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10日（星期四）上午9時30分
地　　點：臺大醫院國際會議中心402A/B
出席領域：CI：能源、水資源、交通、緊急救援與醫院

【記錄開始】
主持人：
資通安全管理法子法草案正式開始，我們先請行政院資通安全處徐副處長為我們致詞，有請徐副處長。
主席徐副處長：
各位與會的來賓早安，非常歡迎各位能夠來我們這場次有關資通安全管理草案法的座談會，這次座談會的目的是希望能夠把我們送到立法院的資通安全管理法草案的版本各位想進一步了解的地方我們跟各位做一個說明。如果各位對現在草案的版本裡面有些可能後續需要進一步做明確的規範的地方，我們後續也可以納到子法上的訂定，作為子法的參考，這是我們今天會議的目的。
在今天之前必須跟各位說明一下，今天會議會有逐字稿，會記錄今天會議每個發言人的意見，這個逐字稿後續也有公開，這個在會議前跟各位做一個說明。
今天的議程首先會由我們同仁對資通安全管理法草案目前的進度還有各位比較關心的議題做一個簡報，簡報完之後就會開放給各位的提問，提問的時候就麻煩請各位報上你們單位的大名或個人的大名，之後比較好做記錄。我不知道這樣的程序與會的規定有沒有特別的意見或者需要調整的地方？沒有，如果沒有的話，我就請我們同仁先就資通安全管理法草案的簡報來跟各位做說明，請開始，謝謝。
賴分析師：
主席、各位與會的貴賓大家好，首先由我來為各位說明資通安全管理法草案的架構，這次的簡報內容跟去年、之前的內容都不太一樣，之前我們是針對條文的內容做一個介紹，我們這次會針對外界比較關心的議題，例如：行政檢查，也就是簡報中的資安檢查或者是一些罰則做一個說明，

我們另外有把其他類似歐盟或者國外一些相關的法做一個比較，我先做一個簡單的說明。

這個是我們的基礎大綱，請參閱。首先針對推動歷程做一個說明，整個資通安全管理法在104年7月到105年1月我們大概有找相關的政府機關、民間機關召開一個座談會，各位也有一些參與。105年8月資安處成立，我們在8月底的時候就調整完一版草案的條文，我們在去年9月到11月找政府機關、民間團體跟學者專家召開7場座談會。我們也為了整個條文的內容做一個檢視，在12月的時候在策略會議上把這個案子提出來，對一些與會的專家學者做一個解釋。在今年106年4月的時候完成了政委審查也提到院會，在4月28日函送立法院審議。在5月的時候已經由立法院交付司法及法制審查，目前是完成一讀的程序，我們會在下個會期今年的9月繼續請立法院協助我們審查。其實我們除了一些實體的座談會以外，我們在去年的9月22月到11月23日我們有在做一個平臺，就是國發會的公共政策網路參與平臺來公開這個母法，收集一些外界的聲音，這個是我們推動的歷程。

我們在推動的過程中，我們把一些各界的意見彙整在這個表上面，主要是針對政府機關、民間團體跟專家學者的部分，政府機關有反映不要因為立這個資通安全管理法造成一些比較瑣碎的行政流程還有一些相關的文書作業，因為現在機關都反應人力、錢也不夠，希望不要立這個法而造成機關的負擔。

在民間團體的部分，他們建議因為現在非公務機關有可能是中央事業主管機關稽核，還有一些可能被行政院稽核，他們建議稽核的時候不要造成重複的稽核。這個資安法各位手上的版本我們已經做了修調，第2點，目前規範對象除了公務機關跟特定的非公務機關之外，我們這邊講特定非公務機關就是「關鍵基礎設施提供者」、「公營事業」跟「政府捐助的財團法人」，目前的規範對象是這樣。可是在最初的版本不是這樣，之前版本其中有一個由中央目的事業主管機關指定的特定行業，例如他可以依照這個法去指定其他業者為規範對象，因為考量整個法案推動的機制之後，我們考量希望由政府機關、關鍵基礎設施提供者依序推動，我們按照外界的聲音把這個「指定」的部分拿掉，也不會造成這個法的不確定性。民間團體部分也提供建議我們這個資安管理法可以提供一個投資抵減的優惠，民間團體覺得這個罰則有點過重。學者可能有比較不一樣的聲音，當然學者專

家也有部分覺得這個罰則過重，但是大部分的學者專家認為這個罰則過輕了一點，這大概是我們推動過程中主要意見的蒐集。

接下來說明我們的架構跟內容，這個是資安管理法的架構，我們總共是環繞這五個圈圈，針對資通安全推動組織、非公務機關資通安全管理、資安整體環境與產業發展、公務機關資通安全管理以及資通服務之委外管理，我們最終目的就是為了維護國家安全以及社會公共利益。

周圍藍字的部分，原則上我們未來會朝訂定子法的方向去處理，我們現在已經有一個草案了，因為現在這個草案可能還不是很周延，目前沒有提供給大家，所以大家手上的版本是針對我們4月28日函送立法院的母法草案的條文，目前這個子法我們覺得還有一些討論、檢視的空間，相關子法的內容我們是放在附件，我們希望今天focus在母法，看看哪邊還有不足的地方。藍字的部分我們未來會朝訂定子法的方向去處理，大概有五個子法。

我們針對各國資安法規的義務內容做一個比較，主要是針對我國、美國、歐盟、新加坡做比較。義務類型大概分成：資安維護計畫、報告繳交、通報應變、稽核、資安檢查（行政檢查）、罰則，從這個表可以看得到，大概除了FISMA沒有針對行政檢查跟罰則做一個訂定之外，其他的歐盟、新加坡跟我們資安管理法的相關的義務類型是相當的相似。

進入第三個階段各界關心議題，我們有做一個彙整，針對規範對象、稽核、資安檢查、罰則我們做一些比較。第一個是針對規範對象，我們資安管理法目前規範對象除了公務機關之外，還有關鍵基礎設施提供者，這個場次就是關鍵基礎設施，各位未來有可能是關鍵基礎設施提供者，或者是公營事業還有政府捐助的財團法人，這邊政府捐助的財團法人原則上都是以中央政府或者是地方政府捐助的財團法人，大概補助資金比例達50%以上，原則上這個我們是參考財團法人法的內容去作訂定。

我們在推動的流程上希望立法三讀通過後半年後公務機關優先實行；再過半年CI提供者、關鍵基礎設施提供者；再過半年（第三個階段）是由政府捐助的財團法人適用。我們希望立法通過後2年，我會整個再做一個檢視，這個是我國的部分。在美國FISMA的部分，他的規範對象是聯邦政府，也就是他們的公務機關，FISMA的規範對象不包含非公務機關，但其他的州法會有一些相關規定，就從其相關規定。在歐盟NIS的部分，除了

規範公務機關，也規範CI提供者跟數位服務提供者，我們大概會比較像歐盟，會由公務機關優先，CI提供者跟數位提供者後續才生效，有優先順序。新加坡網安法跟我們資安管理法一樣，目前都還只是草案的階段，還沒有完成立法的程序，新加坡網安法草案規範對象除了公務機關，特別說明一下，新加坡網安法規範對象主要是針對關鍵資訊基礎設施提供者，並不是for全部的公務機關，公務機關如果是關鍵基礎設施提供者(註：這邊其實是關鍵資訊基礎設施提供者)才會納入，在非公務機關也是一樣，不管是公務機關還是非公務機關規範都一樣，是關鍵基礎設施提供者(註：同上，是指關鍵資訊基礎設施提供者。另關於簡報上提到的對資訊服務提供者或廠商的規範，主要以證照規範等為主，因此在此賴分析師未特別提及)，這個是規範對象的比較。

在稽核的部分，我們稽核內容主要是針對資通安全維護計畫，我們跟美國FISMA比較相近的。在歐盟的部分，稽核資安相關文件的措施；新加坡的網安法草案，稽核網路相關跟其他必要的事項。我這邊特別說明一下，美國FISMA的部分主要是由檢察總長(註：此處原文為inspector general，與台灣的檢察總長並不是一樣的職位)或第三方獨立稽核員來進行；歐盟NIS主要是由他的會員國自行去規定；新加坡是受指派的稽核員去辦理。

在資安檢查，特別說明一下，我們在啟動資安檢查其實有兩個要件，一個是當資通安全維護情形有重大缺失的時候、或者是有發現重大資安事件的時候，我們才會啟動行政檢查，目前這個行政檢查也是外界比較關注的，怕我們在執行行政檢查的時候把一些機構的基本資料或商業的營業秘密洩漏了，所以現在外界比較關心的是行政檢查。我國資安管理法行政檢查檢查內容就是與本法相關的資安維護相關的事務；美國FISMA沒有針對這個部分，因為美國只是針對他的公務機關，行政檢查主要是針對非公務機關；歐盟NIS的部分，檢查內容就是資安相關的文件跟措施；新加坡網安法，是檢查受影響的電腦狀況及相關資料。

罰則的部分，我們在資安管理法草案目前的版本，原則上我們是希望由輔助的方式去輔導非公務機關，立法的目的不是你不符相關規定我就罰你錢。目前針對罰則部分我們都有訂一個限期改正，除了兩點沒有限期改正就直接裁罰之外，我們都有做限期改正的規定。有哪兩點會直接裁罰？

第一個，知道資安事件發生，可是沒有通報，這個就直接裁罰；還有一個是拒絕行政檢查，這兩個我們就會直接裁罰，其他的我們都有訂期限改正的規定。原則上針對罰則的部分沒有依規定做好的話，大概是處以10到100萬的罰鍰，這個是非公務機關的部分；在公務機關人員的部分，當初資安管理法有針對公務機關人員如果沒有做到相關的規範訂相關的規定，我們在之前座談會、一些會議上，不管是人事總處或者是法制單位都建議，因為公務機關都有一些相關懲處的規定（公務人員懲戒法），所以可以從其規定，不需要在資安管理法針對公務機關人員懲處去做一個規範，不需要，所以各位手上可以看到，目前罰則都是針對非公務機關的部分；美國的部分沒有針對罰則做一個訂定；在歐盟NIS的部分，是請會員國自己去訂定有效罰則；新加坡的部分，稍微比較重一點，有期徒刑還有相關的罰金。

