資通安全管理法子法草案說明會逐字會議紀錄

時　　間：中華民國107年4月30日（星期一）下午2時00分
地　　點：光明客棧咖啡沙龍
出席領域：法律、資訊專家學者

【記錄開始】
主席徐嘉臨副處長：

好，謝謝周科長的簡報。那我們等一下就開始請各位人員給我們一些建議，那在各位提出一些建議跟詢問之前呢，我再說明一下，就是說我們剛剛有提到，就是我們陸陸續續開了好幾場的座談會，那我們座談會，我們現在其實是屬於第一階段徵詢意見的性質。今天各位所提的意見我們會收集，那收集完了之後我們會回去做一些調整，或是再進一步的思考之後，會在第二階段，就是在5月18，就是這個表裡面第二階段開始，我們會再找各位來一次，把我們修改的一個結果，或者是…可能不一定要修改，或者是透過其他方式調整的一些方法來跟各位做一個報告。我覺得這個大概是我們的做法。那我們就是針對這個子法的部份來做討論。

那各位的桌上原本有放一個發言規則啦，不過這是因為原本我們之前其實也有幾個場次因為出席的人多，所以我們其實為了控制那個發言的時間跟程序不要會議拖得太久，所以我們有定一個發言規則，不過我想因為我們今天人不多，所以大概就這個發言規則大概就…不適用這個發言規則。我就直接從這個前面三個部份，我們真正兩個階段，因為我們子法裡面分成兩個部份，也就是針對第一個部份來先做討論。那第一個部份是針對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，以及公務機關所屬人員資通安全業務的獎懲辦法，就這三個子法來請教各位。我不知道各位有沒有哪一位老師要先發言的？給我們一些建議。

中正大學法學院：

謝謝副處長，就是說我們先請問一下這個資通安全管理法草案，它是行政院送至立法院一讀而已嘛，因為之發新聞說快要三讀了，才完成一讀而已？所以它還是有可能再被修改嘛，因為在那個委員會裡面，它是屬於內政…司法是不是？所以它可能會再更改對不對?那所以我的問題其實可

能是針對那個母法相關的喔。那就是說我現在先提起，第一個就是剛才講到的就是說這個母法，就是本法的主管機關是行政院嘛，就是，就我看過的很少，幾乎沒有見過說主管機關是列行政院，因為行政院它不是一個業務單位，不是一個業務單位，就是為什麼是這樣列？

主席徐嘉臨副處長：

老師你先說，我們等一下會一起回答。

中正大學法學院：

對，就是真的幾乎沒有看過法律它的主管機關是寫行政院的。就是說你一定要列一個執行業務的單位，是叫做它的主管機關。好，那再來，就是說這個母法裡面喔，它第三條裡面去定義這個公務機關，說行使公權力的中央地方機關、機構，跟法人這樣的一個定義喔，因為行使公權力這件事情，因為各位，就是說，處長…副處長這邊可能不是那個讀法律的，但是我們讀法律的就會比較…比較對於這個行使公權力的概念，會有法律上的疑義啦。也就是說當然我們理解就是所謂的指稱公家機關就叫做行使公權力，可是行使公權力是不是就這樣子的一個理解，也就是說，有時候私人單位它也會行使公權力，這樣子。所以不太確定你們這裡想要涵蓋的行使公權力這樣的一個中央、地方機關，是指組織法上面呢？還是指它的公權力行使這一件事呢？

我舉例來講，像我們現在大學，我們可能有公、私立大學，那私立大學也會行使公權力阿。那私立大學他其實教育部也是它的主管機關，可是教育部也會管私立大學這個事。所以這個時候我不知道大家想要講的公務機關到底指的是什麼？因為這會牽涉到我們分公務機關跟非公務機關嘛，那這個公務機關剛才報告的，科長說它的就是那個要求，資安的事務喔，它的責任比較重，所以你這個公務機關如果把…就是說，你的範圍到底在哪裡？我覺得這樣的一個定義，就是不是很明確，加上這個行使公權力的這一件事情，如果你不加上行使公權力，你去講說，只要是組織上，就是我們說的所謂公家的單位，那這樣會不會又涵蓋的太廣，會讓有一些其實不是那麼重要的成為公家單位，然後發覺被要求這麼高的一個資安責任。所以我們覺得這個地方可能那個到底想要涵蓋什麼是叫做所謂的公務機關，這個還要再考慮一下，要怎麼樣對他們做一個定義。

好，那這個公務機關的定義裡面有排除，不包含那個軍事機關和情報機關，這個我們是想請問說為什麼排除？是關於他們有額外…就是有另一個法規去規定他們有關資安上面的責任嗎？那個軍事跟情報機關，就是說之前草案就是說的它的那個，你們之前辦的那個不包括軍事和情報機關，不包括，為什麼不包括？他們不是應該更高等級的那一種資安要求，所以我想請問為說不包括的理由，是因為他們是基本上不罰嗎？，還是如果沒有的話為什麼要把他們排除？就是公務機關某一些不是那麼重要的都被賦與這麼大的資安責任，但是軍事跟情報機關卻被排除在外面。

好，那再來，第三點就是那個特定非公務機關的這個定義喔，就是從它第三條的第六款裡面，去講到的這個剛才智禾有報告，或者是說以前開會或參與或者是有在講那個關鍵基礎設施的企業，那你們現在說就是用公告的喔。那我還是會建議是說，這個關鍵基礎設施的概念，就是涵蓋哪些事務喔，還是要把它放在母法裡面比較好。因為這樣子參考過去對應那個它的目的事業主管機關是什麼。而且你在這個母法裡面，剛才也說第二條你只有定主管機關是行政院，喔，或是說是資通安全處，這樣子，但是你卻沒有去講每一種事務它的目的事業主管機關是什麼。你去看就是一些法律它會牽涉到…它會有一個主管機關沒有錯，但是它也會牽涉到各種事務。各種事務的話，那這時候會有各種事務的目的事業主管機關，那這一些主管機關都應該列在母法裡面。像你們說醫療，那一定是衛福部，那就是他的目的事業主管機關；通訊的…這一些甚麼…那個都應該要列在母法裡面才是，而不是說用那個公告的方式。

好，那這個特定非公務機關，因為我看它的責任其實也滿多的，甚至還蠻重的罰則，那在這裡就是說，還涵蓋公營事業、政府捐助的財團法人，那這個就是有一些公營事業他的業務的範圍，對不會那麼重要到說他被要求這樣的一個資安的責任啦。有的或許你會覺得說，像是台電什麼…就是民營化的那一些公營事業，我們會覺得它承擔的是很重要的，可是有的像是台酒呢？做酒的，他裡面那個會有很多這個…會牽涉更多的是商業機密的問題，而不是這種所謂的會因為去影響到這個什麼社會重大利益或國家權益什麼這一些事情，它可能更偏重的是商業的那個範圍。所以像這樣的公營事業喔，那所以有一些財團法人他們是比較偏的是一種商業性的話，需不需要給他們要求那麼高的一個資安的責任呢？所以這一些那個定

