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5月31日（星期四）上午 10時00分
地　　點：集思交通部國際會議中心201會議室
出席領域：法律、資訊、專家學者

【紀錄開始】
主席徐嘉臨副處長：

首先介紹我們這個法務部的官員，因為今天還有一些法律專家在，所以等一下可以做比較專業上的溝通，那我想發言規則在剛剛我們的承辦單位有大概跟各位說明一下，原則上一場座談會的時候有時候一場人數很多，所以為了掌握時間，我們發言規則原則一個單位大概一個人發言，發言每次大概兩分鐘，然後我們會針對三位人員的提問之後，我們會統一做一個回應，原則上是這樣子。

今天照那樣的規則依序六個子法來進行討論，現在就開始開放大家討論。我們先針對第一個子法：資通安全管理法的施行細則進行討論。有哪位專家學者需要先發言？

國立中正大學法學院：

副處長，有關於第一個子法建議修正條文的第三條，今天我建議看那個用詞可能再把它順一下，因為感覺起來有點奇怪，也就是說本法這個，其實我知道你們的意思是加上主管機關、上級機關、中央目的事業主管機關指定的方式和時間，對不對？

那他要依這樣的去提出一個改善計畫，所以我會覺得是說條文用詞應該是說，針對這樣一個的稽核結果，依主管機關的.，然後去提出下面內容之改善報告的施行情形。因為這個條文看起來...

主席徐嘉臨副處長：

意思上是語意不是那麼順這樣嘛？對不對？

國立中正大學法學院：

不然等一下再跟紀錄人員說一次。

主席徐嘉臨副處長：

好的，謝謝。

國立中正大學法學院：

那再來那個第四條是在講這個公務機關委託某些民間業者去辦理這個建置資通服務，然後應該注意下列事項，但是你們的第六款，第六款裡面去講到說：受託者執行受託業務違反資安相關法令，然後就是說...意思是這款我也覺得語意是有問題的，也就是說它應該在講這個公務機關或非公務機關它知悉這個受託者有違反這方面相關規定，或有資安的事件時候，他應該去通知這個受託機關去做這個措施，也就是那個用詞也是怪的我覺得，敘述很怪異，這主體應該是委託者，但第六款看起來變成是受託者，是主體這樣子。

主席徐嘉臨副處長：

好，那時間到...沒關係。

國立中正大學法學院：

還沒講完...那等一下我跟紀錄反應。

主席徐嘉臨副處長：

好..謝謝...

國立中正大學法學院：

這敘述要能讓人家比較容易理解。

主席徐嘉臨副處長：

好，那就先這樣，好，哪位再來提供建議？

國立臺灣科技大學資訊管理系：

在通報應變這裡的第八頁...

主席徐嘉臨副處長：

那個老師，不好意思我們先討論子法第一條。

國立臺灣科技大學資訊管理系：

好。

主席徐嘉臨副處長：

因為這樣可能比較不會...

國立臺灣科技大學資訊管理系：

那我就先停。

主席徐嘉臨副處長：

謝謝...不好意思。

國立交通大學科技法律研究所：

關於第四條的第三款關於複委託的問題，基本上因為我覺得複委託是一個在通信部門上面，如果今天會有這種攻擊事件的話，他其實會琢磨於複委託者，它事實上在我們的資安事情裡面是一個採取做法是...所以複委託這件事情，我覺得應該要把它認真的來待，其實是要強化他們的管制，我建議是說如果關於複委託的事情皆加以稽核的可能性，再進行契約的平等的防護條案，能讓主管機關看用什麼方式來加以直接的管制。

主席徐嘉臨副處長：

好，就這個？

國立交通大學科技法律研究所：

是。

主席徐嘉臨副處長：

謝謝，下一位？那，沒有。我先回應一下，謝謝剛剛老師給我們的建議，原則上如有文字上的修改建議，就等一下可以提供給我們。那剛剛老師剛剛提到的第四條的第六款：這主詞到底是受委託者？

國立中正大學法學院：

也就是說跟剛才老師講的一樣第三條第六款都很奇怪，也就是說你好像第三條第六款講的主體變成好像在講受託者，但是你這一條的目的是在講委託者他應該要怎樣對受託者去做管理。

主席徐嘉臨副處長：

對，去管理。

國立中正大學法學院：

但這個...

主席徐嘉臨副處長：

這我們再想一下，因為一般實務上是這樣，就是說通常會第一時間知道資安事情的人，通常是受託者。我舉個例來講，比如說我們現在很多機關在委託執行所謂的資安事件的監控這件事情，我們的廠商，其實在他們監控的時候在第一時間他們會知道有資安事件，所以他再通報給他的委託者，可是有時候廠商會告訴我說有監控到資安事情所以他會通報給委託者

，所以，實際上運作是這樣子…但是我了解老師的意思，你是說我們這邊實際是要站在，是要去規範委託者，而不是委託受託者。

國立中正大學法學院：

對!