我做一個簡報到這邊，以上，謝謝。

主席徐副處長：

謝謝同仁的簡報，我這邊再補充幾點：第一個，其實各界非常關心規範的對象，我們資通安全管理法主要的規範對象就是關鍵基礎設施的提供者，廣義來說有八大類；另外也包含公務機關、國營事業、政府捐補助的財團法人，大概就是這三類。必須跟各位說明，跟個資法裡面的非公務機關其實是不一樣的，個資法裡面的非公務機關它的範圍是較我們現在的範圍還要更擴大，我們主要規範的範圍就是關鍵基礎設施的提供者、另外除了包含公務機關、就是公營事業、政府捐補助的財團法人，大概就是這三類。

剛剛同仁有特別強調，美國FISMA其實是針對公務機關，如果針對民營機構是算在不同法律去做歸管，他的法制結構跟我們不太一樣，也跟歐盟、新加坡都不太一樣，剛剛列出來這部分就給各位參考。

我們現在初步規劃資安管理法未來推動的期程部分，因為有不同的規範對象，所以大概會針對不同的規範對象會有不同適用的期程設計，假設立法通過之後會分階段施行，公務機關會先施行，接下來可能是關鍵基礎設施的提供者，接下來是剩下其他受管制的對象，大概有這樣期程上的推動。

我先補充到這邊，就開放各位來提問，等一下提問的方式我們先搜集

三個問題，三個問題之後我們再統問統答，以這樣的方式，看各位有沒有要提問的？麻煩遞一下麥克風。

臺灣中油大林煉油廠：

副處長、各位長官大家好，臺灣中油公司大林煉油廠提出一些問題：第一個，關鍵基礎設施包含兩個：一個是可能像金融、醫療；另外一個就是包含ICS的部分，也就是我們所說的工控系統，我們的意見就是在通報的部分我們比較不清楚，因為沒有通報要罰，這個是資安法寫得很清楚，但是通報要怎麼通報？我舉個例子，像2015年烏克蘭的事件，發生網路入侵的時候其實一開始並不知道，而且到事後調查出來， total virus上面也沒有病毒的名字，所以這是一個時機點。

像我們以前在工安部的通報很簡單，我們工廠只要發生異常，我們就通報。以前大林廠也做過所謂的網路攻防，那時候我記得技服對我們的要求是疑似當你發覺可能是資安事件的時候就通報。像現在這種情形通報要1個小時，如果真的確定，可能你的資安事件已經是很嚴重了，像Wanna Cry這種東西是很容易確定的，但是在ICS這部分，可能它沒有那麼容易確定，一開始我們都會把它當成是一個工安事件處理，所以我們的通報部分都會往工安的速報表去通報，等我們真正發覺可能是的時候，都已經下午了，甚至有可能隔1天、3天。

像那時候大林廠演練的時候，在技服中心的談論之下，可能到第三天，我們才被認為因為我們重開又出問題、重開又出問題，才知道這個可能是一個資安問題，所以通報的時機我們就不知道怎麼樣通報？「疑似」要不要通報？如果我們不確定的情形之下沒有通報，會不會被罰？這個是我的問題，謝謝。

主席徐副處長：

我們再來第二個問題，大家不要客氣，可以藉由這個機會來跟大家溝通一下你們過去可能不是太清楚的地方，剛剛中油提的問題可能單位比較關心，等一下再請我們同仁再做說明，有沒有其他的問題？

原子能委員會：

主席、各位先進大家好，原子能委員會想要詢問，關鍵基礎設施提供者是不是指國土辦已經列在名冊裡的都算？如果都算的話，是不是直接列為資安登記的A級機關？因為我們主管的意思，所有有關鍵基礎設施的提

供者它的資訊系統一定都很重要，都會被列到A級，是不是要檢視一下有這個必要？如果列到A級，應辦事項又很多，目前我不知道行政院會支援人力跟經費到什麼程度？因為以我們機關107年資安的經費，在公務預算的部分只有69萬，我們不知道怎麼去完成這些事情？如果我們機關自己去爭取，也爭取不到，因為每年框的錢就是那樣，不可能多出來、把機關所有的錢都放在資安，我不知道行政院可以資源到什麼程度？謝謝。

主席徐副處長：

有沒有第三個問題？如果沒有的話，我請我們同仁就這兩個問題簡單的回答。

臺灣中油大林廠：

有關ICS的部分也是工業界的部分，我們比較care的就是…像今年IThome2017資安論壇裡面，美國的專家，卡巴斯基的speaker自己也講，美國他們自己的系統很多的工控系統在NT的作業環境下繼續再跑，我們也老實講，雖然我們是中油，但是互相都認識，現在國內大概工控系統的主流作業系統是window7，還有很多的XP，也有NT，還有一些UNIX或是VMS一些比較特別的作業系統，未來我們來做防護計畫的時候，比較麻煩的是，這些東西剛剛有提出來，到底哪些是比較重要的？譬如像這邊分級也做過了，還有我們的系統要分「普、中、高」，像NT或是XP在「普」就達不到了，但是又是很重要的工控系統，但這其實不是只有臺灣在做，美國也跟我們一樣，我們在更新也不可能一次編個20億全部都換掉，像這種情況之下，我就不知道會不會有什麼罰則？以上報告。

主席徐副處長：

就請世榮先回答一下。

賴分析師：

首先針對中油剛剛提的有關通報的問題，請看到簡報第35頁，之前我們資安管理法有關資安事件通報的部分，配合簡報，各位可以看到資安管理法母法第17條第2項：「非公務機關在知悉資安事件時應向中央目的事業主管機關、直轄市縣市政府通報」。剛剛中油的代表有提問，如果他們不知道資安事件，遲遲沒有通報要不要被罰？這個其實在當初訂這個法的時候我們其實有想到，第17條第2項是講「知悉」，我們不是訂「發生資安事件要通報」，所以原則上你知道資安事件就要通報。

原則上不管是公務機關或非公務機關，只要知道資安事件就要通報，依照我們現在這個流程，各位可以看到簡報，這個在附件，雖然剛剛在簡報內容沒有講，因為今天是針對母法，既然有代表提問，我們就講一下，這個是非公務機關資安事件通報流程，當然這個流程還是草案的階段，我們這邊講「知悉資安事件」不是「發生資安事件」，當非公務機關你只要知道資安事件或者疑似資安事件，你就向你的主管機關或地方政府通報。

在目的事業主管機關或地方政府接到通報的時候，他會去判斷這個是不是屬於3級或者是4級資安事件，如果是3、4級的話，原則上就是我們講的重大資安事件，這個時候中央事業主管機關或地方政府在判斷是3、4級資安事件時，他在1個小時內就會通報行政院，行政院這邊就會視狀況看是否需要召開資安防護會議。在目的事業主管機關判斷這個是不是屬於3、4級資安事件，如果不是的話，他就會進行相關事件的審核，同時判斷這算不算是資安事件。這個部分以中油來說，你只要覺得疑似資安事件或是資安事件就通報，就沒問題，原則上後面的權責就是在目的事業主管機關的部分，我大概簡單說明。

第二個，有關原能會的部分，原能會提出目前國土辦有分A級、B級，A級有40幾個，B級有上百個，那些對象未來是不是關鍵基礎設施提供者？如果各位有細看母法的話，這個是回歸到母法的條文，由中央目的事業主管機關去判斷，國土辦提供的A級，因為那些有可能是電廠、橋梁設施、變電所，我們這邊講的關鍵基礎設施提供者像：核一廠、核二廠，這肯定都是關鍵基礎設施，它的提供者就是臺電公司，所以臺電公司未來應該肯定會被他的主管機關指定為關鍵基礎設施提供者，函報給行政院去做核定，這個時候臺電公司就是一個關鍵基礎設施提供者，原則上目前國土辦的A、B級那些應該都沒有錯，大致上都會是關鍵基礎設施提供者。

另外有關A、B級資安責任等級看到簡報第28頁，原能會有提到關鍵基礎設施這些會不會是A級呢？目前針對資安責任等級未來會訂相關的子法，A、B、C、D級我這邊也同時說明，這邊的C級就是現在的各位手上的C＋，這邊的D級就是現行規定的C級。剛剛原能會代表提到，關鍵基礎設施提供者未來會不會都是A級？這邊可以看到肯定都是A級，這邊A級有寫到：總統府、國安會、直屬前點之機關、五院的機關，例如：經濟部、交通部；直轄市政府，例如：臺北市政府、高雄市政府；公立醫學中心，例如：

臺大醫院；業務涉及外交、國防、國土安全等等關鍵基礎設施，這些都是列在A級，我這邊同時回答原能會的問題，原則上關鍵基礎設施提供者都會在A級。

至於錢不夠的問題，應該各機關錢不夠、人也不夠，所以我們現在透過資安管理法立法，要求公務機關一定要去做到一些相關資安維護要求事項，所以這也是我們立法的目的。至於經費的部分，就是回歸各機關的選擇，以上說明。

主席徐副處長：

我再補充幾點，剛剛中油特別提到通報的時機點問題，通報原則上是你知道這件事情發生的時候就通報，而不是發生事件時，因為發生有可能在更之前，所以這個部分跟你做一個釐清。

第二個，你剛剛有特別關心到，現在公共系統可能是比較舊版的OS，這個我可以同意、沒有問題，但是我想資安防護不是只是OS的問題，即使在這樣的情形下，你還是會通過種種其他的管理措施、技術面去做到一定的防護措施，而讓你在安全至少在一定的程度之上，我們只是希望你把資安的防護措施做好，而不是要資源去做無限上綱，因為有時候實際上你也不一定能夠做得到，所以這個部分先跟你做一和澄清。