義，因為你這個法就是要去幫到人家，那就會有後續的它的責任、後續的這個罰則，有可能牽涉很大。所以這一些事情如果不把它的範圍弄清楚，到時候就會產生很多爭議。

好，那在座剛剛講到說這一些特定非公務機關，就是我覺得應該是要以它的業務的事項來界定他重不重要，然後才可以去連結他們目的事業主管機關是誰。這裡我就會想到的問題，是說，因為我們這個法，子法裡面它的要求的這一些事項，公告什麼，或是要去稽核什麼，都是交給這個目的事業主管機關。那目的事業主管機關，它有沒有這個能耐去做這一件事情。這個以前應該已經討論很多，就是討論很多次了，也就是說，有人會提出來，說你如果不是把這個事務都交給中央級的這個資通處的話，你交給各個目的事業主管機關，像經濟部、然後衛福部，他們也不是這方面的專業，那會不會有那個能力去做到你包括子法要求的那些事情，所謂的去包括的說他做的這些什麼樣的報告過來，你有沒有那個能力去講他這樣子，去查核，就是說他做這樣子是不是足夠？所以如果說目的事業主管機關每一個的能力的話，你這一個整個法，就主法不足以執行，就會有這一個問題，所以你要不要把它們的這一些資安責任，它的對口是把他放在這個目的事業主管機關？這個是我想一想，是不是要放在目的事業主管機關，還是說都放在行政院的這個資通安全處來去做。這個就是政府它其實會有一個我們所謂的專責的單位，現在就把每一個事務…有關資安的這一些事情都放給各個目的事業主管機關，那一個目的事業主管機關他不是這一方面的專長。他不是這一方面的專長的話，他做不來的這個事實，那這個法就是會變成沒有辦法run的。

好，那再來，第四大點，就是說講到那個裁罰，就是後續那個懲處喔，那剛才科長報告有提到這個公務機關是增加了那個…就是負責這個業務人員的獎懲，可是我們想要進行的，就是說，到時候各個機關，我想想看你說公務機關裡面他涵蓋的，像我們公立大學可能會被涵蓋，就是那個所謂的那個公務機關這樣子，然後還有很多機構想他應該也會被涵蓋在內，現在就是說有沒有那種編制去聘用一個具有正式公務員的人，而且他還是有這一種資訊專長的人，然後用考試…我要考那個任用公務員的那一個方式來聘任，這一個我們覺得大概做不到，沒有那個員額，那個報到銓敘部那裡，他絕對不會給這個名額。那所以這些人都會變成是，如果你這個法

通過，你要這樣子要求，要設這個公務機關裡面的你講資安長也好，或者是去負責這個資安這一塊業務的人，就是我覺得都會用約聘的人來做。那你約聘人員的話，你用這樣的一個懲處的規則，沒有用。因為他們不是公務員身分，你沒有辦法跟他做所謂的嘉獎、什麼的，這一些東西。嘉獎或者是記過，約聘人員約聘人員跟這個機關，跟這個單位是一個契約關係，是一個契約關係你不可能用這個方式去對他所謂的懲處。所以這個問題是說這個子法喔，你更本就沒有去分人員身分，你完全沒有去分那個人員他是什麼身分。那我們一定都…不太可能，未來不太可能是用公務員。你聘不到這樣的專長的人來要列這個國家考試的事項，這個以公務人員任用法來任用的這一種資安專長員工，你大概聘不到。

所以像各位在這個資通安全處，像我們是說有幾個是真實的公務員，只有幾個是正式的公務員，就那其他的單位，你都可以想像。中央級的能夠有幾個是正式的公務員，那那個其他的機關他怎麼提報正式的公務員，而且又有這方面專長的人。所以這個子法那個部份是完全沒有去分他的身分，但其實你去做這樣獎懲，有些時候如果你對於約聘的人來講，完全這個子法是沒有用處。

然後再來是說那個獎懲，公務機關的那個獎懲喔，就是說沒有提到機關首長，你就好像丟給那個負責人，那個負責業務的人，這樣，你完全沒有提到機關首長的責任。那這個就對顯露出一種公家機關裡面的一種現象，就是說出事就是那個最小的那一個人去負責這樣子，然後機關首長好像就不用負責喔，那我覺的這樣的子法訂定不妥當。那再來就是公務機關其實不見得不能裁罰…不能對它裁罰。可以裁罰的，對公務機關可以裁罰的，你照樣可以對它科罰，很多法律都有，喔。所以如果你這個法在到時候進入那個立法院，或者是三讀，那如果要開公聽會的時候，那個非公務機關的那些民間單位他一定來給你砲轟，你開罰到五佰萬，你公務機關你去罰那一個負責業務最小的那一個人，甚至他可能只是個約聘，然後你這樣子可能會有很多問題。好那這個就是我們大概先提到這一些我看這些子法，包括母法的問題，謝謝。

主席徐嘉臨副處長：

我大概簡單地回應一下喔，因為我們今天其實主要是內容是探討子法。那剛剛老師提供的幾個問題，其實在這個立法院的，之前在一讀，在看

這個母法的過程中，其實大概多多少少都有討論過。第一個是這個母法到底要不要定主管機關，然後主管機關應該列誰。那目前我們的這個法律裡面，其實有列行政院為主管機關的部份，我們至少在隨便找一下，大概就是有這個法制司條例，還有花東地區發展條例，那這個其實都是以行政院為主管機關。那另外一個是，剛剛老師…

中正大學法學院：

那種條律不是業務性的，通常法律是政策性的。

主席徐嘉臨副處長：

老師剛剛是說為什麼…　老師剛剛為什麼不能列行政院資通安全處。行政院資通安全處不是機關，它是機關裡面的一個內部單位。

中正大學法學院：

你可以對外發文嘛，只要有權，你可以，不然你其實你只要是有對外可以發文的權限，就可以當主管機關。

主席徐嘉臨副處長：

因為它是主管「機關」，但我們不是「機關」關，我們是裡面的單位。所謂的機關就是…　比如說行政院是一個「機關」；交通部是一個「機關」，對不對？行政院的組織法不是資通安全處的組織，我們是行政院裡面有一個處務規程，那我想我們今天的主要主題不是在談母法這個，因為母法那個其實已經被多次討論過了喔。

比如說像這個行使公權力，這個我們字用於其實是參考個資法。個資法現在的公務機關就是依法行使公權力的中央或地方機關，或行政法人，大概是這樣子。那軍事跟情報機關，因為它特殊性質，我們在說明欄這邊有特別去說明。原則上就是由另外一個規定去做處理。那關鍵基礎設施的主管機關呢，目前其實當然以我們…　這個後續未來會比較做一個…　就是法之後會比較一個一定的程序定義所謂的關鍵基礎設施的提供者。那在這個程序的過程中，以我們現在在run的過程中，各個關鍵關基礎設施都已經有它的目的事業主管機關。比如說通訊類那就是NCC；衛生醫療原則上是衛福部；交通設施，原則上陸海空就是交通部，大概就有這樣子一個規則。