主席徐嘉臨副處長：

好，我們再想一下…為了這個檔案錄音，但怎麼修那個條文…我們再研擬一下好了。針對剛剛老師說的第三條，針對複委託的這部份，我們說的在這邊同時有一些規範之後，其實我們也同時在跟公共工程委員會去談，不過公共工程委員他們其實會對資訊這個計畫，或是應該是說委外案…他們給的契約範本，給的設計方案會再參考，所以我們也因之後資通安全這個調整之後我們會在契約範本上面會跟他們講要加一些條文，加一些內容和做一些調整，所以我可能留到那邊去做更明確的規定。

謝謝，好，那還有嗎？要針對施行細則要給我們提供建議的嗎?

中央大學資訊管理學系：

這點我是建議，這點確實造成嘛，細則法規兩條：一條是規範委託，一方面再增加去調適或再幾個細項，或把規範受委託嘛，那才對！才清楚！要不然這條沒提到委託者和受委託者之間的預設。

主席徐嘉臨副處長：

所以老師的建議是受委託者跟委託者它的權力，它的業務分開談？

中央大學資訊管理學系：

分開規範。

主席徐嘉臨副處長：

好，分開規範。好，那沒問題，那還有沒有問題？，董事長。

中華資安國際股份有限公司：

好，我想各位主席剛剛有提到實務面，因為現在政府基本上資安再做什麼那我不管，您剛剛講的那個範本，我倒是覺得說要去思考一下，因為範本那個東西喔，事實上因為範本，因為時空背景改變，懂不懂？但如果在這裡有一個配套。我舉實務上的例子，也就是說不要用低價搶標嘛！如果低價搶標這種遊戲規則通通破廢，因為你後面一定有去講說一些，如果說今天你如果說我們有廠商對不對，如果說今天有二個單位，他就應該退

場機制！你有這樣的強制作用，我覺得政府單位不會受害，為什麼？因為政府單位從來不會自行處分，不會的。他會製造很更多的事件去解釋，對不對。然後您剛剛上面有提到說主管機關要怎麼定遊戲規則，現在那個主管機關怕向上去扛的那個時候...那主管機關是誰？那他說他還沒有定，所以呢...不在我的範疇之內。那這時候你怎麼去避嫌？那因為一直在強調風險管理嘛。完全贊成喔。

但這個方面...我們還是要去思考一下它的完整性。因為如果這個東西不完整性，我來看真的假設裡面很多去做沙盤推演，我跟你講通通都錯！因為我們這裡講process，那後面就是這些作用。 那我就看你們後面的...現在跳一下，後面處分的都是一些執行者，那處分主管呢？怎麼會處分執行者呢？處分執行者薪水又低，我跟你講他怎麼會去做這件事情？所以我覺得應該說要善處，那我倒覺得說這時候要幫忙解釋一下我們這邊的台灣個資法不足的地方在哪裡，你看GTPR PPC是我們台灣個資法一蹋糊塗阿！對不對？那就是變成外面的批准我們這邊，其實這樣是不對的！我們應該要自律，所以我是贊成這個資安細則很重要，但是完整性和一致性...我倒覺得要稍微注意一下。

剛剛有提到委託者跟受委託者不明確，有些東西要能夠well define，不是define是well define！會比較清楚，這個定下去之後，再來就是說後面執行的時候採購法那邊要來幫忙，不然剛剛那個廠商最後他也不怕你，為什麼？因為你不敢自由主政嘛！對不對，你不敢自由主政，對不對，我還是存在阿！我現在實務上看到很多最近政本單位都被攻，都是變成那個單位沒事，變成第三者要去解決他們問題...然後呢也沒事阿！那都在上面寫耶，那你要告訴我怎麼辦？他們這應該要強化執行面，請多考慮一下，謝謝。

主席徐嘉臨副處長：

好，謝謝。老師談到比較執行面的問題，那當然這個牽扯到整個政府採購法就有利標還是價格標。那這個當然是個議題，但這個廠商服務水準優劣，這如何讓政府機關可以比較...有一個透通透明的管道可以知道，其實這個我想是整個採購體制下的問題，這個部分我們會再跟這個部會做一個...那再來看有關資安部分比較可以精進的地方。

國立清華大學：

好，主席，諸位各位大家好，我是清華大學，我想請教一下在這個同樣的在第四條的第四條款裡面，有提到就是受託業務的人員像他們人員這是適任性查核，那請問有關適任性查核部分主管機關這邊有更細緻規定嗎？或是自己要去呈上去進行適任性查核？同時既然是受託業務合適，應該是以公司或是以某一個團體為主的話，那這邊相關人員是要怎麼去記錄他們的單位？

主席徐嘉臨副處長：

我現在來說明一下，剛那是范老師建議我的受託者跟委託者非法分開，這個我們回去再思考一下。第二個是董事長提到現在採購法不足問題。當然這個問題也不是現在才發生，一直都跟政府採購事處，特別是在資訊類的採購案方面。不過我可以先說明的是針對廠商這個服務優劣部分，其實我們在幾年前就有開始針對資安廠商做評鑑，這個評鑑就是共同契約下的契約，這個共同契約原則上這個契約就是可以讓政府機構可以直接在網站上直接下單，對於採購契約上的名單廠商都可以直接下單很方便政府機關做採購。