有關原能會提到國土辦的部分，現在國土辦把關鍵基礎設施分八大類，是不是裡面規定的都是？我覺得不能畫上等號，國土辦也是從國土安全的角度在看；從資通安全的角度來看，我們會以這幾個大類為原則，但是還是會請各個目的事業主管機關就幾個原則性，譬如這個系統假設它因為服務中斷或者是有什麼樣的資安事件發生的時候，它所影響的範圍、程度來去訂它的責任等級，後續還是會朝這個方向去做，而不是所有全部納入，應該不至於這樣，還是會從它所發生的資安事件、影響的程度來去訂分級原則出來，這個部分跟各位做一個說明，這樣我不曉得有沒有回答到各位的問題，各位還有沒有再繼續提問的？

李忠憲教授：

副座、各位先進，我是成大教授李忠憲，我同時也是國網中心的副主任，在這個關鍵基礎設施上面我有幾個問題。第一個，管理法的座談會我已經參加3～5次了，每次針對罰則太重這個事情我都會提，基本上這個法立的非常有雄心壯志，可是我覺得執行起來可能會混亂。

德國在2015開始這樣做，沒有通報裁罰10萬歐元，但是執行1、2年下來，通報的次數10支手指頭可以數，因為大家不知道怎麼通報，不知道怎麼通報就已經立下罰則，我覺得這個不是非常合理。好像很多東西的是中央目的事業的主管機關來決定是不是3、4級，這樣執行的方式我不曉得每個中央的機關有沒有那樣的能力去判斷這個資安事件的層級？這樣互動的結果我相信會很淒慘，如果每一個電腦中毒就通報，這個東西如果沒有把它弄清楚的話，在施行細則裡面去訂立什麼是該通報的資安事件，這個可能會有很大的問題。

另外，這個關鍵基礎設施最後會不會給我們一個明確的名單，誰是在裡面、誰不是在裡面？而不是一樣由主管機關來核定，主管機關核定的話，也是又太過於信任這些相關事業主管機關他們資安的能力，以上一些小問題。

主席徐副處長：

請問還有沒有第二位要發言？

吳國維先生：

我不知道各位有沒有仔細看資訊安全管理的法律，聯繫到我們今天在談的關鍵基礎設施我覺得基本上有好幾個錯誤。第一個錯誤，我們大家都知道，我們在這部法裡面是把國土的關鍵基礎設施跟網路的關鍵基礎設施兩個混在一起談，這個其實是這個法裡面最關鍵性、最大的錯誤，我隨便舉一個例子，假設一個重要的橋梁關鍵基礎設施，那個橋梁斷掉跟中華民國網路會不會斷掉根本一點關係都沒有。甚至隨便舉一個例子，中油的確是一個關鍵基礎設施，但是他不是資訊的關鍵基礎設施，中油油庫被炸了，又怎麼樣？網路會斷掉嗎？當然我同意是國土的重要安全問題，但是不是資訊的關鍵安全問題。所以我想這個部分至少你在國外看到，是把兩個拆開來看，我們是混在一起談的，混在一起談的時候，你就會無限上綱把很多關鍵基礎設施都混在一起，應該把國土跟資訊的關鍵基礎設施兩個做一個區隔。

第二個部分，我們今天所在訂的不管A、B、C、D級，假設看其他國家所在用的文字，顯然跟我們這邊有很大的差異，不管是在美國、歐盟要求的compliance叫法遵，沒有你一定要做稽核，就好像所有做過ISO 27001的人都知道，臺灣有很多的OEM廠被國外的廠商要求一定要做相關的資訊

安全，但是沒有告訴你一定要做ISO 27001、不一定要做稽核，你只要提出你的資訊安全怎麼做，一本書就解決了，尤其在美國，基本上都不太會做ISO 27001認證這些事情。

所以在整個法案一直到今天講的關鍵基礎設施，你就要求做稽核，似乎把整個資訊安全、稽核、通報變成資訊安全最重要的問題，這是一個很大的錯誤，假設你去跟OECD所定義的關鍵基礎設施，在座多人根本無關，它只定義兩個，一個叫DNS，一個叫inertnet change，因為那個才是當它壞掉的時候會全面性的資訊產生問題。

去年大家最清楚的案例，在美國東部有一個公司叫DYN，他被攻擊，因為他是DNS operater，他被攻擊到的時候，在全美國找不到Amazon，那個才叫關鍵，我們現在訂很多關鍵坦白說跟資訊都不見得一定是必然的關係；通報也是一樣的問題，我相信在座資安處的相關同仁，都很善良說那個通報不一定要即時，你只要發現、真正知道的時候通報就可以了，我相信他是善良的，但是任何被規範到這個關鍵基礎設施的單位，試著想想看，真的這樣就解決了嗎？而且通報要通報到什麼樣的狀況？是很重要的資訊安全漏洞才要通報？還是隨便一臺電腦中毒就要通報？我舉一個最簡單的例子，假設真的大的病毒來的話，那個一泛濫是幾萬臺在中毒，全部都要通報嗎？還是你根本找一個根源就可以了？

你現在當然很善良去解釋，不會在這個部分給你課責，但是你不要忘了，你明明說在裡面告訴人家沒有通報要罰錢，這個邏輯有問題，你說假如盡責通報就不會怎麼樣，問題你的文字不是這樣寫的。任何一個公務機關或非公務機關碰到一個法律上這樣寫的時候，我只能用最嚴格的方式去理解它，所有律師做風險管控的人都會知道，我不可能設在那個平衡點，因為我不曉得那一條線在哪裡，你現在講的很簡單，這個部分我們不會罰你，誰知道？何況在那個法裡面，管的人不是只有資安處，中央目的事業主管機關跟縣市政府，你真的認為中央目的事業主管機關跟縣市政府有這個能力去判斷這條線到底在哪裡？每個人的線都不一樣，這個時候你就會製造困擾，特別我是一個關鍵基礎設施的operater，我最大的困難在哪裡？你現在說中央目的事業機關跟縣市政府都可以管，我可能頭上有好幾個老板，老板多到不知道怎麼處理，縣市政府也要報告、中央目的事業主管機關也要報告，所有跟我能夠牽連到都要報告，否則我可能就被罰。以中

油為例，中油幾乎全臺灣省幾乎都有，他要跟所有縣市政府報告、也要跟所有的目的事業主管機關報告，為什麼不能設一個專責機關？只一個單一窗口就好了，搞了一大堆窗口，所有被你拉進來，不管它叫A、B、C、D都是一個困擾。

我還必須回來最根本一個的問題，我認為稽核跟通報沒有辦法解決中華民國國家資訊安全的最重要的問題，因為臺灣真正網路資訊安全最重要的問題是網路的topology有問題，所有稽核跟通報只要做過網路安全都知道，網路安全必須要即時，等你稽核、通報，那個時效都已經過了，你只是後面大家創造數字給相關機關可以跟老板報告有業績，你看我們今年通報有多少個，除了創造業績，什麼都沒有發生，我坦白告訴你。

最糟糕的問題是你還要被罰，一般大家都會說要有蘿蔔跟棍子，請問你能不能告訴我蘿蔔在哪裡？我們被你列在A級，你有什麼蘿蔔給我？隨便舉一個簡單的例子，我今天碰到一個資訊安全攻擊，我打一個電話誰能夠救我？你們沒有人能救我，就是要來罰我而已，所以這個基本上有邏輯上的錯誤，我看不到蘿蔔，但是我看到棍子。

更重要的是，你沒有辦法解決真正中華民國資訊安全的根本問題，舉一個單一的例子，臺灣只有一個DNS，現在還有第二個的是Google在operation的8.8.8.8，我們現在又規定最好不要用Google的8.8.8.8，很簡單臺灣就只剩下一個DNS。請問這個DNS垮了，我們這些關鍵基礎設施每一個都是受害者，大家都跟你通報70次同樣一件事情，就是DNS垮掉了，我們的通報有意義嗎？因為你知道DNS全臺灣只有一個單一的單位在operation。

我雖然不是的關鍵基礎設施的operater，但是我覺得這個部法律不管是對公務機關或非公務機關，被你管到的真的是欲哭無淚，但是你又不能保證我發生事情你能夠會救我、幫我忙，我唯一擔心的是我不通報要被你罰款，試著想想看，到最後只剩下不通報會被你罰款而已。

稽核更是奇怪，假設我們現在設定的是真的那麼重要的關鍵基礎設施，你說要稽核，我剛剛說國外都是用compliance，翻譯就是「法遵」，我就是要你做到這些事情，但是我沒有要求你做稽核，甚至那個稽核可能內部稽核就夠了，你現在要第三方稽核。我不用那麼重的的話，但是有人說這個叫圖利廠商，因為臺灣只有幾家廠商能夠做稽核的工作，假設擴大去

，臺灣的稽核公司他的人力、能夠稽核幾家？我們自己都心裡清楚，假設今天臺灣有1000家做稽核，根本沒有足夠的稽核人員去做這件事情，就像李教授剛剛說的，那個叫畫大餅，搞的大家累得要死，稽核廠商賺死，講難聽一點，連要排他稽核時間都排不到。

我會高度建議不要用「稽核」，你可以要求「法遵」必須要做到哪些基本的要求。關鍵基礎設施應該要把國土的部分跟所謂資訊的部分做切割。比較重要的，我覺得資安實處應該回來認真看看臺灣資訊安全結構上最大的弱點在哪裡，而不是去干擾這些有的沒的，因為從我的角度來看，他們都不是最重要的關鍵基礎設施，OECD規定，就是DNS跟RX，DNS全臺灣只有一個，RX臺灣只有2、3個，你就把這些好好處好，必須要知道為什麼要關心DNS跟RX，因為我剛剛講過，一個DNS垮了就全垮，所有後面掛的「.tw」一起死。RX的問題在哪裡？因為我們不希望臺灣的資訊流通到國外去，但是我們RX一向做的不好，是我們最大的弱點，但是這個跟稽核、跟你今天的通報一點關係都沒有。所以我會高度建議資安處把力氣花在重要的點，而不是到處打擊，搞得大家雞飛狗跳，緊張死了，那個對臺灣的資訊安全沒有太大的幫助。