所以在這個法裡面我們並特別再去把它定。是在說明欄裡面其實有大概制訂出來，就是大概有說明一下大概關鍵基礎設施是包含哪些。那因為

其實關鍵基礎設施是會兩年被檢討一次的。所以有的國家它的關鍵基礎設施會隨著國家的這種風險行事會去調整的，喔。所以說不是說我現在是八大類，未來就一定是八大類，這是有可能會去做變動的。所以這個把它定在這個裡面，我想這也是其中一個原因啦。那另外一個是特別提到，就是說，政府捐補助的財團法人，那原則上喔，它雖然是納入範圍，但是它確實不是每個都那麼重要。所以我們有一個資安責任等級，也就是說會依據他的業務屬性去…　依據它的業務屬性去定位它是在哪一個等級，是比如說A、B、C、D的哪一個等級，喔，所以其實是有這樣的規定。那依據它不同的資安等級，它就會有不同的一些資安的防護措施，跟應辦事項要求，會放在裡面。喔，所以大概是這樣。那接下來是說，這個目的事業主管機關是否有能力啦，或者是這個能力…剛剛老師最後有說到公立大學能力夠不夠這個部份，那有我們另外一個配套措施去做，最主要我們現在其實也之前也在跟我們人事行政總處有在做人力增補的計畫，除了是人的質跟量也會同步去增加。

像比如說像我們的這個針對這個未來要管關鍵基礎設施的這個公共，這幾個政府中央主管機關，我們就開始有一個資安服務團，在他們的主管的裡面的業務單位去把他們的能量提升，那接下來還會有人力的增補計畫，所以大概是這樣子。那接下來老師有特別提到說，現在的這個約聘顧人員，他的獎懲不涵蓋在裡面，還有這個資安機關的首長是不是也應該有責任這個部份，我們會把它列入參考，因為我們覺得這個部份確實是我們沒有思考到。但是我想機關的首長，地方他負的是政治責任，如果這個事情真的很大，我想那他應該有他們自己的一個處理方式，因為在這邊很多的在那個位置有一定的處理方式，所以大概是這樣子。

好，那我不知道，我們是不是就請兩位老師，那等一下老師，如果老師等一下有需要…就是看兩位，一個，蔡律師，或者是林老師。

國巨律師事務所：

那我簡單就幾個部份提供一些淺見。因為剛才就是剛剛講到有說第一個是為了隱私權，或者是相關的一個針對檢查的部份，未來會想把它做一個刪除嘛。那這個部份其實我想要給建議，是說，雖然有考量一些權利上面的保障，但是如果遇到一些需要緊急事件需要去做檢查的部份，有沒有需要去賦與就是一個依據，讓他們可以去做，讓主管機關或者那個中央目

的事業主管機關能夠去做檢查，這個部份，可能就是看是不是要再衡酌一下。

那第二個有關於我們在那個委外的那個部份，如果是參考個資法的情況之下，那其實針對於一些項目，其實他們都有做一些定義。然後在母法本身，針對於那個責任的一個歸屬，其實有一個依據是第四條的部份。那其實在我們定義上面的話，就是這個部份的那個…在子法草案的部份，就是它是不是會有參考相關的一個部份，讓他比較能夠去做依循。那有關於那個稽核的部份，因為我們現在稽核的對象是特定非公務機關，那針對於公務機關的部分，我覺得我把以上解釋應該會涵蓋在那個被受稽核的範圍之內，那這個部份可能已經是大概先前對這個部份有做一些討論。

那接下來是有關於那個懲戒的部份，因為其實公務人員他們在執行一些可能跟資訊相關的部份，假設我說不定碰到緊戒事件的情況之下，可能會讓很多的公務員很擔心他們的一些處置，導至於可能到時候動輒會因為考量到被懲戒，而有一些那個顧慮。所以這個部份也許在那個制定子法的草案的時候，可以考量到是說那個懲戒的一個制定輕重跟認定的狀況。

主席徐嘉臨副處長：

對不起，妳剛剛妳的第二個意見是說，委外監督的時候？

國巨律師事務所：

我是說因為在個資法，其實個資法它在母法其實它有特別明文，但是這一些我覺得法理上，我們在做責任認定的時候，其實跟實際狀況的間隔，那個不見得是說法律關係會不清楚。那是因為其實個資法其實它在委外的部份，它說了，在母法去規定是說，就是受託機關會視為委託機關之外，其實它還有規定說，就是那個委託機關必須對受託機關做監督，那監督的部份，其實在細則上面它有去訂定。那我想我們應該會在細則或者是在一些子法裡面去訂定一些委外應該要注意的事項。但是能不能可能就是，看是不是說能夠做它的一個委外要監督的一個部份能夠考量到應該要監督的事項去做定義。

主席徐嘉臨副處長：

好，謝謝。那我想就先大概先簡單回答。就是行政檢查的部份，你知道行政檢查的部份就是本來其實在立法院一讀的過程中就是把它拿掉了，就是把它拿掉了，所以這個部份大概就是這個樣子。那委外監督的部份，

妳剛剛提的是有關個資法施行細則的規定，是不是可以比照的意思嘛？

國巨律師事務所：

從個資法的角度來看，大家在看監督，事實上其實應該還算是有一個依循啦。那我不太確定是說，在我們這邊的一個委外監督相關的部份，是不是能夠幫大家辦理，就是母法實施範圍之內，大家能夠去了解說應該要監督的部份，就是讓大家比較具體的知道。

主席徐嘉臨副處長：

這個部份我們可以來參考一下，我們回去思考一下，看是不是要比照個資法這樣子處理。不過原則上，一般我們現在在實務上，就是如果機關還是透過委外，一般機關的資訊系統跟服務透過委外公司去做的話，原則上負責任的還是這個機關。

國巨律師事務所：

這個法理上其實是分得出來，但是連結到許多在我們的那個上稽核的部份，他有沒有在我們會稽核的範圍之內，免得到時候我們就是把它稽核了。

不好意思，我剛才其實在獎懲的部份，其實有一個部份是因為剛才我們有講到是說，在應變的時候再通知會有一個時間上的限制，那其實可能包括就是我們的事件嚴重性的不同沿用是不同沿用、不同的處置時間的一個狀況。可是因為這個部份其實都會連結到一些的可能懲處的一個部份，所以可能也可能要考量一下大家應變的時間，是不是能夠在我規定的時限之內去做一個回覆，或者是下面的動作。因為那個部份呢，其實可能是資訊人員會比較擔心，因為有連結到懲處的部份。

主席徐嘉臨副處長：

我們現在這個對於公務機關，現在比如說一個小時之內要通報，然後接下來通報之後你就開始去做復原，或者是讓它的服務可以持續運作，大概一個是32個小時。

周智禾科長：

36跟72小時。

主席徐嘉臨副處長：

36個小時，跟72小時要完成這一件工作。目前大概試了幾年裡面，在看起來是處理機關跟處理效率看起來是沒有什麼特別的太大問題

，不過我想這個部份我們會去，因為我們自己也有大概在這個子法草案，因為我們公務機關這麼多意見的徵詢，那初步看起來好好的，大概沒有太大問題，不過我們會再注意一下，這個當然還是關係到他們有沒有辦法遵守，因為畢竟有獎懲的問題，這個部份會再注意。林老師。

元培醫事科技大學資管系：

副座，各位同事，首先我非常肯定資安處做的事情，我想如果過的話，因為這個是蔡英文的政績嘛。我也跟各位今年預告很久了，不是子法是母法，第一個，我對母法我不想再講了，因為已經都在立法院大概已經呈了，就是希望提升我國資安的能量，那這個對不對很難講，因為統計那邊新的法律，在你那邊傳統的都沒有…就像司法檢察官，在刑法的部份，92年通過以後搞到現在，我的學生很多人都搞不清楚，這個有空再講。