那針對這些廠商其實我每年都有做評比。評比其實都會公開，其實所以很多的廠商他們會care我們的評比結果。那另外一個呢，機關現在在寫RFP在開採購規格的時候，其實他們都會把這個當成是一個指標吧。通常應該沒錯嘛？基本上原則上你要進入網路要兩個以上才能可以來投標，所以我想也進而紀錄至少去製造一個良性循環的結果，這個部分我再先說明一下。

另外關於這個清華大學老師特別提到的適任性查核這一塊，這個部分對象主要是受託涉及國家機密部分才會進行這樣的查核，那目前以是適用，當然這也包括涉及國家機密保護法裡面，包含那個法規裡面是講國家機密嚴謹的一個非常受限制的受託範圍，那以我們現在的認知來講的話，設計查核原則上來講的話它會是比較所謂的...如果用一般術語稱良民，通常我們會請你們提供良民證，會針對這個部分去做查核。

但是如果你是回歸到國家機密保護法它裡面還是有它的規定的還是要遵守那邊的規定，原則上是這樣子。那這個涉及到國家機密部分，原則上大概是以國家單位為主啦，一般政府機關來講，可能就一點點，可是不多，因為國安規定就是這樣。

就以我的政府機關裡面其實有所謂的機密等級分級這件事情，國家機密保護法有三級，那一般公務機關叫一般，好像是叫密級，對！密級，我們現在一般公共安全裡面其實對於這個分級都是非常清楚的。

所以這個過程假設你是接觸到某個政府官員，那原則上你就是假設你涉及到是國家機密，原則上就會牽涉到裡面去，大致上實際上作法會是這樣。那請問針對這個子法還有意見的嗎？

國立臺灣科技大學資訊管理系：

剛剛有講到國家機密定義，我們也有國家機密保護法，那還是要遵從機關的認定或者對業務的認定。那業務的認定很難，很難說...譬如說我在這個假設資安處，犯了一個屬於國家機密，那這個處所有的、相關的、有跟他互通的人員等等，你就要製作很多相關可以在那邊查核。這樣實施起來你這樣會牽一髮動全身。

我建議就去把這個在第四條這一邊公務機關本來就會有所謂的屬於剛才那個變議，在原來第三條的監督機關，就回歸到那邊各別去定，不要把行政機關的編修跟那個又夾雜在一起，因為這樣會很難去認定。

我覺得這個在未來施行的時候會很難定！因為如果你是依據原來國家機密保護法裡面的規範，你接觸的人都是要去做，那個和你同坐辦公桌、旁邊的都是要，那影響起來算很大！那如果你是一個機關，那就不一樣！比如這個機關，我是剛剛講的電信局或等等這類所犯的事項，那就按照它裡面的整個組織裡面的規範。

這樣就比較簡單一點，這樣施行起來就比較不會有窒礙的感覺。

主席徐嘉臨副處長：

那，好，還有其他的意見嗎？

親民黨立法原黨團：

主席，還有各位先進，我想確定一件事情就是說，施行細則裡面針對母法第十六條的指定關鍵基礎設施的提供者這個程序你們不做實施規範嗎？所以你的意思是，你們認為要到時候由各目的事業主管機關依照行政程序法的那樣程序或是選用前任沿法條案程序去闢指基礎設施嗎？那這邊也提一個問題喔，那如果說他們用行政程序把這個主用兩個來去處理的時候，那就會有人說那我把..我可以指定我不符，我是不是可以行政救濟？因為去年台灣法學會有辦個公聽會的時候就有提出這個問題出來，那你們在

施行細則你們不做...那.當然我很樂見你們不做這個指令，那就回歸到用行政程序法去處理！對不對，你們自己思考看看，我倒是很樂見，如果你們繼續把程序法我反對，我跟你們說我的意見就是反對！如果你們自己覺這應該回歸行政程序法，謝謝。

主席徐嘉臨副處長：

好，還有第三者意見嗎？好，沒有，那我就先說明一下好了，剛剛老師是建議我們在處理國家機密的部分直接回到軍事機關和警報機關去處理，但是我不確定一般公務機關裡面...

國立臺灣科技大學資訊管理系：

那個叫做業務機密國家機關的公務機關業務機密，那個有特別限制。

主席徐嘉臨副處長：

那不一定，那還是，國家機密的範圍當然行政..我這一份還是可能會有少部分的機關會去接觸到。

國立臺灣科技大學資訊管理系：

那是接觸到是比照軍事，你剛講到那個軍事機構會去辦，但是你這個法理該是要去規範那個主辦的行政人員，那是規範受託業務，是阿，受託者，那邊還有那邊去，那就考慮在執行上，我沒有很特別的強烈的這個概念說這樣ok不ok，我是提供這個建議，那你可以去考慮這樣如果在執行上會不會有很難去推動，是建議您然後它這個法出去的時候你們會去推，然後不是它解釋了之後或者他看完這些，也沒有辦法去推動往下一步去走。