主席徐副處長：

謝謝吳顧問我們這麼多的建議，我想剛剛吳顧問的建議我們都是謹記在心，但是回應到剛剛李教授、吳顧問的一些問題，我想還是先就通報上的一些問題，譬如怎麼通報？什麼樣的層級要通報什麼程度？這個部分我們大概把現在的想法跟規劃跟各位先做一個報告。接下來，針對剛剛吳顧問特別針對國土跟資安如何做結合或切割，到底現在比較關鍵的問題，像是DNS、RX這些問題，到底稽核跟通報的責任應該如何看待？我等一下再做一個說明跟溝通，先請世榮把我們現在目前如何通報、什麼時候通報、通報給誰這樣的規劃，先跟各位做一個說明。

賴分析師：

大家看我們簡報附件33頁，目前我們針對資安事件的等級原則上分成4個等級，1、2、3、4級，有關3、4級主要是針對重大資安事件，雖然我們沒有把子法提供給大家，這個表會很清楚可以看到我們用什麼狀況分成4個等級。

我大概舉幾個例子，我們是以機密性、完整性、可用性作為分級的原

則，第1級，有關非核心資訊遭洩漏的話，原則上這個是在第1級，非核心資訊遭輕微程度的篡改，這個時候也是1級；2級的話，是核心業務資訊遭輕微篡改；什麼是3級，以這個要來看，是一般公務機密或者是敏感資訊，無論是篡改的嚴重程度與否，只要涉及一般公務機密或敏感資訊都是3級；什麼是4級，只要是涉及國家機密的，一律都是4級，有關關鍵基礎設施的部分，如果他無法在可容許的時間內回覆的話，這個也是4級，我們大概以資安事件先做一個區分，作為嚴重程度的判斷。

下一頁是針對公務機關的部分，我也簡單說明一下，我剛剛上一輪是針對非公務機關通報流程作一個說明，再就公務機關通報流程說明，原則上公務機關、非公務機關稍微有不一樣的差異，可是整體的流程大致相似，在公務機關的部分，一樣是公務機關知悉資安事件的時候，就要向他的上級或監督機關以及行政院通報；這個在非公務機關不一樣，非公務機關主要是向他的中央目的事業主管機關、地方政府通報。在公務機關除了還要他的上級或監督機關做通報之外，也要向行政院通報，這個部分是比較不一樣的差異。還有一個跟非公務機關不一樣的地方，在公務機關知悉資安事件的時候，要1個小時內來做通報；在非公務機關我們沒有這個規範。後面原則上我們針對事件等級的判定跟一些請求資源，這個是公務機關；非公務機關的部分剛剛我有做一個說明。

吳國維先生：

我舉一個最簡單的例子，以中油公司為例，他發生一個資安事件，你要他1個小時通報，我都懷疑他做得到嗎？因為他還要簽報他老板，尤其是越重要的，搞不好簽得越久，你以為一個電腦中心的同仁他敢通報嗎？我覺得你那個都是理想狀況，你試著想我是一個被你設定在A級的關鍵基礎設施，我要通報，我不要經過我的老板、資訊副總同意才通報嗎？我是一個科員，我敢通報嗎？這個公文的來往你認為1個小時走得完嗎？你就告訴我乾脆把錢準備好，讓你罰就好了，我坦白告訴你1個小時做不到！所以我才跟你說，假設你把罰則拿走，沒關係你就給我記一個警告好了，反正警告又不會死人，但是罰錢會有問題。所以你這種1個小時、4個小時都是你自己理想，自己想的，你從來沒有在operater的角度去想，他們怎麼辦？國網還比較簡單，他的層級沒有那麼多，中油去試試看，到副總才能夠通報，有多少層級、有多久的時間才會做得到？

賴分析師：

我這邊澄清一下，一小時這個是公務機關的部分，我們因為考量到整個通報應變目前都是針對公務機關，因為現在還沒有資安管理法立法的時候，我們現在其實有個通報應變綱要，公務機關依照我們通報應變綱做通報，所以我們這邊有規範，公務機關的部分是在1個小時內知道資安事件的時候，向他的上級監督機關或者行政院通報。在非公務機關的部分，我們沒有規範1小時內要去做通報，因為目前整個通報應變機制非公務機關或許都還不清楚，所以我們原則上針對公務機關的部分是要求1小時；非公務機關我們沒有要求1小時，我們原則上是知道資安事件的時候，向他的中央目的事業主管機關去做通報，以上說明。

主席徐副處長：

我這邊再補充一下，我們先談通報這件事情，還是回歸到為什麼要做通報這件事情，來去看它的目的性，如果它應該做、值得做，我們再看後續的程序怎麼去做設計，這個是原則性的問題。站在行政院的角度，為什麼要做通報這件事情？以我們公務機關因為已經行之有年，大概有這樣的通報層級來說，我想通報的目的第一個是為了做損害管制；第二個，如果需要協助，我們可以做適當的支援來去協助這些受害者、已經發生資安事件的這些非公務機關，目的應該是這樣。回到剛剛吳老師講的，如果真的我需要支援，怎麼辦？當然你就要往上通報，讓我們知道你需要支援，我們能夠調配什麼樣的資源去協助你，這是站在行政院的角度去看。損害的控制部分，假設今天中油駭客事件發生，他的很多的operation是停擺的，但是就整個國家的高度來說，他影響的範圍不是只有中油單一個entity，還有其他的entity、相關的一些基礎設施都會連帶受影響。所以這個部分在國土辦，現在很多關鍵基礎設施機關都是每年在演練的範圍裡面，應該都有類似的做法，我想應該是可以理解的。我想我再做一個這樣的補充，這是為什麼要做通報這件事情，站在行政院的立場，其實是這樣在看的，我先做一個說明。

接下來第二個，國土跟資安這件事情，國土裡面是分成八大類，其中有一類就是通訊，剛剛吳理事長特別提到DNS或者是RX，他可能後續都是可以在這個domain去做討論的，我覺得這個部分到時候如何去定義剛剛所特別關心那幾個domain的議題，我想後續我們再去定義每個關鍵基礎設施

的時候，可以跟一些中央目的事業主管機關，尤其是NCC來做思考，這個部分是我們目前可以做得到的。

另外是針對稽核，目前的資安管理法裡面規範的稽核，其實你必須提資通安全維護管理計畫，也就是剛剛所提到，目前其他規劃大部分是用compliance，你要提送一個文件化的東西，你到底要怎麼做？在法裡面也是希望不管是公務機關、關鍵基礎設施，都能夠提報自己的資通安全管理計畫。剛剛特別提到被外稽，那個其實是在資安責任等級裡面被規範的，像這個是子法的範圍，大概現在都還沒有定案，如果剛剛吳理事長的意見，如果真的不一定做稽核，反而要求應該做到哪些事情，他自己的計畫做好，我想後續我們可以把這樣的意見跟調整回歸到子法上資通安全責任等級去做一些調整，這個都是我們可以再去做參考的地方，以上做這樣的回應。

李忠憲教授：

其實通報這個東西做下來，結果會怎麼樣我們都可以預料得到，大家可以想這個法過，大家再來想我說的這些話有沒有道理。為什麼會有這些東西呢？是因為我們國家出了一個問題，我們沒有國家級的SAC跟SOC，Wanna Cry出現的時候，誰知道臺灣中華民國資安的狀況是怎麼樣，全臺灣沒有人知道，如果有國家級的SOC跟SAC，這些通報都到那邊去，這個部分就可以了解整個臺灣、整個資安的狀況，而不是用這些公文、通報、系統、用罰則的東西來做，這個是我個人一個淺見，如果要這樣推也是可以，不過我相信最後還是會回到國家級SAC跟SOC是不是有必要的問題。目前這麼多資安的經費這樣下來，如果要走這一套，是不是真的有效可行？這個值得資安處好好去思考一下，謝謝。

親民黨立法院黨團：

我覺得跟資安處講很痛苦，你們很喜歡答非所問，我是親民黨立法院黨團的助理，我真的覺得跟資安處講蠻痛苦的，你們很喜歡答非所問，也不針對問題回答，譬如說剛剛原能會說我們一年只有69萬可以做資安，剛剛這位賴分析師說：「我相信資安法過了以後，行政機關就會編錢。」如果真的是這樣的話，為什麼今年資安處要編35億的特別預算？去汰換所有中央和地方政府逾7年未汰換的電腦呢？你可以告訴我們嗎？你們為什麼不能針對現實來回答呢？我其實不曉得要哭還是笑。

剛才很多先進都已經講很清楚，你要有一個很清楚的上位概念，確定以後才能討論下面這些技術的問題，如果今天我們根本不要設立關鍵基礎設施在資安法裡面，我們討論稽核，有第三方稽核的必要嗎？沒有！難道你們對於自己的行政機關的資安不能透過行政處分或是行政裁量去要求嗎？或是制定行政機關本身整體的資安政策嗎？不需要啊！其實就是沒有錢、沒有人的問題，你應該要去找人事行政總處以及銓敘部算帳，跟他們要資訊長以及資訊的錢跟員額，而不是繞彎去立個法，來要錢、要人，而且要的錢可能不是正常公務預算，要的人可能也是編製內的員額，這是一個行政機關該做的事情？謝謝。

主席徐副處長：

我大概先回答一下，剛剛李教授說臺灣其實沒有SAC，臺灣現在很多政府機關裡面都有做SAC。

吳國維先生：

沒有國家級。

主席徐副處長：

因為我知道政府機關裡面有SAC，他們會往上通報到我們叫區域聯防的SAC，目前其實是技服中心在維運，是一個國家級的SAC，但是我想SAC跟事件這件事情其實是兩回事，SAC其實是如果你有一些事件就通報，你可能有一些事項就可以去做匯報跟分析；但是事件它必須是明確的，去確定它已經落在這4個等級裡面的部分，才叫做通報。

我想這個都回歸到原始點，要有國家這個SAC其實沒有問題，但是要有人通報給我們，我們現在有GSAC、也有GISAC，但是誰來把這些資訊給我們？讓我們從國家的層級裡面去看這件事情，其實也是我們要去考慮的地方，所以才會有假設現在的未來關鍵基礎設施或公務部門已經在做的事件通報，都是拉高到往上層級通報的做法上，能夠統一從國家角度來看，我想這個就是剛剛李老師所要提到的這件事情。