那這個為什麼要做，我是覺得很重要，子法這六個是來補助原來母法的不足，所以各位專家學者應該是從這個角度來看，讓他們各單比較說其實他這個有沒有適用，但是你不要傷害太大，就像個資法一樣，通過以後都沒有人在做，都做憨頭。那我接下來講的就是，一，我就用ISO來跟各位講。我講第一個，剛才那個施行細則喔，第五條，這個所謂的資安安全維護計畫很重要喔，包括不知道要怎樣安排，然後第一項該做的提報項目是，這個法律類的說明怎麼來的我不知道。

現在問題來了，現在各學派不一樣，那我現在是ISO的信徒，那我舉例一下喔。因為很多會他說他有聽過ISO，我弄錯了，今天我再澄清一下，我舉例一下，105年，一銀的這個事件，他都只有通報ISO27001，可是他是導入內容是27002啊，他有沒有導入銀行的27015，他有沒有導入27007，他有沒有導入270，通通沒有。我說有沒有導過27005？沒有啊，為什麼？輔導廠商便宜行事，他就導入2002。2700裡面有講風險評估，你大的單位一級，你要導入27005啊，27005現在已經第三版了耶，所以在寫這個規格書的時候就不認識了啊。所以我跟他講過，你這個麼改我沒有意見啦，就是裡面太薄弱了。就是我舉一個例子嘛，你這麼大的比如去控這麼大的銀行，他應該除了導入27002內容以外，他還要加27005，因為27005有風險評估啊，它是很詳細的啊。那

他們在唸這個的都有沒有動作？沒有嘛。因為pay的錢不一樣。

所以各位你去看27005，沒有一個單位開會的時候，做出一個這個導入27002，沒有說27005，都沒有。好，我們再舉例一下，去年剛通過，所謂的sencond specification,，這是新的觀念喔，你們有沒有了解。就是說我們驗證的時候是27001對不對？可是在去年，條例通過27799。它是什麼意思？它是income還是什麼？它是for sencond specification。什麼叫sencond specification，就是說你是電信產業，你應該27012加27011。那早期只有27011，27012加27011，它沒有事喔。可是驗證的時候，早期是27011，不足啊，所以在去年通過一個27799，它要很快地要符合27011、27005。啊現在有哪一間公司有沒有在做？只有一個人現在一直在做，我說很常沒有人去導入27799。

所以我們的夢想就是，副處長妳這個應該是不懂啦，因為可能這各充斥了我們的幻想。我再講一下舉例，電信產業，它應該是27012的內容加27011，因為27011新版2016年出來。可是保護內容是這樣以後，他們怎麼做？早期就是做27011，現在27009出來了，他就是second。我的意思說，你這一個法條，第五條整個內容，你沒有去看。你委託不曉得誰，你看現在再內容，這個都沒有錯，然後我再舉例一下，這方面沒有錯，我再舉例一下。我們的智慧醫療，所有的醫院到現在，長期我也參加，醫院現在通過27011了，我發現有講的系統都毀了喔，我先講正確的觀念。醫院他到現在幾乎只有導入27012的內容，那27799已經三版去，今年出來了又第三版，2018年，27799就通通沒有人用啊。

我講內容就好了，因為它是specific center啦。因為國際上有說三大產業，包括現在又四大能源，能源的出來以後他有一個27009。可是這個觀念，你怎麼樣化為在子法裡面，因為子法我剛剛講，就是補足母法的不足嘛，那實行單位可以去plan嘛，那你去plan法條你就多了，那什麼是專家，我不知道專家在哪邊。這個國際上已經在做了，我們沒有做，所有國內的所有的醫療產業，現在沒有導入27799的內容，只有27012，它是一般的。所以未來醫院一定會出問題的，個資嘛，都包括嘛。我們今天講銀行，好。

所以在這裡面我也希望這子法是必然的，但是應該更符合，更科

學。那現在在專家學者說得更科學，我們國家子法，就是ISO可能需要參考，我不知道你這個是委託誰，通通沒有，退貨。

我現在講第二個更重要，資安事件，先講這個責任分級，責任分級，各位可以翻一下責任分級第一頁這個附錄裡面，四級裡面，各位這裡面的分類裡面，表一、附表一，好，A級、B級、C級。然後你看喔，第五頁，你看這個數字，簡直不可理喻，都是回到20年前。你現在還寫這個CNS 27001，這寫這個都不對啊，這個內容驗證是驗什麼證嘛？所以你們要把它弄進來，造成你分級制度，你沒有把強度出來。所以在相關的ISO標準都有分很清楚了，我就說實在的，你這個導入內容，你只有寫27001，如果我們今天是子法在定又回到20年前，我們要推動，完蛋了，那這個我們政府要資安處怎麼辦。這個我是覺得很嚴重。所以這邊，這邊寫的內容，辦理內容的說明表，不夠精準！不夠專業！所以這個分級的部份，相關的標準，都有分類去參考。

那我再舉例一下，剛才這個主持人講，包括那個基礎建設，那因為我剛好做GI，幫政府做第四期，那我也跟你講，那個就是抄美國，然後更改國名，那個是完全不符，那個責任不是在這邊，那個是國土安全方面的區域。那以後會不會改，不曉得，因為可能這個一直在改變，可能會改。那當初為什麼去把它改變？因為我是第十期資通主任，我不想，我是遵從第一期。我曾經也提過研議，為什麼改？後來他們解釋說，因為美國分們將近50個分類。後來我覺得算一算，後來做一做才40個。好啦，那現在政府法條寫這樣子，我覺得以後彈性可能會比較大啦，這是第二。

那各位，這個如果我講細的話，這個網際空間，跟所謂的CI、跟CIIP喔，這個很多人還是搞不清楚，這個法條已經出來了，我看很多人。27103，今年才通過，那就界定三十年，各位你應該知道，他一定沒有做完，我剛好才看到，附註一下，27013，我也是現在才看到，那它是2018年2月1號剛通過，它就要定義cyber security of 相關的ISO，這個條文我是看那個，看摘要，這個條文要去看。那我覺得它上面其實定義就很清楚了。所以這個方面應該未來我們資通安全這個定義，當初很多教授、委員是說，最少三個有講，就是說用列舉，所有的法條要改，就是最少三個，就是用明示的喔。後來我不曉得母法有沒有改過

。後來我也鼓勵，就是用列舉的這個是所謂的特定非公務機關嘛，這個名詞。後來講說，這個公告出來，跟當事者講說，你被認為違規，嚇他一下，然後你給他記過，這個部份我是覺得未來就是要從，就像日本他們是這樣，他們剛開始就沒有很多，列出來，列幾個?然後你再更新嘛，這樣影響可能非公務機關不會那麼大。因為這個涉及到特定非公務機關，所以這個分級部分。那再來就是，剛才那個盧教授提到我剛剛一起看，這個我要講一下，就是說，管理原來獎懲都有，但是對於資通安全還沒有講，這個就是說母法中的母法。可是我們國家現在也在制定法律，制定基本法，就是說對政府機構資訊的一個法律。政府對於資訊的法律，不要說資安人員，我們都沒有法律保護，所以資訊人員就是變成犧牲品，所以這個部份我覺得很重要。剛才是妳有提到是說，這個沒有包括長官跟約聘人員，就是說，對公務機關裡面的公務人員，包括廣義的公務人員，不然你說不是公務人員，比如說老師，公立大學都不算嘛，你們有沒有算？

中正大學法學院：

要看，行政職的才是公務人員。

元培醫事科技大學資管系：

對啊，他有接行政職的才算。所以可能還是指公務人員還是指正式高普考及格的。因為目前政府是說找不到所以要用約聘的話，約聘的那薪水才會高，那我們的行政機關可能也會這樣，因為他們以後會聘請一些不是真正公務人員，但是他有那個技術人員就會比較高。所以那個部份我不曉得副座有沒有報告，就是你們機關後來要訓練，那些人有沒有算在獎懲?