主席徐嘉臨副處長：

好，那我們再來了解一下好了，看還有沒有其他更好的方式，那剛剛那個治棋提的那個就是現在的關鍵基礎設施指定程序，我們會在後面來做個補充，這個程序上的規定，第16條，我們出來最新的版本，就是由中央電視主管機關事業群公務機關民間團體的一些指定，然後提供給主管機關核定，所以原則上就以這個維繫它基本上的程序，剛剛你提到說萬一指定完不對，救濟當然可以，可是回到行政團隊它的所有程序指令這是沒有，那我再斟酌一下有沒有其他問題。

親民黨立法原黨團：

謝謝主席，不好意思，我想你還是不太懂我的意思，就是說你這個指

定原則性的規範並沒有規定說到底要這個細部要怎麼展開什麼之類的，到時候就是各目的事業主管機關方面自己去執行的時候就一定會碰到困擾，是不是，OK阿。

可能就是比如說你們給他比NCC要再指定新的電信業者去做的關鍵基礎設施的時候，他們會不會按照行政程序法上面的規定？好，對不起，我不能夠接受你們這個東西，所以我要求行政公證，對不對，你這個程序沒有規定沒有明確的規定程序要怎麼進行嘛。所以如果是，好，我是這家公司的法務的人員，我當然會重新一切的就是提出我想要一個存款者的一個行政程序的過程嘛，我不是念法律系。

好，讓我講完，好，第二個我還是要重複，再三的重申，有關於細則第五條第11款資通安全業務人員之獎懲及處置這部分要刪掉，因為這不是這個資安計畫的核心嘛。你資安業務人員，我昨天已經有再問過一次了資安業務人員的定義為何，範疇為何，有沒有包含主管？有沒有包含基層工作人員，有沒有包含被委託的廠商，你今天在一個資安計畫裡面，逼著一個人員獎懲到底意義為何，因為其實你沒有違法嘛，公務人員就有公務人員懲戒嘛，子法有子法的規定，業務人員違法的話相信任何一個人在打契約的時候，絕不會把廠商違約的規則全部都寫進去，我相信任何一個機關你跟他們要他們簽訂的契約他們不會給你看的，那你把這個列在這個地方是為了什麼，我看不懂，謝謝。

國立中正大學法學院：

我並不是說要要說明跟代表持不一樣意見，而是反正這個東西我是想改善這個責任管理級分級辦法裡面去提出這個問題來，因為它這個就是說一直覺得資通法可能一個很大的重點會在整理幾分級這件事情上面，應該是上禮拜我正好去南部開一個..它是一個軍校，但他們應該很重視資安問題的研討會，很多與會其他單位的人他們很擔心這件事情，很擔心自己被列入是什麼等級？自己被指定成什麼？來參加的人，從他們出去畢業的到去其他單位工作，像有一個他跟我講他是中山大學裡面的一個研究單位的研究員，但是他承包，他去攬了這些計畫，就是國中小學的一些資安業務，他非常的擔心就一直說，學校這種因為中小學是公立的，因為私立比較少，公立他被納入應該是B級，他一直很希望可不可以不要被納入進去，因為他覺得他被納入進去責任扛不完，所以這個在等級整理辦法裡面它這

是最重要的一件事情就是說我們到底要怎麼去核定他的資安等級？

就我所知道參與這些法令的制定以來，就是說知道困難度分成四個等級，但是這四個等級看起來在這個分級辦法裡面 看起來是事務做分析 這個資安業務涉及到甚麼事務？會不會影響什麼工作或是以事物來分級，但是你看起來這個辦法又是是以機關來分級 所以我一直覺得這個就是會非常的混亂，因為這個機關裡面有的業務可能完全沒有什麼機密性，就我們學校裡面有各種業務，比如就說學生的成績是什麼等級？老師申請出差、出國又是什麼等級？學校有沒有那種規則好壞這又是什麼？會議紀錄是什麼等級？

光一個單位他的事物就有不同性質，然後你到底是要約我去依他的事務確定他的資安等級？還是要以這個機關，這樣子可是我看分級辦法就是覺得，分級辦法就是非常的錯亂這樣子，搞不清楚你們到底是要，以什麼用什麼東西來定他的等級這樣子，像是第三條雖然修很多但看起來就是非常的混亂。主管機關這些都是他們自己來核定自己的等級，然後其他又要主管機關報定他的等級，就以我自己的理解，母法它把很多單位核定為它的目的事業主管機關，經濟部甚麼的，他是那是他們來核定的嗎？是他們來核定自己下面所屬的單位的資安等級嗎？光還沒有談到那個核定的程序，光以甚麼樣的基層來核定就已經是很大的問題了，這個辦法根本沒有解決這個問題我覺得，那這個是呼應剛剛那個立法委員代表提出來的。

主席徐嘉臨副處長：

我還是要回應一下，剛剛治棋講到說施行細則第五條裡面第十一款，資通安全應用人員獎懲機制，這個部分是其實昨天開會已經再講一次了，針對政府機關裡面針對資通安全業務人員獎懲，昨天其實在開會的時候就有特定非公務機關的人員反映說，他們在一般的特定非公務機關裡面，他們可能比較沒有特殊的人員獎懲機制再針對資安領域這邊，這個我同意，我們後續會做調整，但是公共機關裡面要做獎懲這件事情其實是當時在修母法的時候也是因為民意代表的意見我們才把他放進來的，這是我必須先說明的。