李忠憲教授：

現在又說事件是明確的，剛才那張表沒有一個事件是明確的，我昨天才去一個重要的機關做資安稽核，那個重要的機關核心業務通通沒有列入給我們稽核，因為你的核心、非核心機關自行決定，他最核心的業務就沒有列在那裡面，所以我昨天去那裡呆坐一天，我真的不曉得問什麼。

這張表如果能夠有什麼具體的東西，我不知道這個大家是不是可以認同？這個東西有什麼可以具體出來？什麼叫「輕微」？什麼叫做「嚴重」？什麼叫做「核心業務」？什麼是「非核心業務」？是誰定義？這些都沒有，那跟SAC有什麼不一樣？你要通報SAC那些軟性的東西，如果一個國家級的東西好好把那個部分做好，這個事情不就解決了嗎？你訂出一個不可以執行的法案，德國也有明例在那邊，卻要這樣去推，我覺得看到這個問題一定要講出來，如果這個法還是這樣過了，是不是會有我們之前講的這些問題？如果我有先講我就不會後悔，我大概這樣回應。

主席徐副處長：

我請我們同仁說明一下，其實核心業務跟非核心業務，既使是目前我們政府機關運作的方式，是有去把核心跟非核心業務定義出來，這部分就世榮我們目前的規劃說明一下，核心基本上我們現在有一個資訊系統的分級管理規定。

吳國維先生：

你所謂的核心業務是跟他們公司的核心業務？還是影響到中華民國的資訊安全的核心業務？這兩個是不一樣的，這個核心業務在我公司是很重要的，但是跟中華民國的資訊安全有什麼關係？到底你指的是哪一個核心？光在這張表裡面一大堆東西都是形容詞，假設我在一個被你規範的單位裡頭，不管是公務還是非公務，坦白說我都不曉得什麼叫輕微或嚴重。

我舉一個最簡單的例子，臺灣政府有真的把所謂的國家機務都classify嗎？我們有做到這麼清楚的classification嗎？有真的像美國這樣子，classify多嚴格，他清清楚楚知道你這個叫classify，是真的被定義在國家機密裡頭。其實我們自己很清楚，因為以前我在那個單位，我當副主任，我們那個classification根本沒有定義，在美國是非常清楚定義，人、事、物都定義出來，我們沒做，我們有定義一些人，但是光人我都覺得假設跟美國比，都做的不夠細。

所以你現在所訂的東西馬上今年9月那個法就要在立法院審了。我再講一個比較現實的問題，真的有多少立法委員搞得懂什麼叫做資通安全法嗎？坦白說不多，尤其你跟他一直講關鍵，假設那個立法委員沒有找專家去幫忙，他根本搞不清楚什麼叫「關鍵」，所以只有兩個可能，一個讓你過，一個不讓你過，因為他無從跟你去談這個東西。你自己開那麼多公聽

會都知道，真正知道的是誰？假如一過了以後，很多東西都是在一個模糊的線上，你又偏偏沒有一個專責單位，你是落在縣市政府、中央目的事業主管機關都可以開罰，不得了，我真的不知道，我基隆人，基隆市政府預算少的不得了，你真的認為基隆市的資訊處有能力去判斷什麼叫做核心嗎？他有能力去搜集這些通報嗎？你的預算有撥給他嗎？以他目前的預算跟人員的編製，你認為他做得到嗎？你只是把你的業務丟給別人，叫別人幫你蒐集，蒐集出來通通彙整到你這邊。

再講一個，我們今天的A、B、C、D級，跟你所有的通報稽核，沒有法你也在做了10幾年，從911做到現在，以前你沒有法也在做，我們大家也很認真的配合你，不是嗎？你還不滿意，要訂一個法，到時候告訴我們你要罰我。坦白說我很衰，還被你罰，以前我已經配合你10幾年了，沒有法也可以做，誰告訴你一定要通過法才能做你現在所要做的事情？你只是把過去10幾年來做的東西把它納在法裡頭，我們以前在配合的時候是活該的？表示我們過去沒有法律也都配合你，我們很後悔為什麼過去10幾年要配合你。

主席徐副處長：

我大概做一個說明，剛剛吳理事長提到，其實我們現在大部分以公務機關為主，公務機關現在是透過行政規則，但是關鍵基礎設施的部分其實目前並沒有；現在法裡面所規定的來做，這個是要說明的。

吳國維先生：

你們罰則寫得很嚴格。

主席徐副處長：

我剛剛只是回應理事長說的已經被規劃很多年，其實沒有，因為現在很多關鍵基礎設施沒有，現在是公務機關。剛剛親民黨黨團有特別提到支援的問題，我們同仁說透過法的規範，當然可以push機關去做必要的配置，是從這個角度，但是從內部實務面來看，我們過去也已經請政委召開會議，針對未來關鍵基礎設施，為了推動資安管理法，會配置相當的資安人力跟資源，這個是我們在內部的行政裡面已經有做這樣的事情，剛剛原能會所提的…

親民黨立法院黨團：

你自己去看資安法，這也許是一個巧合、命運的偶然，我真的不知道

，但是你自己看你立法的時程圖，前瞻計畫數位建設有關於資安這一塊所有經費、附件的施行，剛好是吻合的。我的問題很簡單，你這個特別預算過了以後，你又說這個法要設資安長，資安長是由副首長兼任，應該設置什麼必要的資安人員，你就不能針對我的問題回答我嗎？設這個法以後是不是可以強制公務預算編列多少錢給資安預算嗎？資安長由副首長兼任，他懂嗎？這個資安人員是外聘？還是你們員額裡面去支應？你可以告訴我嗎？你為什麼不能就事實來回答問題，你要講抽象空泛的，我人生很短，我沒有耐性去聽抽象的語言，謝謝。

主席徐副處長：

我來回應你的問題。

李忠憲教授：

這個我可以稍微反應一下，因為這個法我是跟著他來的，從第1條我開始看，我也寫了一篇文章，這是一部一個進步的法案，因為世界各國都是在往這個潮流做，這個也是國家重要的事情，所以基本上我是支持這個法。可是對於裡面的一些罰則，還有裡面的施行細則跟做法，基本上我是有一些意見，我那篇文章大家如果有興趣的話可以去找找看，這是一部進步的法案，裡面我也講一些事情，我們對這些東西重視的方法，不應該處罰的方式，因為我們還沒有到那個地步，這些明確的規範還沒有出來之前，先把罰則訂出來，我覺得這個法的爭議性會太大，本來是一件好事，因為它的一些瑕疵，讓這個法造成大家對它不是很容易接受。

像剛剛親民黨立法院黨團的先進說，這個法預算這些東西，那是政治的問題，我是學技術的，我跟著這個法從第1條開始，它的很多事情、規定這些來重視資安，我覺得是符合世界的潮流，因為全世界都在做，只是裡面有關於關鍵基礎設施方面，是採取以上對下、以罰則代替鼓勵，促進的方式，這個部分我是有意見的，我要稍微澄清一下。

主席徐副處長：

謝謝李老師，我還是回應一下有關親民黨黨團有關人力跟資源的部分，現在目前機關的資安長本來就已經有了，由副首長兼任，這個已經行之有年，我想資安長並不是需要懂到非常技術的部分，他一定是在一個leadership的角度去看，做資源調配的分配跟資源放在哪裡，一定是這樣，現在的部會首長他也不太可能對每個事實都了解，但是他是一個資源分

配。

吳國維先生：

他剛剛講這個真的是一個問題，我認為政府真的要重視資安，要設立，跟人事總處去談要設立資安長，那個要獨立出來的，不要用現在的副部長、次長、相關的主秘做這個資安長，講難聽一點，摸著良心，真的有效嗎？那些資安的副首長都只是出來開過會，有時候開過頭10分鐘他就走了，這個你自己都知道，你要認真去跟人事總處溝通，我們重視中華民國的資安，所以要給我們一個資安長的職缺。

主席徐副處長：

這個議題應該一直有被討論。

親民黨立法院黨團：

你講那個行之有年真的有效的話，你現在不會跟我們要特別預算35億，要去換逾7年未汰換的電腦，如果真的有效果，我這個很實際，我只看實際的效果，如果你的資安長像神一樣有用的話，你不需要去舉債35億，跟我們要汰換中央跟地方逾7年未汰換的電腦，冠上一個這是為了資通安全的計畫。

主席徐副處長：

我可以澄清一下嗎？我們現在的資安長其實是在行政院所屬各機關跟中央也有設資安長，你剛剛講的特別預算其實主要是處理地方政府的問題。

親民黨立法院黨團：

沒有，中央也有。

主席徐副處長：

中央的部分你講的主要是CIIP，關鍵基礎設施，為什麼要建這個？就是回到這個法，他們要建立ISAC。

親民黨立法院黨團：

你的預算書裡面有編中央也有編地方。

主席徐副處長：

對，你剛剛講的那個是地方，這個是可以確定的，這個是地方政府，尤其是在比較基層區公所的部分，這個沒有問題，因為計畫書畢竟是我們送的，所以我大概知道。

親民黨立法院黨團：

我的意思非常簡單，你連政府機關都做不好，你現在來要求民間，不覺得這個順序是錯的嗎？我首先要說我們沒有反對要立資通安全法，我們親民黨目前可能的方向以及立場，僅限於適用中央（包含政府機關等公法人），我們不希望馬上跨到關鍵基礎設施或者是民間，我現在說明我們版本可能的立場跟方向。

我要特別強調一件事情，我不太喜歡作文比賽，我真的很討厭作文比賽，尤其討厭聽到講話作文比賽，你告訴我這個法要用什麼方法去達成你的目的？你的員額哪邊來？經費哪邊來？你要告訴我們這些事情，不要告訴我法過了，全部事情都好了。

