡面的用語未依規定17條第3項跟17條第4項，我在看第17條裡面內容，第3項和第4項感覺一樣，一個是提出報告規定一個是有關通報內容規定，是不是同一個問題，第4項有沒有？第19條第1項的第5款跟第6款，第5款的後面最後一段違反第17條第4項所訂的辦法有關報告提出之內容，跟6項違反17條第4項規定法中有關通報內容，這是不是怪怪的，我昨晚有做筆記，一個17條第4項內容怎麼好像會在兩個裡面規定？另外還有一個，我要問一下副座，如果按照刑法電腦犯罪專章，他有刑度不太一樣，我看這個三條規範下來都是10萬到100萬，他的立法基礎是怎麼樣？都是10萬到100萬，如果是一樣的話會列在同一條，這樣列下來。

主席徐副處長：

你說罰的錢？

林宜隆教授：

對，三條，19、20、21。你如果要分開的款項應該是要有輕重，你又一樣又分在不同法條，沒有人這樣立法。

主席徐副處長：

所以老師的具體建議是什麼？

林宜隆教授：

第一個方式就是，應該要有層級啦，這三個哪個違反的比較重處罰就比較重，譬如50到100，再來是30到70，再來是10到50應該是這樣。如果你要一樣，第二個方式這三條應該並在一起。

再來我要幫民間業者說這個法律，好像是來處罰非公務機關，我已經繳稅了你還要來處罰我，這個國家應該是保護我們才對。你這次公務機關都沒有處罰，當然你會講公務機關都有相關規定了，這次為什麼非公務機關很害怕？有些銀行被處罰他還是可以得到CSA，就是公司治理，我有研究這三年被處罰最嚴重的，他居然還可以得到公司治理，就是公司治理最好的，這個很奇怪。因為是不同兩個單位做的，這個沒有意義。這次法律最怕的是這個處罰，因為資安產業不好賺，100萬算很多了，不像銀行比

較好賺，所以我剛才提案這兩個部分你回去看一下，第一個第19條第1項第5、6款有沒有重複的地方，第二個立法的基礎如果三條的罰例都要10萬到100萬那應該要併在一起。

第三個建議，如果不一樣，那應該要有個層級，這個層級是因為重大，當然你們要定義。我要補充剛才黃老師有講重大ISO 27035去年剛通過他就是ISIM，incident management，而且這個法條這次為了更清楚他把他翻成part4、part1、part3，定義都很清楚你可以看裡面，ISIM，大家都是專家，不用我們就看這裡面定義，來參考就可以，你不只要參考FISMA，那我也最後補充一些，我們今天這個法律，我們台灣把他當大國，所以我們參考的都是歐盟、FISMA，你不要生氣。因為我們法律專家都是留美留德，所以我們訂定法律是用大國觀念來看，所以什麼都要cover，這個沒辦法，我們參考FISMA，人家FISMA是美國在用的，你怎麼可能全抄，歐盟也不能全抄，所以我建議，參考他之後再把他narrow dwon，符合比例原則。

我建議，剛才有人提議2,000家我們不可能，現在是怎樣把他列入候選，那有個機制，他剛才同意，我剛才私底下。Risk分析不要從A跟VR，從T拜託一下，駭客已經講了我們國家投資資源都不對，已經不符合第一個原則，投在重要的上，法律是平定社會安定，但是它是有技術的。以上做第二次的補充，謝謝。

主席徐副處長：

好，不好意思，因為我們這個會議只到5點，我想要請還沒發言的老師。

林盈達教授：

剛剛聽吳老大的發言，他的聲音有恢復了，上次我聽你的聲音非常沙啞，所以我感到欣慰。不過我要建議吳老大，因為公部門普遍心態都很保守，它為什麼會變得保守，就是因為你一直罵他們，他們就越來越保守，因為做這個也被罵做那個也被罵，那乾脆都不做，所以就是說你可能要先讚美他們一下，不然好像一無是處，整部法都爛的，但不是嘛。

我先讚美一下，我有參加過稽核，一整天我感受到那個稽核是有用的，因為它看得很細，而且它不只那天其實它在那個禮拜，有三天的測試，已經有技術檢測的報告出來，然後再做一天的稽核，其實大大小小的問題

都已經看到，當然像ISO的東西基本上沒有涵蓋到這麼多，那樣的檢測是有效的。這部的法與後續的技術支援，capability可以到位，我比較關心的是capacity，也就是說因為這資安管理法，它的管理方式是階層式的，等於是說資安處和技服中心去稽核各個單位，可是被稽核單位是主管機關，也就是交通部下面的政府單位或關鍵基礎設施是由交通部去稽核，不是資安處，它不是star狀是一個hierarchy，這時候稽核員的教育訓練變得很重要。