那第二個是也因為這樣子我們訂了獎懲辦法，那你就獎懲辦法再回到資安機關裡面，我想其實在用資安的人都非常熟悉，很多的資安問題是在於人而不是在於技術，所以這個人去做好他應該做好他意識的認知。因為

我的管理是非常重要的，所以我才希望這個計劃涵蓋他對把資安的人力怎麼去做，不管是人力還是他管理面上他怎麼去做，包含他的獎懲制度這個是我必須說明的，他的範圍不含委外廠商，我昨天已經講了一次了，我再講一次他沒有委外廠商，他是公務機關裡面的公務人力，這個部份我們再次說明這樣。

另外的是，剛剛有老師回應到資安責任等級這件事情，我大概講一下我的概念是甚麼。這個資安它是從風險的角度來看，今天的機關業務裡面，他有非常高風險的需要去被保護的，這個事情他絕對是列在高的等級，所以他是就這樣的邏輯去分，那我們來看到我們現在的資安責任等級分級辦法裡面，那我們如何去定義他所謂的高、中、低，當然現在的條件是可以被討論的，剛剛在這個會議上我也特別強調，針對如何去分A、B、C、D這個我們還會再去討論，但是我們現在初步至少我們能夠參考國外、國內現在的實務做法裡面，初步擬定出來是按照你的影響程度，換句話說，你今天有一個非常重要的業務，比如說內政的地政系統，他是全國性的系統，他有我們全國性的個資，他當然就需要受到保護，那他的等級就會非常高，所以他必須投入很多的資源去做這樣的保護，所以這是在設計這個資安責任等級的基本概念，這我必須跟各位講一下我們的邏輯跟想法，那當然如果是地方性的，你自己的業務裡面就沒有伺服器也沒有server，沒有所有的資訊服務，其實他的資安責任等級就不會這麼重要，可能就會被編到C或D，所以相對的他所需要的資安保護就不會需要投入很多資源在做這些。

國立中正大學法學院：

可是各機關不同單位會處理到的事務的性質不同，所以他這個機關當他受到上級的機關的指定的時候，是不是要根據他每一個系所，以學校來講單位來講就是，每一個系所的每一個單位、人事室的會計室的，你都要去指定不同的資安等級，這樣你怎麼指定的完？

主席徐嘉臨副處長：

現在公務機關和學校的作法，學校的作法現在是照教育部教育機關統一在處理，那以公務機關的做法來講，那他會列成他是一個核心業務，那核心業務訂出來後再和資通安全維護計畫去做說明，這些後面所需要的維護措施，一定事以這個風險最低的業務為主，但是我跟老師說明一下，一

個機關裡面，雖然有這個業務很重要對不對，不代表其他的機關就不重要，因為我們的網路架構設計會交叉感染，其實這都是要去做的，不是說就就這個機關就我們最重要，搞不好他的跳板可以從這個電腦跳到那個電腦再跳過去啊，必須還是要整體的看這件事情的，至於老師剛剛說學校裡面有這麼多所，實際作業面怎麼做？那這個部份我們會再跟教育部做討論，老實說教育部，教育單位不是現在才施行，他已經施行好一陣子了。

國立中正大學法學院：

我舉例說一下，其他機關，其他機關你可能他的業務好像不是那麼重要，因為它裡面已經是是不是何種單位，像台水他裡面牽扯到什麼公務，那個關鍵基礎設施等級一定要非常的高，但是其他的業務他就不是那個重要，那裡面全部都已經是一般約聘人員和契約人員這樣，那這樣的人事管理就那樣可能到底是什麼等級？還是搞不太清楚。

主席徐嘉臨副處長：

那個老師，我剛剛講那個核心，所以它的水廠管理控制就很的重要，所以他是資安等級是列在A級沒有錯，但是你回到他的控制措施就是它的核心業務，比如說你可以看到我們後面的應辦事項裡面，其實大部分都是針對你的核心系統應該要辦理什麼樣的事情， 所以主要還是會落在你的核心系統上怎樣去做處理。

國立中正大學法學院：

所以如果它有核心的業務是屬於A級，那是不是整個單位全部的，所有的都是A級那樣的，因為等級會牽涉到他訂定怎樣的資安計畫的話。

主席徐嘉臨副處長：

原則上是這樣，因為我剛才提的，比如自來水廠，他這個廠，就是一核心任務， 他就是A級，對。定的就是A 級，對，那A級的保護措施就是他的核心系統，他的核心業務，那妳說其他的人又沒有關係嗎？不一定喔。還要看他裡面的架構設計會不會影響到它的核心業務。

中華資安國際股份有限公司

我是中國科大的資訊學院院長，我要跟教授報告一下 ，其實在作那個教育部的時候，我們有做資產清點，那最重要的是什麼，我想你可能沒有去參與這個的案子，我們去抓資料的時候，我們就發現實際上很多