主席徐副處長：

當然沒有全部事情都好。

親民黨立法院黨團：

問題是原能會那69萬問題很顯然你們就沒有辦法解決。

主席徐副處長：

我必須要澄清一下，其實原能會剛剛講的部分，核能電廠上面的主管機關應該是向上彙到經濟部，而不是原能會。

親民黨立法院黨團：

我舉另外一個很簡單的問題，按照你們的分級，公立醫學中心是屬於A級，我剛剛查一下，目前我們的醫學當中大概有5到6家是屬於公立的，我問一個很簡單的問題，如果真的發生你們所謂的資安事件時，他要跟誰通報？是地方政府通報？還是跟衛福部通報？衛福部負責資訊處的那位長官我也認識，你認為公立醫學中心發生這樣的資安事情他要跟誰通報？誰有能力處理？而且就公立醫學中心哪些東西應該要包含在你們資安保護的範圍之內？

主席徐副處長：

他的通報，如果他是屬於…

親民黨立法院黨團：

我希望聽到實質回答問題的內容，我們今天講的所有問題，應該是在立這個法之前開的公聽會就應該要討論到。

主席徐副處長：

對，如果是醫院的話，他是部立醫院基本上一定會向衛福部通報，這是一定的。

親民黨立法院黨團：

部立醫院按照你們分級是公立區域醫院，因為你們部立醫院他還沒有到醫學中心的層級，你連你們自己子法的內容都不太清楚，你還要來跟我們說明這些東西，這不是很奇怪嗎？

賴分析師：

部立醫院是公務機關。

親民黨立法院黨團：

這就是問題之所在，因為你們自己A級裡面又分公立醫學中心，請問一下部立醫院到底是屬於公家機關還是什麼？因為有些部立醫院根本是在偏鄉，他的經費也少的可憐，從你們自己的回答就發現你們認知就完全不協調，你可以告訴我…你B級又列一個公立區域醫院，通常部立醫院依照它的等級而言，通常是屬於公立區域醫院的等級，因為它的能力並沒有到醫學中心，你要到達什麼樣的層級必須要經過衛福部的評鑑，你們自己要不要先調和自己認知的矛盾？謝謝。

主席徐副處長：

我們剛剛說的部立醫院…

親民黨立法院黨團：

你們公立醫院是依照醫院本身的層級去區分的，不是因為他是公務機關，如果照你們這樣的說法，你們根本不需要區分公立區域醫院這個東西，因為沒有公立區域醫院這種東西。

主席徐副處長：

區域醫院是說，其實他服務的是區域的性質。

親民黨立法院黨團：

但是前面寫「公立」。

主席徐副處長：

他是「公立」就屬於B級。

親民黨立法院黨團：

所以你連衛福部方面的專業都搞不清楚，因為區域醫院或是醫學中心是以醫院的規模大小以及能夠提供醫事服務的科別去區分的，醫學中心是

完整的，什麼科都必須要具備，才會叫醫學中心，而且醫學中心是有限量的；區域醫院可能只要有幾科，不需要每一科都有，如果你們認為只要衛福部的部立醫院都屬於公立機關的話，根本不需要有公立區域醫院這個東西，你可以舉一個公立區域醫院的例子給我看嗎？

主席徐副處長：

我了解你的意思，你剛剛是說部立的醫院要向誰通報。

親民黨立法院黨團：

沒有，我從來沒有說部立醫院，部立醫院都是你們提的，我一開始就是說公立醫學中心。

主席徐副處長：

回到醫院的話，就是按照現在目前的規劃，這只是暫時的規劃，因為現在這個是在子法的裡面細節，其實都可以還有討論的空間。

親民黨立法院黨團：

所以我建議接下來的會議都應該把子法拿出來，因為你一直拿抽象的原則大家來討論，其實沒有任何實質的意義。

主席徐副處長：

如果親民黨委員覺得可以，我們直接把子法拿出來，那沒有問題。

親民黨立法院黨團：

我從來都主張把子法拿出來討論。

主席徐副處長：

我覺得這樣很好，現在大家比較關心的，母法其實是一個原則性的規範，但是子法怎麼去做，是可以做一些共通性的討論獲得共識。

親民黨立法院黨團：

禁止討論子法是國民黨團說的，不是親民黨團，我們要強調的聲明這件事情。

主席徐副處長：

如果這句話可以讓我們進一步做下去的空間，我們非常歡迎討論。我不知道剛剛有沒有哪些問題是還需要再做說明的，我必須說原能會自己的預算，他講的是資訊系統內的維護預算，但是就核能這件事情他的主管機關是經濟部，這個部分必須先做說明。

吳國維先生：

我建議聽聽真正被設定在關鍵基礎設施這些單位的他們意見，我想我們這邊閉嘴好了。

國泰醫院：

各位先進好，剛剛親民黨團有講到醫院，我是醫院的代表，目前沒列在上面，我也蠻擔心未來列在上面的時候。公立醫學中心列為A級，以臺大醫院來說，他的核心業務應該是醫療服務，在去年5月5日如果發生一個當機事件，他的核心業務算不算影響資訊安全？如果算是的話，他要向誰通報？應該是社會媒體播出來之後，我們才知道臺大醫院當機，如果這個之後影響到私人醫療也要納入的話，我想做資訊管理委員這個位置應該常常會換人，因為只要一罰則下來，按我這個位置可能就要換另外一個人來當。剛剛又講到核心跟非核心，所謂核心是不是影響資訊安全？還是他的核心是因為他不能提供服務造成他這樣子？以上。

主席徐副處長：

我不知道還有沒有其他要發言的？

中華電信：

主席、中華電信這邊第一次請教，翻到第33頁，我的問題其實跟剛剛國泰醫院有點像，我第一次看到這個表的時候，以中華電信來說，我們會對應到關鍵基礎設施的業務，但是大家都知道中華電信非常的龐大，所以回到吳老大講的，到底這些關鍵基礎設施裡面哪些是屬於我們公司critical，整個國家安全有關的？或者他只是支援業務？

以這張例子來說，標的受影響於容忍時間回覆與否，看到關鍵基礎設施第3、4級都在這裡面，譬如我們遇到颱風、天災，以目前NCC定義的關鍵基礎設施標準，只要影響1000人我們就是關鍵基礎設施，所以有時候看到的行動推車，現在也變成是關鍵基礎設施，假設我今天一個基地臺因為天災的關係，不能夠服務，其實我們本來就有一定的障礙搶修的機制，這樣到底算不算資安事件？該怎麼通報？變成我們無所適從，尤其是目前在關鍵基礎設施業務，這個真的是很大的term，不管是分級的定義，也許在行政院或是在主管機關的定義都不太一樣，非核心業務跟核心業務，我們現在也不曉得以我們非公務機關來說，到底要怎麼去mapping。目前所訂分級的規定或者事件等級的分級，比較像原來政府公務機關的這一套方法，再套到我們非公務機關的身上，我覺得現在這個部分我們會有點無所適

從。

再舉例來說，剛剛前面很多先進有提到，NCC現在也有要求我們電信業者必須要通過ISO 27001，現在導入ISMS制度其實也都也所謂的風險評鑑，可是我們可以看到，現在在國土辦針對風險評鑑的方式，跟我們一般在做ISMS風險評鑑方式，甚至我不知道未來如果行政院這邊要稽核，會不會又有一套風險評鑑方式？因為我們一般在定義非核心業務或核心業務，這些其實都跟風險評鑑方法論有關，當我們國家沒有一套一致的標準的時候，我覺得就會變成是各說各話，以上是提出來請教的部分。

主席徐副處長：

我先大概簡單回答，剛剛中華電信跟國泰醫院提的問題，回到一個關鍵問題，到底要怎麼去認定核心業務跟非核心業務，至少目前按照我們資安事件的等級是這樣去分。以目前的規劃想法，資通安全是從CIA這三個層面去看，可用性、機密性、完整性。其實目前的風險評鑑方式，是從這三個面向去評估這個資訊系統，假設你被評估出來風險等級有一個是高的，它就是你的核心業務，目前我們規劃做法是這樣，但是這個做法都可以討論，這個會回歸到資通安全責任等級子法的內容，我們先提出來初步的看法是這樣，所以未來你們就是用這樣的方式去評估。

我必須特別強調，我不曉得NCC或者是衛福部現在有沒有對於資安事件的認定有一個範圍，但是未來在法的施行之後，一定會一致、一套的，不會有不同的，這個就是我們要努力的方向，我是不知道個資法講不同套是什麼意思，但是這個法既然要做，一定主管機關跟行政院這邊有一個共識，到底什麼樣的東西是要被放在管理的範圍，這個部分大家應該可以不用那麼擔心，這個我可以跟各位做一個保證，這樣可以回答到各位比較擔心的問題。

剛剛提的問題都是子法，這個只是暫定的內容，其實也是透過今天的會議，來聽聽各位的意見，未來我們怎麼讓子法裡面，譬如核心、非核心的業務更明確，來去做一個表示，這個是我們後續可以再強化的地方。還有沒有問題？NCC。

國家通訊傳播委員會：

主席、各位先進大家好，國家通訊傳播委員會第一次發言，首先我們肯認行政院資通安全處就資通安全管理法這樣一個立法，我相信也會提升

我們公務機關、CI提供者、公營事業、政府捐助財團法人資通安全措施的提升，有助於我們整體國家資通安全的能量的建立。

只是剛好在今天行政院資通安全處這邊的先進有針對各界關心議題裡面整理了國內外的一些立法，也提出了像歐盟、新加坡，他們在非公務管除了CI提供者以外，也把數位服務提供者或者是資安服務提供者或者是資安服務的廠商列進去有所規範，我覺得這一點在我們將來如果這次的法還沒有納進去的時候，未來可能有機會再進一步思索。

我會這樣提的理由是，剛才中油的先進有提到他的ICS，一般來說資通安全的維護除了各機關自己人為管控以外，在天然災害是必要的防護，再來就是產品的瑕疵，就像剛剛中油的先進所說，所有ICS的系統裡面目前所用大部分主流都是windows7、windowsXP或者Linux、unix，這一些的OS好像都不會是我們目前這些公務機關、非公務機關所規範對象，這些單位自行開發的產品，這些產品如果有風險，我們可能只能在發生資安事件之後才會去提報，等於是事後提報，我這個單位目前有發生這樣的資安事件，但是如果從預防跟聯防的效果來看的話，應該是從產品的提供者他最清楚，例如微軟公司，他在全世界有哪一個國家用了他的產品之後有產生了怎樣的資安風險，他如果第一時間掌握之後，第一時間也跟我們國內的機關提報之後這個windows的型號，目前在國內有提供哪些用戶，這個產品在國外已經發生了資安風險，他能夠讓我們第一時間掌握，或許我們就可以用聯防的效果，通過ISAC來分享給所有相關單位，也避免再產生資安事件這樣的維護。