剛剛吳老大講的是你要去估你到底有沒有這麼多人要去做這麼多事，我覺得是要去估稽核的人力，就是培訓稽核人力夠不夠，有沒有辦法做到這樣的hierarchy，當然另外一塊，被稽核的單位它的IT人員必須要有資安的訓練或專長，這部分當然沒辦法估計，被稽核的單位它當然要想辦法，不管是外包或找人進來做，本來資安就是一個成本，maybe它增加組織營運成本1%或2%，只要這個成本是合理的其實是OK的。你說人才到底夠不夠？資安處是要去估稽核人力，被稽核那邊很難去估這個東西，第二點就是有關於罰則或通報，我的想法是凡是會影響通報的，你要讓通報多，也就是你要讓未報有發生但沒通報的比例下降，當然就是會影響這個通報的你要把罰則去掉，不然你看不到通報。

另外第三個意見就是關鍵基礎設施，剛剛李忠憲教授提到德國的模式就是同步公布，我的建議是說，剛開始是一個short list但是你註明會逐年的更新，不是沒在list就沒事，它可能明年就會進那個list，所以這個list，因為你這個法一公布出去馬上就會被問這個東西，所以你乾脆就把它公布，但是一開始是一個short的list，以後逐年評估更新，進來的以後大概不會出去了，但是沒進來的以後可能會進來。

我最後一點，就是我去參加稽核後，資安處有寄出來那些被稽核的單位，我們去勾選，有幾個單位我覺得應該在第一波但是沒看到，有點失望。然後有些關鍵基礎設施的廠商，為什麼沒有在第一波。你既然關鍵基礎設施納在法裡面，有很多疑慮，那你就真的去稽核幾個關鍵基礎設施，那你得到了一些feedback以後，如果你要defend說其實你在中華電信看到了不少問題，那這個稽核是有效的，你要去defend這個就比較容易。以上，謝謝。

主席徐副處長：

林所長有沒有要特別發言的，我想說再聽聽其他意見，我們其實每年去挑選稽核單位都是有原則的，不是隨便亂挑的，這個我會後再跟老師做解釋。

林宗男所長:

我很快的補充幾點，在那個4月初的時候我們有和消基會合作，從消費者的觀點來看我國的資安環境，在那個調查裡面很多消費者，他其實會發現當它對一個公司的資訊設施有安全疑慮的時候，他是不會去那家公司做消費的，那很多消費者本身或親人面臨資安的威脅比例其實滿高的，消費者知道政府有意要健全我們資安的法規體制，他們的贊成比例是滿高的有80多%，從大方向而言政府制定資通安全法是正確的，那我們也支持，那對於一些民間公司，民間公司應該是要promote，要從消費者保護與公共利益的角度來encourge這個公司為什麼要投入資安的投資，那公司的IT與資安漏洞他可能會損害股東權益與消費者權益，所以公司應該像是上市櫃，政府會要求它做財報，財務資訊的揭露，同樣的我們應該也要promote這樣的觀念，因為資安它牽扯到不止是單純公司本身內部的information，它也牽涉到其他的顧客，所以應該要promote，公司它也應該要來主動disclose它在資安方面投入的防護做得多好，投入的資源做得多好，因為這樣子它會增加消費者對這家公司的信任感。不過我們要注意到這個資通安全管理法的方向是正確的，不過在一些實施的步驟裡面，可能要拿捏得好，來降低在立法過程中的阻力，謝謝。

主席徐副處長：

謝謝所長。我可以請廖主任先發言嗎？因為他還沒發言過，請廖主任。

廖志明主任：

各位先進，我只針對一條。第七條應該建立資通安全情資分享機制，我覺得這條一定要留住，因為即使其實是美國，美國國土安全局他們還有法律，去年他們就成立一個機制就是說，要求情資要分享而且要資訊化，所以他去年有個program叫AIS Automated Indicator Sharing，國內很多重要機構都必須要加入這個機制，所以他可以用情資來自動分享，情資分享不是只有Email或PDF而已，很多資料都已經格式化互相分享，分享資訊才可以做關聯做比對，我知道技服中心這裡也有在做，我覺得這東西是很

好的，而且這東西一定要標準化，標準化一種就是follow國外標準，而且follow國外標準我們國內可以互通情資，而且還可以跟國外互通，我覺得這是滿好的一件事情，報告完畢。

親民黨立法院黨團：

報告，我一定要補充一些意見。剛才那個廖主任，其實我們親民黨對第7條並沒有反對，我個人滿贊成李忠憲教授意見，可是你要先成立一個中央級或國家級的機構去做這件事情，但是你法條就定我們要訂一個分享機制，然後下面就沒有了，你的什麼程序指定的事項你都沒有，你覺得這樣的立法技術這麼的粗糙，你可以接受嗎？我不能接受，就算我只念過法學緒論而已，我並不是法律系畢業的學生，我覺得你立法技術這麼粗糙，你覺得你可以接受嗎？對不對？好，我這個人從來就不喜歡講什麼抽象，很空白的東西，我沒有指誰。剛才有位林教授談到說什麼消基會做一個調查，我想要問一件事情，如果這個調查前面加上「你知道如果成立資安法，行政機關可以不經過法院，就可以因為資通重大事件就做行政檢查，你還會同意這個資安法嗎？」我相信前面如果有加這段敘述的話，很多民眾他可能不是這麼的支持，我要強調一下，他那份問卷是有很多，對不起我是念政治學，我雖然不是專攻民意調查，他那份民意調查一定有很多的陷阱，我們都覺得要加上資通安全，這個立法沒問題，可是你如果告訴他這個法律不用透過法院正當程序，然後你可以直接依照所謂的資通重大的定義，你只要有資通重大的理由你就可以做行政檢查，你覺得民眾還會這麼支持嗎？我覺得這個是一定要反駁的。