主席徐嘉臨副處長：

你說我們資安子法嗎？

元培醫事科技大學資管系：

不算，我是不知道，好，沒關係，我一併回答。我是說應該不會有機會，因為你們處長說未來這個資安處要去那一些類似幫各單位因為各單位沒有，啊然後這個有沒有包括在裡面，我不曉得。所以這裡面我剛才稍微看了一下，因為這個，盧老師，因為我今天才拿到紙本，那我想看，我要去台大，你給我兩千五要全部看完，應該是一個要

兩仟五，然後六個要一萬五，要不然我們教授太便宜了。所以啊，我綜合來講，子法他們也很辛苦，是必然的。我們可以從另外一個角度，就是說，我剛才講，母法定義不清楚不足的地方，就用子法；可是子法的目的是explain，可以強化我們資安能量，這個原則是這樣子的啊，所以我第一次的發言先到這邊，謝謝。我心裡很難過，我開一個半小時的車來這邊，你怎麼會給我排在這裡？我住林口。

主席徐嘉臨副處長：

老師不好意思，我們下次。

元培醫事科技大學資管系：

不如後面再多一個零，兩仟五變成兩萬五，那我就還可以。

主席徐嘉臨副處長：

老師剛剛其實提到真的非常多這個ISO的建議。

元培醫事科技大學資管系：

剛剛講的觀念真的妳要寫下來。

主席徐嘉臨副處長：

這個ISO的建議，就是說把一些現在的標準規範放進去。老師剛剛提的，你剛剛說的這幾個重點，就是幾個現在已經有的標準規範，但是其實這個規範。

元培醫事科技大學資管系：

我沒有叫你寫完啊，你要集相關的。

主席徐嘉臨副處長：

對，因為這種規範很多啦，不是只有ISO，還有很多，另外一個，還有加上現在那個CI他們自己的規範，所以…

元培醫事科技大學資管系：

我現在跟妳講，妳的解釋內容如果寫這樣，那是定義不能這樣，你能不能在括弧舉一兩個，不然沒有進步啦，還在用二十年前我寫的這樣子。

主席徐嘉臨副處長：

老師的意思是說應該也要把特別著重於那個的部份，也要…

元培醫事科技大學資管系：

那叫second specific，那是一個標準的英文。

主席徐嘉臨副處長：

我們回去思考一下怎麼樣去寫，我們思考一下。

元培醫事科技大學資管系：

不然這樣，我跟你講，很多人…我再講，我再針對27005就好了。大的機構，AB級都應該要參考，不是27002，應該要參考27005，沒有人保護啊！27005它是，你們去看一下它的這個標準喔，因為它的CNS 27005也出來了。它的標準很複雜，很細。比如台電，就應該通過27005啊，他導入27005。你怎麼變成在這裡用法條，那是你的工作，不是我的工作。

主席徐嘉臨副處長：

我們會再去…　特別是針對每個領域，但是怎麼樣用表達是說怎麼可以涵蓋到每個領域，這就是…

元培醫事科技大學資管系：

這要看妳啊，我現在是跟妳講觀念正確的話應該是要這樣啊。

主席徐嘉臨副處長：

這個我們再思考一下。

元培醫事科技大學資管系：

你們再思考？一定要列入，拜託一下，你這樣會很慘啦。你看喔，一銀就是亂搞啊，馬上跟妳講，亂搞你這個懂不懂啊？你的保護內容是27002，要怎麼說？你27005也沒有用，後來說我們都不知道，那為什麼不知道？喂，這個處罰的。

主席徐嘉臨副處長：

老師、老師，保護某個規範或者是某個標準是一回事，其實我們現在我們先看的問題是有沒有落實才是比較重要。

元培醫事科技大學資管系：

好，我再補充一點。

主席徐嘉臨副處長：

這個部份，老師，我跟你講，我先回答到你的問題再給你發言喔。原則上老師你今天所提的建議，我們都會回去再思考，第二輪的時候我們放進去的，我們就會把它再做調整，完整出來再跟各位討論。那如果是在實行上有困難的，我們也會再說明，再跟各位請教，老師

你不用擔心，我沒有說我們不放進去。

元培醫事科技大學資管系：

等一下，妳誤解我的意思，我沒有說妳一定要導。我說妳在做子法，妳就要參考它啊！妳們是立的單位，那這一些東西要不要完全拿來用，我沒有意見，我只是告訴妳一個正確方向。這個剪出來看，裡面內容都沒有放入新的概念，那妳怎麼，我剛剛也講，子法是action plan，那要全部參考，我沒有意見，我是跟你講正確觀念，通通沒有做。那27005你要不要提供參考，我也沒意見；導入之後要不要符合它，我也沒有意見。我是跟你講說，你是立法單位，你子法是來補足母法，那資安就是國安，那這整個內容都是舊的觀念，我是強調這一點，不要誤解。

主席徐嘉臨副處長：

沒有，沒有問題啦，老師這邊有提的，就是針對我們特別針對特別領域這一塊的一些。

元培醫事科技大學資管系：

這個沒人教你們也不知道，ISO的觀念你們也不知道，子法怎麼樣改成這樣，這是你們的專業。

中正大學法學院：

因為這個子法喔，它有那個責任等級的那個應辦理的事項，在這邊，你剛剛說的文件是子法公告的內容，那如果沒有做到的話會被懲處，就是那個特別非公務機關，就是會被裁罰。所以變成說，你這個其實會變成處罰的內容，那這個地方我們覺得它麻煩的是科技這件事情它一直在進步，一直在進步，有點像就…我也當那個什麼評審會的，就是調糾紛的那一種調解委員。那每一次跟醫生他們在溝通那個法，他們都會希望說你有一個所謂的標準，醫療常規。

可是醫界的就會說：可是你每次說什麼才是醫療常規，你一定要去…因為醫療也是不斷的在進步，一般的東西都是舊的。就是他們都很不希望說把這個東西很特定很具體的訂成一個法律，你子法也是法律的一部份，訂下去就…所以這邊要用什麼樣的一個用詞，但是你要考慮到業界他在…特定非公務機關他在更新這些設備的這個速度還有它的預算。也就是說你要如果訂到最高等級，然後你連最高等級的那

一種標準，ISO的標準，你公家機關都說沒有那個預算，那業界也是一樣，我覺得這個會是也是一個很麻煩的事情。但林教授說寫下去的那個是二十年前的事情。

元培醫事科技大學資管系：

我的意思是說，我再強調，你應該要參考其他法律都要納進來，當初要看。

中正大學法學院：

對對對，但是這個我覺的這就是會遇到困難的地方，因為你寫下去。

元培醫事科技大學資管系：

那些的單位他就要去做。

中正大學法學院：

對啊，如果他們…如果是寫得太高等級，你全部都裁罰嗎？罰他五百萬，誰要？對啊。

中正大學法學院：

只是說提供這樣的一個想法，就是說，我們要用麼樣的一個，就一定要把具體的那一種…　訂定的什麼樣的標準要擺在子法。

主席徐嘉臨副處長：

所以我才說我們需要思考一下這個立法企圖在什麼樣的。

中正大學法學院：

對啊。

主席徐嘉臨副處長：

下面還有嗎？蔡律師?