，像新竹我們有兩個校區，我們有百分之三十二學生在貸款，我跟各位報告一下我們去抓資料的時候，抓到那個戶籍號碼通通都有在學校，最後再做資產清點的時候就發現，個資裡面中間怎樣影響。 像剛剛講的學生資料中間我們就叫老師怎樣，我們會有學生，不瞞你說當資料老師想看的時候，傳給校務的時候，他去把那個成績單竄改掉，它就這樣。常見的，這就是我講的用去識別化的概念，所以我說有些東西資產完之後，你去看你那個關鍵，從風險的角度去看list，你用技術來解決。

我覺得那是OK的，所以我這邊要強調的是說，要看學校有沒有去配合這個落實的做法，我去看了很多學校，真的沒有落實的做法， 那是各個學校要去訂的，那跟各位報告一下，為什麼私立學校很重要，是因為私立學校會講個資如果違反的時候是關誰啊？是關董事長。國立大學關校長，所以我這邊要強調，你要把這個東西告訴他；我們學校要出400萬，董事長出四百萬就把這個落實去做。要不然你不把這件事情講清楚喔，我跟你講喔，通通都有問題喔，這不是這邊的議題，教育部怎麼做喔，所以我再跟各位釐清一下，我清楚學校怎麼做，所以跟教授報告一下，好不好，謝謝。

行政院科技會報辦公室：

我想簡單補充一點，那剛才是集中在資安管理法的實施，事實上所有的機關，今天先說這個部分，不要忘了行政院裡面還有一個叫資通安全會報， 所以那個會報的等於說我們除了這個法的機制以外，行政體系有行政命令的協助，也就是說剛現在有個疑惑就是像資安的A、B、C、D分級，或者某些部會主管機關它的認定，和別的目的事業主管機關鬆緊不同，或者是核心部分的認定和鬆緊差異很大，資通安全會報就會有這種調和的存在，就是說當不同的關鍵基礎設施，不同的事業體系，有這種認定標準不一的時候，安全會報體制應該可以發揮它的功能，就是資通安全管理法這個部分的實施，那我就是建議說就是將來整個政府運作都應該那納進去，整個去運作不是只靠這個法。

主席徐嘉臨副處長：

謝謝這個執秘的補充，那資通安全會報有各個機關的組成，原則上都是資安長的組成，還有幾個地方政府的六都整個資安長都會在裡面，所以這個機關提報資安長裡面會再去做核定，那核定的程序會再去做討論，有

一致性的標準會再討論一個過程，原則就再補充說明一下而已，好，麻煩。

親民黨立法院黨團

我不是要問問題，我是要澄清，剛剛副處長說有民意代表的那件事情，我要再次講一次，在審查會的時候，是民進黨立法委員堅持要把這條放進去，不是在野黨委員，然後，在朝野協商的時候我們有被行政院代表提出第19條可不可被刪除，結果行政代表告訴我們說對民進黨他們對沒辦法交代所以沒辦法刪除，所以這個責任一定要釐清，用詞要精確，謝謝。

主席徐嘉臨副處長：

謝謝補充，謝謝，那請問這個細節還有需要討論的嗎？

理律法律事務所：

我是理律法律事務所李劍非律師，是這樣的我這裡有個小小問題，在施行細則第四條裡面其實這個裡面用詞的問題貫穿了子法的設計，就是它把公務機關和特定非公務機關叫簡稱叫各機關，但是特例非公務機關在母法的定義它是包含了三種，那關鍵基礎設施，那關鍵基礎設施提供者它很多不是機關它是私人的，那這個問題會牽涉到剛剛與會者提出的，比如像細則第五條提供的這個資通安全維護計畫，對於公家機關和私人他是提出這個計畫內容，其實某程度某些設計他的項目應該要是不一樣的。

那在施行細則因為我們全部都叫他機關，這樣會有兩個問題，第一個是他把公家機關和私人機關他所要提供的，所規範內容全部都用相同的方式處理，第二件事情是，這樣的意思是他把私人視為機關的意思嗎？因為私人他畢竟不是機關但是在某些情況下，譬如說公權力委託，或是廣義的行政機關可能會把私人變成機關，那我相信這個施行細則跟其他子法應該沒有這些意思，或是有這些意思也不能只是透過子法用這樣的方式把私人指定是機關，就是這個定義可能，這個簡稱可能要考慮一下說是不是要再做一個修改。

主席徐嘉臨副處長：

好，謝謝，那朱律師是?

國巨律師事務所：

那個延續第四條的委外的部分，我有一個疑問就是說，因為適任行查

核這件事情會不會太過於公版，以至於是說這到底是要目的事業、主管機關那還是私人機關我們還要再定一個，這認定的機制還是，還是一個什麼情形，那這個會不會好像又多了一個標準在，我記得好像在其他地方好像也有出現說，受託機關可能要有備有一些資安管理的證照，是不是在那邊就可以直接處理，還是這兩件事是連在一起的？是說要備有資安證照，還是業務經驗，那這個因為適任他這寫的是抽象，我不曉得寫適任性這三個字是不是足夠，是不是夠清楚的知道，到底要看人家是有證照還是有經驗什麼的認定，那另外一個情況是說，針對那個事故調查的處理機制及改善報告，像金管會他們那邊有針對是說，如果發生重大的個資外洩的情況之下，要有專家快速的回覆意見，去檢視你們改善措施的有效新增然後目的是否有達到，那在第6條這個地方是不是要強調快速行這件事情? 那他有一些限制，那變成是說事故的調查報告，假設是說我們在重大的事件有外部的專家去解釋他的改善措施達到管理的要求，那或許這是可以讓主管機關可以去做查詢的。