所以我想為什麼歐盟或新加坡會把數位服務提供者跟資安服務提供者納進去做一些規定？是不是有這樣的考量？我不知道，因為剛好中油這樣一個分享，是不是我們將來在對象方面，對於核心產品的軟體公司是不是要一併納進去作為我們規範對象？或許可以思考，這個是第一個建議。

第二個，回應剛才中華電信公司所提的議題，目前NCC在通訊傳播的設施裡面，就電信業者有1000人以上，那個是規範在行動通訊領域，一般民眾當他有無法通訊的時候，我想1000人以上已經是一個可能是需要掌握的資訊，所以我們要求有設施災害發生的時候，這個是屬於災害通報的範圍，這不是屬於資安事件。資安事件我們在國土辦有CIP跟現在資通安全的CIIP，關鍵基礎設施國土辦有針對我們CIP的部分有要求，因為我們目

前有1000多的設施被規劃為CIP，這樣的量真的蠻多的，而且專家學者是在行政院開會，有要求我們NCC就CIP類別再做進一步檢討。

我回應吳國維先進，你提到IXP的部分，網際網路的交換設施部分，目前有列到關鍵基礎設施，DNS部分我們也列進去，而且今年年初NCC已經針對國內所有DNS重要的提供者也辦了演練，所以這兩個部分我們目前都有在關切。

最後，未來我們還是會針對行政院的資通安全管理法通過之後，對於CI的業主這些設施，我們會依照這樣通過的條文來落實執行，以上補充報告，謝謝。

主席徐副處長：

這個問題我就先不用做回應，不過剛剛NCC提到歐盟有把其他的業者納進去，現在的資安法是不納，不過資訊相關業者非常多種，譬如你就是一個網站、店商，目前其實都不在這個法規的範圍裡面，這個必須先說明的。我們政府目前有一個叫GISAC的機制，就是做一個資安、資訊分享的平臺，以資安處來說，我們是這個平臺的主政，不過我們連結非常多，包含微軟、趨勢，很多家公司他們如果有一些資安訊息，分享的時候，目前都是透過這個平臺做資訊交換，有加入這個會員的平臺，我們也可以把這些公司給我們的資訊即時提供給會員，目前這種的資安資訊的即時分享機制，已經在實行了，這個可以跟各位做一個報告，剛剛的回應的部分我想就不用做一個說明。接下來有沒有特別要提問的？

陳映竹助理研究員：

我是臺經院陳映竹，整個聽下來，大概可以明瞭，因為科技跟攻擊方法會改變，所以不確定定義出什麼叫關鍵基礎設施，避免日後常常有修法的必要，但是以現在的文化來說，如果不明確的話，可能會造成所有操作電腦的人的困擾，這個部分可能還是要請長官考量一下。

第二個，剛剛提到要請各部會自己提供自己的資安管理計畫，就我之前接觸open data的經驗，很多單位不會寫這個東西，變成哪個部會的版本經過了，大家就跟著抄，這樣的實際效益在哪裡？

第三個，不管在前瞻或是數位國家裡面，都有提到要把各部會的資訊單位人員重要性、責任還有他們的位階提高，還有每個單位人員的資訊安全教育訓練都加強，但是要怎麼讓每個人都有維護資訊安全的意識？這個

東西要怎麼去衡量？最矛盾的地方就是，在我們還沒有規劃整體意識的教育情況下，我們就先訂罰則，會造成相關的人覺得，與其會犯錯，我乾脆就不做，這樣反而造成整個資訊產業沒有辦法好好的發展，甚至造成在行政流程上面有更多的阻礙在裡頭。

最後一點，在第1條有講到促進資安產業的發展，但是我們都沒有看到怎麼發展？目的是什麼？方法是什麼？衡量的KPI是什麼？這個部分都沒有提到，唯一我剛才看到比較類似的的是GISAC，提供給會員跟分享的機制，這個就是所謂資安產業的發展嗎？或者是有其他的政策規劃在裡面？目前我是沒有看到的。

主席徐副處長：

謝謝，還有要發言的嗎？

高雄捷運公司：

謝謝，高雄捷運公司資訊室這邊有兩點建議，因為剛剛也聽大家提到，怎麼去規範責任等級？以我們公司的做法，我們自己會先去研究，自己應該哪些會納到核心系統，自己做這樣的研擬，我們也相信沒有任何一個單位可以那麼明確定義，有哪一個東西應該規範在哪一個資安等級。在管理法中，我們在講的ISO、PDCA，在子法中或規範裡面是不是可以納入這樣的流程，讓大家自己來提報，有哪些要納管的，透過PDCA的方式來做改善、不足的地方再做補充，這是第一個。

接下來有兩項建議，因為在資通安全管理系統的建置規範裡面，我們是關鍵基礎營運單位，基本上我們營運的設施是由公務機關所發包的系統，我們接手來做營運，但是在這樣的發包建置的時候，是不是建議把政府的公共工程採購規範把資通安全所要求的系統建置要求予以納入，以避免當初建置沒有這樣的要求，日後要變更或者是要做改善，會造成關鍵基礎設施營運單位會有困難，這是第一個。

第二個，因應目前已經有這樣的系統建置，包括我們系統建置現行的條件，譬如剛剛大家有提到，國內各個單位對系統技術的掌握程度可能不一樣，因為這些系統都是從國外來的，或是引用國外的作業系統，所以要我們這些營運單位去克服這些的狀況會有困難，而且有區域間的關係，剛剛所提的公務機關建置、關鍵基礎設施提供者來做營運，這樣來訂罰則或者其他系統變更的事情，是不是在以後的子法跟作業規定裡面能做一些有

彈性、可行的要求？而不是由營運單位沒有辦法做變更的情況之下，就進行處罰，這個是我們這邊的建議。

主席徐副處長：

你剛剛說有什麼營運單位被處罰？可不可以再說明？

高雄捷運公司：

剛剛有特別提到，目前罰則主要是針對非公務機關，也就是這些關鍵基礎設施的營運業者，他沒有通報或者是系統發生事故，沒有做改善，我們害怕這樣就會被處罰，但是這個系統建置又不是我們建置，我們只有營運的操作管理作為。人工的管理作為或者人工的維護措施，我們都很樂意努力做到好，但是要變更這個由國外進來的系統或者由公務機關所建置的系統，我們很難去做任何的改變，譬如我們在責任分級作業規定，A級作業規定就要做APT攻擊的防護，要做SAC的防護，對我們捷運系統的機電系統，根本難以達到，而且一般在談這個都是在講資訊系統，所以會有這樣的系統條件…也就是說，國內各單位對所有系統技術掌握程度、能力的問題，所以有這種契約狀況或者是系統掌握程度條件不一致的情形，是不是在以後的子法或作業規定裡面，能夠增加比較彈性可行的管理辦理。

主席徐副處長：

謝謝，我大概簡單的回應一下，我說明一下臺經院特別提到，關鍵基礎設施在母法不明確，沒有把每一個關鍵基礎設施訂出來，因為它是一個法，法的部分也沒有辦法現在就說誰是誰，關鍵基礎設施明列出來，我想這是在設計上的限制，所以我們在法裡面做法是，後續當然會有中央目的事業主管機關或者他的主管機關來做指定，大概是這樣的做法。但是訂定的過程中，關鍵基礎設施一定會目的事業主管機關做溝通或者是取得共識上的認定，一定會這樣做的，這邊我大概先做這樣的回應。

第二個，有關自己寫的資通安全管理計畫如何去落實？訂不訂跟能不能落實是兩回事，如何去訂跟如何去落實？這個部分我們有一個子法，叫資通安全維護施行細則的管理辦法裡面，裡面有說大概計畫內容要訂寫什麼東西、之後怎麼去做落實，這個在子法裡面會去做規範，大概先做這樣的說明。

另外一個有提到，人員的部分，我們在公務機關裡面，在座如果是公務人員就知道，除了資訊人員以外的公務人員，我們平常是要做社交工程

演練，目的就是在提高一般公務人員的資安意識。不管是人事行政總處或者是國發會，包含我們資安處，通常在不定時就會對我們國內的公務人員做資安的教育訓練，這個教育訓練也包含很多線上教育素材，其實是可以讓公務人員上網去看，所以一般公務人員的資安意識本來就一直有逐步在做的，這個是我要先說明的。

接下來是有關促進產業的發展，剛剛特別提到KPI如何指定，因為這個法，不是在講計畫或者你如何做、KPI如何訂，通常法裡面不會訂KPI。但是我必須跟各位講一下，資通安全管理法因為有一些對公務機關或關鍵基礎設施有一些要求，甚至會促進一些研究或技術的發展，產業面應該有供應端去支持它，所以當然會也一些促進產業的發展可以出來，這是第一個。第二個，不在這個法裡面，我們有一個國家資通安全發展方案，其實每4年就會訂一次，每次訂的方向，以今年來說，其中有一個就叫做資安產業的發展，那是由經濟部主政，裡面的內容包含技術的研發、人才的培育、實驗場域的提供、新創公司的成立，其實在那個計畫都是有的，這個部分我做一個說明。

剛剛高雄捷運公司裡面有特別提到，因為你們畢竟是BOT的單位，可能有些不是你們可以掌控的範圍，這個部分我們後續再看資安責任等級的定義，你剛剛有一些建議，我們都可以納入參考，沒有問題，這個部分可以做一個比較深入的思考，我先回應到這邊。