國巨律師事務所：

目前沒有，謝謝。

元培醫事科技大學資管系：

好啦，我舉例一下，刑法電腦犯罪專章，三十六章，那幾個我就會講了。它就是抄歐盟的法條用過來，然後我們到最後草案是357，可是跟原來的刑法比較以後，後來就降低變成355啦，這個立法過程我都知道，我就可以跳進來，法律也可以講，那我不曉得這個，因為他們有業界叫我們要以這個說為什麼要罰款？

主席徐嘉臨副處長：

因為我們在第一次評的版本跟現在大家的版本是不一樣的啦，之所以會調成這樣子，其實是要立法院一讀之後，立法委員做調整。

元培醫事科技大學資管系：

他們也沒有說？

主席徐嘉臨副處長：

也沒有。

元培醫事科技大學資管系：

立法院，他們喊這樣就是這樣啦。這也是一種解釋啦。都不會尊重法律專業。

主席徐嘉臨副處長：

好，那麼，因為我們還有等一下還有下面三個，那我們就是直接進到下面三個子法，是不是就請那個簡報切換一下，這三個，就是資通安全事件通報及應變辦法，特定非公務機關資通安全維護計畫實施情形稽核辦法，那第3個是資通安全情資分享辦法，就是請教這3個法規，委員有沒有一些建議，或是其他提出指教的地方。

中正大學法學院：

這種情資分享就是，有沒有辦法去識別化這一種。因為你如果不去識別化的，反正個資識別化的這一種。你這個像在外國很多單位，稅務機關他跟戶政的，他就不能夠互通，等等的這些，他會這樣子。但是這種資安事件你如果，就是如果是去識別化，像我們在討論其他法案，就是像衛福部他跟法務部他們就要求做，像你說吸毒的人口，毒品的人口的這一種事情齁。然後，他因為位於產生醫療衛生上的問題，那包括像愛滋什麼什麼，我們要去做這個大數據的統計的事情的話，都一定要去識別化。所以我是建議說，情資分享這一個地方可能，如果沒有辦法做到這個去識別化會牴觸個人隱私，個資法等等的個資的問題。

主席徐嘉臨副處長：

我找一下條文。在座其實講說去識別化很重要，所以我們那時候，當時有考慮到，在現在子法的這個辦法這邊的第4條，其實有做一些規範。就是涉及什麼什麼不能夠分享。

中正大學法學院：

只能是用經過他的同意這樣子的方式。有一個但書。經當事人同意就不在此，是你其他的都是法令另有規定，或為避免生命身體重大損害等，那個就還是可以分享阿。這一版的，後面的但書，看來都不在此限，就還是可以分享。原則是這些情形不得分享，但是有法律所謂的但書。

主席徐嘉臨副處長：

你是說，但法律另有規定。

中正大學法學院：

或為避免人民生命，或是當事人條例，不在此限。

主席徐嘉臨副處長：

對這個是可以的，因為法律有規定說可以嘛。

中正大學法學院：

對對對，但是就是說我是希望說，就是說在定罪的時候就是要用去識別化的方式。變成重點是那個資安的，而不是在那個取得個人資訊這一件事情。所以如果能夠做得到去識別化的話，只是去看什麼樣的一個攻擊或什麼樣的一個入侵這樣子。

主席徐嘉臨副處長：

去識別化的方式，因為我們現在是用法規規定說那些部門不能去做分享。

中正大學法學院：

如果刻意做分享，他還是有可能牽涉到那個，有講到說分享，那可能沒有明文說就是去識別化之後，但你們訂的變成是，其實還是可以分享，但是有那些我們講…。就是那些，條文就是怪怪的，對，條文訂的怪怪的。

主席徐嘉臨副處長：

因為如果說文字表達上我們可以再思考一下，可能就比較容易理解，就是第4條文。

中正大學法學院：

因為他會combine在一起阿。所以變成說你如果技術上做的到，界把它寫下去阿。就對於這個情資安全的一個，得以這個去識別化的方式加以這個收集分享，然後，有什麼事情是絕對不能分享是可以定義。

元培醫事科技大學資管系：

你把它寫下來，她不曉得。妳把這段寫下來，第4條改一下給他們。真的阿，好不好。這樣比較快。因為是如果這個她講的觀念我同意。

中正大學法學院：

但是我比較不會寫條文這樣子。

元培醫事科技大學資管系：

不然他們這樣太辛苦，你幫他改，我同意你想法。那個草擬案。

中正大學法學院：

對呀，就是妳把專家列進去進是哪一個等級之後。那個東西可能會被人家挑戰，它是說要走什麼程序。它後續的那個爭執。就把它列進去管制，算是一個，考慮說有些業者阿，民間業者，他對於被列進去這一件事情他有意見。對，然後他會去爭執，去打聽這東西。因為你們主管機關是行政院。就沒有訴願這一件事情。

元培醫事科技大學資管系：

對沒有訴願這件事。我補充一下。當初我們訂行政會議。都沒有人敢裡會。

中正大學法學院：

有些條文，也希望說一些事情的層級拉到行政院，但是，還要再寫一句，就是說他可能什麼單位去負責這樣子。所以那個主管機關即便行政院，你還是要把業務分成是什麼單位負責這樣子。條文可能要這樣子寫。行政院裡面那麼多部會這樣子。大家都推來推去受不了。希望能夠通過保護法案，把層級提高。整個草案才會成功阿。

元培醫事科技大學資管系：

可是這邊我打個岔，個資法當初主管機關算是法務部，法務部弄出來以後就不管阿。

中正大學法學院：

所以主管機關很重要。實際去做這個業務的人很重要。

元培醫事科技大學資管系：

對對對，就是你講的。所以接洽業務就是家裡有部門阿。他代表行政院，他們出來有行政院講，行政院長如果不講不就沒了。

中正大學法學院：

牽扯應該不是這樣子，行政院它下面那麼多部會，你還是要有業務的負責單位這樣子。條文要那樣子寫。就像我剛剛講說，我們是人家列進去。那人家才知道對口是哪一個。你的行政處分指的是誰阿。到時候要跟你爭的話。

主席徐嘉臨副處長：

這邊跟老師報告一下就是我們在母法裡面是這個指定關鍵基礎設施這個程序，其實在立法院也討論很久。原則上關鍵基礎設施提供者是經中央目的事業主管機關指定，並報主管機關。對，所以他們一定知道說誰指定它，所以這是比較沒有問題的，而且現在這個書面阿也特別提到，我要被指定的時候其實它是一個公開的程序。我必須要徵詢很多的意見之後才去確認那些是關鍵基礎設施。