主席徐嘉臨副處長：

好，謝謝，那還有沒有在徵詢一個問題。

國立清華大學：

我想呼應的是剛剛那位先生代表他所提出來的有關關鍵基礎設施的指定，以及這個事要由主管機關去核定的程序的問題，的確這個在未來讓法律上的確會產生一些疑慮，到底目的是目的事業機關指定關鍵基礎設施之後，那如果相關業者不符合他就可以直接提起行政救濟，還是說他要等到主管機關、行政院核定之後，才算還是正式的行政處分，所以這個部分的話可能在施行細則需要再改，如果你把規範清楚的話會更好，因為我看施行細則裡面並沒有把相關的程序。

主席徐嘉臨副處長：

所以老師是對行政救濟的時間點有問題嗎？

國立清華大學：

其實也是涉及到程序與目的事業主管機關跟主管機關之間的職權問題，到底最後誰才是有權決定關鍵基礎設施的?

主席徐嘉臨副處長：

等到核定之後，原則上等到核定之後。

國立清華大學：

對，但是在你們的那個新的資通安全管理法的第三條第七款裡面，他有去講到說就是，對不起是第八款，關鍵基礎設施提供者是必須經由中央目的事業主管機關指定，並報主管機關核定，所以指定的時候就可以產生法律效果了，還是？

主席徐嘉臨副處長：

核定，他們在最終的是那個核定，他的程序是他先指定再報各主管機關核定。

國立清華大學：

對，我的意思是指這個部分的話.可能要，我建議是把他要再寫清楚，因為其實對於因為坦白說被指定為基礎設施者，他其實對他來講就是肩負著更多的義務。

主席徐嘉臨副處長：

所以老師的建議是在這樣的程序上行政救濟時他的時間點， ok。

國立清華大學：

也就是因為這個程序，是先經過了指定程序後才彙報，是不是能在指定程序之前，譬如說如果目的事業主管機關知道說這可能就已經給相關的事業單位，就給他們一些陳述的機會，已經開始在進行行政程序的流程，舉行聽證，還是什麼，還是這件事情要等到報給主管機關核定之前才舉辦？這些程序。

主席徐嘉臨副處長：

好，我回去先看一下行政程序法，看是不是有規定，我再看一下好了，那我就先說明一下這個，剛剛理律法律事務所提到這個到底是要不要用「機關」這個名字是，因為在這個子法裡面其實他就是公務機關跟特定非公務機關 ，但是到後面每一次都要講公務機關跟特務非公務機關有點太冗長，所以在第四條裡面他有簡稱各機關，所以原則上是這樣，那，如果有更好的名字去取代，這可以再思考一下，我們會再想一下，這個我們也想過，但這實在是很難找到另一個代名詞。那另外一個是你剛剛提到第五條，剛剛確實是因為這是各機關應該要遵守的，應有的內容是這樣沒有錯

，但是我剛剛也有強調，昨天我們在這個座談會的時候一堆公務機關認為，他們比較不適合用這樣的獎懲機制，他會有另外一個公司的制度，所以跟我們公務人員可能會有點不太一樣，所以這個未來可能會分開，目前還是會這樣的處理。

那第二個是剛剛朱律師提到，適任性查核，可能是針對這個還不是那麼的明確，那在原則上它的意義是，很多的這個委外受委託任務的人他其實是屬於敏感資訊，也是在政府機關，那是不是能夠做好他應該保密的義務或是認為其他的事情，是不是需要做一些確定，針對他們人為上的一些處理，原則上這樣的一個制度其實在國外是真的有這樣的制度在執行，我們只是希望各位能夠把它回到，回到透過適任性這個字 但是你說怎麼去…

國巨律師事務所：

我講是依照這個第5條第2項他是有一個項目，可以收集與工作無關的隱私、資訊，所以說你施行細則你寫了一個適合性查核，是代表我可以調所有的資料出來，他是可能會有牴觸的可能性，畢竟受託機關都可能是民間業者居多啦，那假設今天你要的是叫良民證，或者是要他的身家，那些的身世調查，這個時候可能就會形成是說，會不會反而會有違反母法授權的疑慮。

所以我覺得如果真的要做適任性查核，要不要就把適任性這件事情，這個它的範圍是甚麼，看是要查良民證，我講以保全業為例，保全業你要去調任何資料，他是寫在母法裡面去講，他在調閱的時候是不會有個資的問題，個資所以變成是說，假設是我講忠誠調查這件事情，是你在執行國家機密的關鍵的時候是重要的，那是不是要在國家機密那裡去講這件事情還是在這邊講? 不然你那個適任性查核這件事可能會是說，他一來是沒有辦法救濟，二來是他可能會變得非常不確定，以至於你要管制的目的，會成為人家叫做藉口，覺得這個地方可以再做個參考的地方。