吳國維先生：

我做幾個比較具體的建議，我會建議資安處，關鍵基礎設施必須要把CIP跟CIIP兩個切割做討論，因為兩個東西的維護或者是相關的東西做法都不一樣，你把它混在一起，變成兩邊都要做額外的，CIP也要去做CIIP的東西，CIIP也要去做CIP的東西，這個其實是不必要的，因為我們很清楚有時候CIP根本不是真正的資訊關鍵基礎設施，他的關鍵不是在網路或是資訊系統。所以你把它混在一起，變成用一個大帽子去蓋住所有的人，我覺得這個是資源上的浪費，我們沒有人不知道方便跟安全是一個衝突的問題，這個是抉擇的問題。你為了要把CIP跟CIIP納管，結果只好用一個非常大的帽子蓋死所有的人，真的坦白跟你說，你要認真去思考CIP跟CIIP分割來談，國安會自己都知道這個問題，你們今天還要把這兩個扯在一起，只是給自己找麻煩，這個是第一個部分，你應該把CIP跟CIIP做切

割來處理，看怎麼樣去定義、去解決這個問題。

另外一個，我具體建議把罰則拿走，我舉一個最簡單的例子，所有operation資訊系統的人，他認為他喜歡被入侵了嗎？沒有人願意，入侵真的是他的問題嗎？不是，假設資安處很願意負責任，我倒是高度建議資安處跟微軟講，以後入侵我就罰微軟100萬，而不要罰他們，就罰微軟，你有能力叫微軟不要有漏洞嗎？都是微軟造成的，那個系統都不是臺灣人自己做，你為什麼不敢大膽跟微軟說你的系統很爛？

主席徐副處長：

我提一個問題，我們做意見交換，我同意每個系統都有它的漏洞，假設今天微軟有漏洞，他發布一個了更新patch程式，不管公務機關或關鍵基礎設施它沒有更新，那還要罰微軟嗎？

吳國維先生：

他的patch都是在事後。

主席徐副處長：

對，沒錯。

吳國維先生：

那我已經被入侵了，那個根源你沒有辦法解決，所以我才說你不要用罰則，鼓勵大家來做，這個我可以接受、可以同意，我也原則上同意李教授剛剛所說。做這個法本身不是壞事，但是你把它搞成是壞事，不管在美國或歐盟做complies，除了德國很特別，幾乎都沒有罰款，在中華人民共和國有，我們是跟中華人民共和國站在一起的，因為我們用罰款，很多國家網路安全法都不罰的，因為他知道做不到沒有問題，所以我只能去鼓勵大家做。政府要把資源集中在做有效的事情，我們不是把它放在比較末端的通報、稽核，這個反而是末端的，通報稽核那個都事後。

我舉一個最簡單的例子，我剛剛說去年1月份在美國東部DYN被攻擊，那個垮得多慘，多少網站都垮掉，那個DNS垮掉，你有看到美國政府罰DYN嗎？你有看到美國政府去罰他嗎？沒有，DYN還因為被攻擊了以後，市值還上漲，後來被Oracle還把它買走，在我們今天被罰的時候，我們本來是受害者，中華民國政府再來加害我們，這個很奇怪的。

主席徐副處長：

如果以DYN的例子，在我們現在法裡面，他也不會被罰。

吳國維先生：

你知道他有通報嗎？

主席徐副處長：

我們現在規定是你知悉的時候。

吳國維先生：

現在是沒有通報就要被你罰，你自己看法律第17～20條那4條，你是怎麼罰的？用什麼罰？

主席徐嘉臨副處長：

你知悉這件事情的時候要通報沒錯，但是我們沒有說他被攻擊就要罰，我們法律裡面也沒有這樣規定。

吳國維先生：

所以我說你把罰則拿走，鼓勵大家做，而且那個罰則還有很多大的問題，不要忘記了，假設這個銀行被入侵的時候，金管會本來就要罰他，罰的還不只100萬，請問你要重複罰嗎？金管會已經罰他了，資訊處又要跑罰他100萬嗎？是不是要重複罰？

主席徐副處長：

請問金管會現在的資安事件有罰嗎？

吳國維先生：

有啊，第一銀行那件事情不是被罰嗎？你開什麼玩笑，你到今天都還不知道嗎？

主席徐副處長：

我必須強調，我們今天被入侵在資安管理法裡面沒有罰，這個部分要先做釐清，那個是金管會的罰，還是回歸他原本的罰。

吳國維先生：

很簡單，我只告訴你，資安這個部分在其他國家都去不罰，連美國這種國家都不罰，請問你要罰的重點跟目的在哪裡？你是要學中華人民共和國嗎？全世界就只有中華人民共和國在罰，剛剛跟你講德國都有這個問題了，你們只會找一個德國，你為什麼不說我們就是抄中華人民共和國的？

主席徐副處長：

理事長，我同意你剛剛所說的論述，我們現在跟中華人民共和國立法目的是不一樣的。

吳國維先生：

怎麼會不一樣你罰人家錢，哪有什麼不一樣，你在說什麼？

主席徐副處長：

你可以繼續，但是那個立法目的還是不一樣，我們必須做一個澄清。

親民黨立法院黨團：

我要接續吳理事長的的話，任何的人面對罰一個最簡單的避險措施就是花錢去找能夠處理這個問題的人，不管是外包公司也好，或者是專業的服務公司也好。所實在很不想講，你們這樣的設計就是在替別人創造商機，我覺得一定要講這句話留個記錄。你們連行政機關自己有員額、有錢，自己都做不到的事情，還要去規範民間團體，不是逼民間業者跟團體花錢去消災了事嗎？

第二個，剛剛副座談到，關鍵基礎設施要怎麼樣態沒有辦法列出來，說這個以後再來跟NCC討論、定義，這點我非常不同意，因為從法理的角度來說，你這樣的說法完全違反法律保留原則以及法律明確性原則，這是很嚴重一件事情。不管我是不是立法院，我就從一個普通平民老百姓來說，我不可能認同一個立法的條文是可以這樣子的，完全不符合法律保留原則以及法律明確性。

歐盟的網路與資訊系統安全指令是採取正面表列，把第一級到最後一級、主部門、次部門、行業別全部都列出來，你們現在就只能在法裡面用一個「關鍵基礎設施」，要用子法訂定，我真的覺得這種立法技術不管我不是立法院的助理，從一個平民老百姓，有念過法學緒論完以後，我都沒有辦法同意你們這種立法原則，要不要大家再把法學緒論拿出來看一下，有沒有說立法要有什麼原則？你們這種說法我是完全沒有辦法接受，要不要再去找你們的行政院法規相關的人員去討論這件事情？這樣的說法我覺得是很嚴重的。

我再回應一下NCC這位先進，你剛剛一直提歐盟，歐盟的網路與資訊系統安全指令，他們明確指出各會員國政府對於資訊安全之管理應採取輕度及事後監理的模式；美國的聯邦資訊安全現代化法更不用說，因為他只規範聯邦政府。我不曉得這樣的立法怎麼會是個趨勢？當然如果你是國安機關就不是這個態度。所以我覺得行政部門在表述你們的立場的時候，你們真的要記住你們的分際，「分際」這個字好像是現在熱門的關鍵字，記

住你們的分際，你們要記住你們是行政機關，要依法行政，你們不是國安機關、CIA、NIS這種單位，你們都會去違反法律的明確性以及法律保留原則，無限制去擴張你們的行政裁量權，這個是有違行政機關依法行政的份際，謝謝。

主席徐副處長：

我回應一下剛剛講的，國外是有主部門、次部門這樣的規劃，在我們安全法裡面說明欄有明訂我們是依據這個國家關鍵基礎設施安全防護綱要中，這個綱要裡面也是分主部門、次部門，其實是有去指定跟明定的，所以我們的做法應該國外沒有太大差異。

親民黨立法院黨團：

你要符合法律保留原則與法律明確性，這個東西應該列在法上面，不能整部法裡面就只有關鍵基礎設施以及關鍵基礎設施指定者，這樣就沒有了，所有的規定都在子法裡面，我說難聽一點，立法院甚至一般的老百姓很不關心子法的訂定，而且從你們優良的紀錄來看，在今天公聽會之前，你們已經辦過6場，那6場的會議紀錄我都大概看完了，也是言者諄諄、聽者藐藐。

我會把我的意見再寫成一份書面給你們，還會要求你們再回覆，你們都不用急，我這個人是非常有耐心的。請你要深刻了解到你們行政機關的分際，你們是依法行政，所以你們所做所為、所立的法，全部都要符合法律保留原則及法律明確性原則，我不認為從一個有讀過基本法學緒論的普通老百姓的眼光來說，你們這樣的訂定立法技術是完全違背這兩個原則的，完完全全是空白授權給你們，以後你們愛誰規定誰是關鍵基礎設施就規定是誰，我覺得不是這個樣子的，謝謝。

主席徐副處長：

因為我們現在這個法案其實在立法院，我們就是還是會尊重立法院到底之後怎麼給我們建議或者是修正，我想都沒有問題，但是我還是必須強調，我們現在這個罰則部分，你被攻擊沒有罰，不是因為你被攻擊就罰你，現在這個法沒有這樣的規定，我們主要罰的還是在於你知悉通報這件事情，就這個部分做一個處分，就這樣而已，所以這個部分還是必須做澄清。

剛剛理事長特別交代未來CIP跟CIIP我們如何做區隔跟定義，這個部

分我覺得是可以討論的，沒有問題，我知道其實現在大家比較關心的是，到底哪些是跟Internet有接觸、哪些是不跟Internet接觸，SCADA、ICS這個部分是不是要納入把它放進來？這部分是理事長比較關心的議題，這個是可以再討論的，我們今天也沒有做特別明確說是或不是，都還有討論的空間。

接下來，剛剛還有什麼沒有回答的？不要罰則這個部分就看立法院到時候，因為我們法案畢竟已經送到立法院了，這個在立法院也可以再做一個討論。各位還有沒有需要特別提問的？

吳國維先生：

可不可以撤案把這個罰則拿走？

主席徐副處長：

以我們現在行政處理程序，就是送到立法院，就是由立法院做一些審理，我們尊重現在立法的程序。各位還有沒有要提問的？如果沒有的話，我們今天會議就到這邊，謝謝各位。