中正大學法學院：

還是一樣啦，因為像那個古蹟，我也會參與，那個類似評審會的程序。但是它被指定了它還是照樣跟你爭阿，因為變成古蹟它就不能改建不能幹麻。一樣的觀念啦

元培醫事科技大學資管系：

對，你現在講用古蹟的。

主席徐嘉臨副處長：

因為我們這邊有行政院的法規會在這邊阿，所以這個問題其實都有討論，如果說他們有意見的話。原則是就走到實際的程序裡面去做一個處理這樣子。

元培醫事科技大學資管系：

我剛才看這三條。你看那個，我先跳一下，情資分辨辦法，你看你的說明，你就參考美國的，這邊我跟人家層級一樣。美國的標準是國家標準還是國際標準。那我們國家只有參考ISO，所以你既然敢參考美國標準，那你ISO你要放進來阿。這一個情資分析ISO相關標準都沒有用，會被人家笑，翻開前面來馬上跟你指正。這個資安事件剛通過，那個我去年就有講了27035，抄起來，它有part 1、part 2，那part 1是什麼，裡面的定義都不知道是誰做的。那part 1、part 2都定義好了。我唸給你聽，27005，part 1，2016年通過，這個定義很清楚。那各位如果擬這個草案是參考美國標準

，我就馬上用手打趴。ISO是國際標準不是某一個國家標準。然後27035，part 2，裡面action plain都好清楚。其實上次我就有講了，上次他主持我就在那邊，27035出來，你這個裡面沒有改沒有東西我就看不下去。拜託你參考美國，我就會打，因為他已經提出來了，27035資安事件。這個周科長知道，他怎麼沒有跟你講？，這個我就很生氣。27035阿，這誰做的你跟我講，這草案誰做的？你馬上它查一下27035，馬上。來，抄給你，我氣到沒力氣。科長長查一下這27035，裡面講的好清楚，拜託一下。你們不要再用舊的好不好？你參考美國，你們應該用更新的ISO。

拜託一下，資安事件你一出來了。你沒有名詞還有recycle怎麼做，那個定義已經很清楚了，ISO已經出來了。不要一直在參考美國標準好不好，拜託。各位我們國家的標準只參考ISO，那你學術的研究你要參考美國標準那是你的，但是我們國家行政單位應該是以ISO為依據，不要只參考VSI或是某一個國家的。27035，part 1、part 2都出來了。它定義很清楚喔，定義裡面很清楚喔。只是我再補充一下，CS還沒出來，我有去跟標準協會我有跟它，因為他們會訂子法，那子法今天內容我對過，都符合最新的標準。

那這個是參考我知道，是參考美國的東西，當初舊的管理的。這個是我比較，我今天講這個代表負責任，你要寫紀錄喔，你不敢錄沒關係，以後我就拿這個當證據來。資安事件不能這樣搞啦，拜託一下，資安事件當初草案我有參加，一開始標準還沒有出來的時候，我跟他講說，原來最早的是20年前的草案我有參加阿。訂A、B、C那個是我在做的。這個，拜託一下，我舉例一下，你既然敢，你看你這邊自己就寫啦，剛才這邊講的，資通影響你就可以參考，美國Cybersecurity Information Sharing Act。你敢參考美國那你ISO，你把它放在哪邊，它已經出來了阿。一個做草案的人不知道，你應該去問他阿。

主席徐嘉臨副處長：

老師講的是資安，資通安全的定義是不是。

元培醫事科技大學資管系：

不是，裡面的cycle，裡面的整個用名詞都沒有去參考27035就對了。你既使不用也關係啦，我是以我的專業來講說，這裡面草案裡面做的都是舊的觀念。

主席徐嘉臨副處長：

好，所以老師你說的是我們的這個情資分享辦法應該要去參考……。

元培醫事科技大學資管系：

沒有。第一個資安事件通報應變措施應該參考27035，這個part 1、part 2，三讀出來，那情資這個的部分，你去查相關的ISO標準你就曉得。不應該只看美國Cybersecurity Information Sharing Act而已阿，美國是一個國家，沒有錯，我們說的它就是應該以ISO為主。我的意思是曾經，ISO是國際標準，這個觀念你要澄清，好不好。

主席徐嘉臨副處長：

我們先來看一下就是到，至少他已經是轉換成我們的國家標準了，如果有已經是我們的國家標準，那我們直接來參考採用當然就沒有問題。它那個變成國家標準還是要有一定審議的程序包含。

元培醫事科技大學資管系：

我跟你講他那個案子沒有很多，他們說資安處如果今天跟他說處理CI要用，那馬上大概半年到一年就會完成，這個我參加20年了。

主席徐嘉臨副處長：

不過至少還沒有成為標準，我們可以先參考。

元培醫事科技大學資管系：

對你可以先參考阿，那我就一直說你可以看一下包括part 1、part 2它裡面寫的很清楚，你整個建議的過程裡面阿，這樣處理標準裡面，都沒有符合ISO的標準，我覺得很可惜啦。我沒有說你一定要用，我的專業是說應該要用，那你create要不要用，不用沒關係，那做紀錄我負責任，那未來以後這些都歷史紀錄，就可以提出我的觀點啦。

主席徐嘉臨副處長：

好，沒有問題，那可以有多一個可以參考的這個標準。

元培醫事科技大學資管系：

今天是我今天在意這個。

主席徐嘉臨副處長：

好那蔡律師這邊呢。

國巨律師事務所：

我想說明其實還是一樣，就是說因為在我們那個懲戒辦法裡面，對於就是辦理資通安全情資分享部分，其實針對於他前面新舊有不同的一個處分的一個部分，那因為在我們的那個，我們的那個情資分享辦法裡面，如果是下對上這個部分其實我也不曉得是說在他們一個待辦項，如果說只是單純地從上下級機關來分說他是「得」分享，跟不「得」分享的話，會不會造成說有些事件他可能會造成嚴重的一個後果。

但是因為如果說下對上是，「得」，的話，「得」沒有去進行相關的情資分享，導致情況嚴重，會不會有這樣的情形。然後再者就是說在情況之下，如果沒有去做分享，會不會就是因為他是「得」，所以其實我們也沒辦法去做懲戒，那上對下也是，他如果說判斷，可能例如說今天像主管機關有聽到一個，也許是耳聞的一個攻擊事件好了，可是因為他可能也覺得這樣子的部分無法查證或什麼的，但是因為上對下是一個應的一個狀態，那回到我們的一個懲戒辦法裡面，會不會造成是說，這個部分會影響到他們自己會不會受懲處的一個情形。

主席徐嘉臨副處長：

這我們當時設計這個「得」跟「應」，原則上當時的想法是這樣，就是說上級機關對下級機關，因為他會蒐集各國的情資，他基本上就「應」分享給他的所屬，這是「應」，但是下對上是不是一個「應」分享，這個當時的法律是因為，其實我們有公務機關跟特定非公務機關，特定非公務機關其實裡面蠻多是他們有可能是私部門，私部門你去要求他去「應」，這個就是有點在這個，我想就是說至少他沒有辦法像我們公務機關有這麼強的一個規範所以還是「應」。