第二個，我們都講我們要怎麼樣去做，我就舉這個行政院資安處提供給我們立法院預算中心的報告好了，我們專任與兼任的資安人員，中央加地方總共只有7,958名，這裡面7,958名還有1,296名也就是16.28%，是屬於勞務採購，簡單講就是勞務派遣，他就是用委託費用或業務費用去人力外包，他根本就不是專責人員，全國行政機關中央加地方專責人員只有600人，你想想看這600人他要資安通報，他要擬資安計畫，今天這個資安法過了他們要做這麼多事情，我們舉個很簡單的例子，你們定公立醫學中心是A級的，他們要2個專責人員，根據我自己不精確計算就有6個分屬不同部會的公立醫學中心，6個公立醫學中心就要乘以2等於12，請問這12個人他們是公務人員還是約聘僱人員還是所謂的人力外包，你可以告訴我嗎

？公務人員根本就不可能，你們為什麼不敢回答那位林教授講的，為什麼經費和人員無法成長，很簡單啊，主計處卡住你們，然後你們的總員額都是控制在銓敘部與人事行政總處的，你想要公務人員額不可能，你想要約聘僱，對不起，約聘僱名額也是被控制的，我們之前對於這種有關於人力外包的事情，都想要把他轉成正職，我們跟人事行政總處戰了這麼多年，都沒有一次成功過，你覺得過了這個法了之後就會有專職專責的行政人員嗎？那好，今天為了要達成這個法的所賦予各行政機關的業務，你們的方法是什麼？人力外包嘛，人力外包的資格怎麼去認定呢？適格廠商是什麼？所以我們說要什麼比較勞動檢查專法去立一個稽查專法，不是沒有道理的，而是考慮到很現實的問題，當你立了這個法，給行政機關這麼多的資安核心業務的時候，他的公務人員不能增加，他的約聘僱人員不能增加，他就只好人力外包了，那人力外包的話，可能用最低價標，那一年一標，總不可能用最有利標吧？你告訴我你不定一個專法去處理這些問題，很實際的問題，我講的問題都很實際，我從來就不喜歡講那些玄虛的東西，你們也沒辦法告訴我，你們保證那個法一定主計處會給你們錢，銓敘部會給你們人，對不對？所以我講得很實際，所以我們黨團沒有反對資訊資通安全法，但是我們主張的是行政機關資通安全法，然後要先建立一個國家級的資安中心之類的東西，不然你要任務編組也好，你要財團法人也好，你們就想辦法去生出來一個，我們不會去阻擋這個東西，因為我們也砍不過銓敘部和人事行政總部不給員額。所以anyway，我們的立場是很清楚的，我們都只講求實際上做得到的事情，我們不會去打高空，定了一些核心業務，然後你們要花錢委外去做這個事情，這個是我們不能接受的，謝謝。

主席徐副處長：

謝謝，陳助理研究員？好像有時代力量對不對？時代力量今天有來嗎？有，今天有來。國民黨沒有，民進黨也沒有。因為時間已經到了…

陳映竹助理研究員：

今天4場下來大家都是在講母法，那其實主席也說了要討論子法，現在有子法草案看不到子法內容，所以我比較希望就是說，針對子法的部分如果有這麼多需要考量的地方，是不是可以透過一個公開的途徑，讓大家提供意見，那再麻煩資安處這邊的人整理一下，讓大家可以把意見呈上來。那可以再提供比較具體的方向，不會這麼發散。

第二個建議就是，如果以民間的角度考量，我第一個比較擔心的就是今天法律這樣定了，那我要怎樣去配合你們，像資安事件通報，銀行事件就是跟金管會，也會請相關的人處理，但是如果像網站跟電商，他們在台灣的網路資安事件有非常大的比例，資安事件是從它們出來的，那個資外洩要找誰去協助他們處理？避免這個電商在日後可能要負擔的一些責任，他們有沒有一個明確的部會幫助他們？經濟部要找經濟部的誰？要找國貿局還是商業司還是找標準檢驗局？因為他們完全不曉得要去怎麼面臨這樣的事情。還有像是證照制度，台灣的證照制度真的很多，像是個人資料保護法出來之後，資策會這邊就有個TPIPAS的認證，但是我建議在法律裡面去明訂檢查員的資格，而不是他要有什麼證照，這樣子會更好一點。

主席徐副處長：

因為今天時間的關係，各位提的寶貴意見我們後續都會再做整理，做一些相關的討論。子法上能夠明訂的部分，我們會再做明確的規範，最後再次感謝各位，謝謝。