但是我想有些事情是非常我要強調的是說，這個特定非公務機關如果他發生資安事件他是一定要公告的，所以這個機關他如果發生資安事件他通報在我們這邊，我們可以掌握這個機關是發生什麼資安事件。那這個資安事件的這個訊息，我們會轉化成情資分享給其他的機關，讓他們可以及早因應，所以當時的設定方法是這樣子，那就剛你不要講，如果說覺得可能疑似別的組織或者是有發生，但是他可能覺得，如果他沒有查證，他來通報，其實也是會有問題，所以原則上是這樣。

國巨律師事務所：

因為我剛剛是在想可能就是你們在討論一些立法問題，那我也有想到就是說如果今天就是我已經查證散佈，散佈下去，其實導致大家人心惶惶，其實以相關的法規來講，好像也很難處罰到這樣的行為。所以我是說在取捨下可能沒有那麼容易訂定，可是因為這個條文對應到懲處，其實還是會考量到就是說，實際的公務員他們在辦理的狀況，他們所遇到的一些處境，主要是建議看是狀況。

主席徐嘉臨副處長：

所以剛剛蔡律師指的是，特別是指第七條跟第八條，裡面有一些針對情資分享辦法裡面有一些申誡、或者是記過。

國巨律師事務所：

對對對，記過，第七條的第二款，跟第八條的第一款，還有第九條的...哦沒有沒有，不好意思不是第一款，第八條是第三款，對謝謝。

主席徐嘉臨副處長：

好，這我們回去再去把它處理。

元培醫事科技大學資管系：

我還可以在講一下嗎，剛才忘記，我講這個稽核這是很重要的，你去對這個稽核辦法，其實我從第一屆就參加行政院任務編組的辦公室還更早，行政主計處的時候，那時候還沒有27003，就是到各單位去。那現在2017年出來第二版它是怎麼導，它就是ISMS-O，他的稽核標準出來因為很嚴格，我們只有看27001跟27005，很多人都還不曉得27003，那我反過來講標準就是參考27003，寫下來27003。那稽核標準是很嚴格的，那我現在還是強調，我說我是提供一個方向給你，你行政院要不要完全參考或是不參考，我沒有意見，只是我看這個標準這個稽核的動作完全不符合27003的國際標準。而且現在2017年出來這個版，這個本來都沒有，就是說怕你稽核單位你要有國際標準，那你既然這個特定非公務機關你要做稽核他，我是覺得你要符合ISO標準，那如果通過以後，他還更高興，那不外乎他是符合27003，這個你們步驟，真的把27003，這也是我當初在講行政院後來成立這個處以後在稽核，你們裡面內部的稽核辦法，你可以去對27003，沒有完全，早期沒有通過，草案的時候我就不管了，現在有通過。為什麼要管這個？各位，你去看那個稽核他叫就是ISMS標準已經出來了，，那我還是呼籲，你行政院當然你是主控權，你要不要符合他，還是用老舊的

，還是用學者的，我沒有意見。

那我個人的專業，也跟各位講，數位證據，現在上個月，高檢組要到六都及兩個地方要成立一個數位採證中心，那我這十年來在推動，所謂的刑事訴訟法專家證明，可是ISO不利專家證明，因為專家只有你一個。可是ISO是幾百個專家，那這個訴訟很大一個，符合ISO，在法律沒有規範。那我希望行政命令比ISO更高階阿，可是你的行政命令你的內容應該要符合世界潮流，這是我們要擔心的，我不曉得我這樣講有沒有聽懂，所以這個稽核部分希望可以參考一下27003。不好意思我今天我這個長期在做這個研究，因為我發現，法條你要不要全部用，這個是你的主控權，但是你不要以為你是專家，專家算什麼，ISO才是標準，那行政命令下來後方向就不對了，這個你要思考，當然因為行政命令還是比ISO更高階在法條使用上，但是我們曾經發生過，當行政命令可能會發生錯誤，不符合潮流，這個是未來有可能會衝突，這邊情資我剛剛有講，好，這個是我再補充一下。

另外一個，這個代碼弄錯了，剛剛那個ISMS是27007講錯了，那27007應該是什麼，就是早期各位輔導機關，給國內譬如四大會計事務所，他們在都亂搞亂搞，因為個人的專業，然後270014，現在有出來了27003，那現在四大在輔導的時候有沒有遵守他，沒有。所以你剛才你在講那一個，原來再上一個那個子法，裡面的內容我忘記了。27003　ISMS要去參考一下，我覺得很可惜，不然我一個廠商講得他說他輔導單位他們是最高的，狗屁，因為他們都3C。所以這邊我附帶建議，未來行政院稽核團隊，我覺得因為這個你要做紀錄會負責，但是不講，就是曾經有，我是以專家學者，我們有找相關的廠商，可是他在稽核的過程裡面，他對利害關係人，他說他是代表行政院專家去，可是他也是廠商，所以這樣不好所以我希望未來稽核團隊，除了這些行政院政府單位，跟專家學者，相關的廠商也要找，太明顯了，被稽核利害關係人罵得要命，說你在那邊什麼，這個曾經前2年就發生過，我也希望在做稽核的時候，這部分應該是要以公學會，以及專家學者，如果他本身公學會又是相關廠商應該把他剔除，這樣子對於被稽核的利害關係人他才可以信。這個以前發生過，我講這個，跟我說而已啦，但是我沒有講不要緊張，怕我得罪人以後我很難生存，可是這個不做很嚴重，因為我們的稽核團隊以前到現在都有包含相關廠商，這是我想

要力圖要改進的。

因為業界有跟我反應，不好，因為站在自己的立場，我覺得很可惜，所以未來的稽核團隊的成員，除了政府和專家學者，應該避開他本身是相關的產業，這個公司，總經理、副總經理都可以，如果他是代表總公司，我覺得不應該，包括業界公司，包括輔導公司也不該在裡面，這樣子我覺得我可以跟你保證，如果學者有去某個公司當顧問，不找他。這個是我是覺得未來要避免的，以上。這個稽核我覺得很重要，因為我當電腦稽核協會理事長也四年了，我太懂這個，那這個27007這個IS檢定，我跟林董說很多東西都不曉得有這個標準27007，27007是針對你這個稽核辦法，你應該參考，那我們在講子法的部分，保護令的27003他也有標準，而且是第二版，他是很重要，稽核過程裡面要遵守的法，依循，我想這個子法如果可以參考國際標準，未來國際化對我們國家更有幫助，以上作第3次說明，謝謝。

主席徐嘉臨副處長：

好，謝謝老師，今天就是就ISO部分就是鼓勵我們去做參考。

元培醫事科技大學資管系：

對啊，我沒有說全部都要用。

主席徐嘉臨副處長：

OK我了解，這沒有問題這個部分我們就是，再來請示一下有沒有適合放在我們現在的法裡面的內容，那大概就，老師的大概就這樣，那請問一下還有沒有？

元培醫事科技大學資管系：

今天只有我們三個，可以的盡情發揮。今天到4點半。

主席徐嘉臨副處長：

今天讓你暢所欲言。

元培醫事科技大學資管系：

弘光的沒來，李忠憲沒來，要跟他商討事情。李忠憲怎麼沒來。他都在台中，叫我來治他們。

中正大學法學院：

他叫我來的。

主席徐嘉臨副處長：

那我們今天各位老師都沒有意見要發言了？好，那我們今天的會議就到這邊結束，謝謝大家。