主席徐嘉臨副處長：

好，謝謝，針對這個他的名詞，希望我們都在把它做一個比較明確的定義，我們回去討論思考一下，

法務部：

主席，各位先進，您好，關於第十六條這個程序核定和行政法合併的

問題，那我想母法在第十六條，就是說關於這個部分被指定的機關，它在合併之後才會，再通知之後才會被指定，所以當時在指定之前其實這個部分，這個機關它是在未確定的狀態，所以這個部分竟然它在未確定狀態，大概很難認定它是行政救濟的主體，這個部分如果說，當然這個部分也許事後業務單位他們有另外的討論。它在子法要再做更明確的規定會再協助。那在你以行政救濟而言，它還會被核定，還會確定是被行政處分的對象之前，我想這部份可能暫時沒有行政救濟的問題。

剛剛老師有提到聽證，是民法第107條的備註，是要舉行聽證計畫是是在法規有明定？或是行政機關決定它們要聽證的情形？ 如果說今天聽證程序經過業務單位需要他們要訂在法規裡，當然我們還會認為這個法規是確實具體明確授權的情形，那當然如果說主管機關是用個案決定，這個案子是不是要經過聽證，是否是他們進行核定之前的行政程序問題？所以是不是一定要在施行細則裡面去擬定一個聽證或者是就這一部分的程序部分，我們可以協助討論。 那至於說我想一個行政處分的不管在母法的第三條和第十六條已經寫：其實就是經過行政院核定，才有被通知公務機關，所以這個我想核定的部分應該是以行政救濟來看，可看來已經無法判斷這麼明確。

國立清華大學：

因為這個部分應該已經涉指定跟核定，但是如果說怕日後有其他廠商的部分話，但我建議還是要把它寫清楚。因為如果說當時是整個報主管機關核定的話，其實之前就不太適合用指定，或者已經通過，所以對那些也什麼大影響。

主席徐嘉臨副處長：

這個用詞的問題。

崇錦法律事務所：

主席，報告一下，我是崇錦法律事務所曾律師，那個其實這個議題上次我們在電腦公會的時候就已經有提出過，我一直很好奇大家琢磨在行政處分出現的時間點，就是你核定這個時候我們才可以救濟，但是在遵守法律的業者這邊的角色或是人民角色來看，我想我們比較在乎的是哪一個主管機關比較有能力去判斷我們應該被指定。

就是目的事業主管機關的專業程度事務專業程度和主管機關的專業程度，是不是應該把人民的聲音在指定前就先納入？這是我覺得這是一個比較重要的考量，也就是說我今天有80%的可能性會指定進去，而且有可能80%的可能性會被核定，那我的聲音可不可以在指定前就先進來？那當然呼應一下就是說依法才能舉行聽證或是主管機關或是行政機關覺得適合的時候才可以去聽證，那如果可以的話我們在子法部分納進去，就是說在指定前應舉行聽證，或是陳述意見情況，這個邏輯先被納進去，我被指定我會比較甘願一點。與其事後去訴願，我覺得這也可以解決一部分訴願案件的量，一點意見，謝謝。

法務部：

謝謝你們的意見，我還是強調。那如果這個法性上我們會把提供業務單位，當然舉行聽證都有它的程序，如果說，今天上來如果指定，他不是一個行政處分，這個接受意見的話陳述意見這個絕對有的，所以這個部分是不是需要在施行細則裡面規定到目的事業主管機關需要提供的指令這個部分真的可以再說，但是，可能就不要用聽證這樣子。

崇錦法律事務所：

我不知道，可能是不是可以在指定前就有通知這樣子，你至少有通知讓我知道說我有可能會被指定進去，我覺得這種東西可以讓我們先被知道一下。那通知這是不是一個行政處分，或許可以再討論一下，謝謝。

國際通商法律事務所：

你好，我這裡國際通商法律事務所法余若凡律師，我想就指定這個部分其實我也是有相同的意見。我覺得這個部份到底它是不是有造成一個相關的影響，我相信其實很多時候其實你是需要知道正在指定中，或是在指定的時候，它是需要公司這邊一些相關的information，不然其實它很難知道它到底是不是有這樣的影響？

那我們可以看到說，新加坡他們這邊被指定這個關鍵基礎設施的時候，其實它們有一個程序在核定之前，其實等於說主管機關它今天把它認定這個樣子，為什麼一個關鍵基礎設施，它先通知這個公司，讓公司來陳述就是說，你的認定這個部分，其實有一些部分你是錯誤的，因為其實你並不知道我公司裡面的狀況到底是怎麼樣，你可能只是base on相關的公開資

訊，可是對我們公司來講你的認知可能沒有那麼清楚。

所以它以這樣的一個方式，其實讓公司有人，有一個這樣的機會，去提供相關的資料就是說，其實我不是像你認知我是這樣的影響力，之後它再做一個核定這樣子的狀況，不知道在這個整個程序裡面可能去加入這樣子一個部分，所以我想平常看到那種聽證法那種聽證，通常以一個比較簡單的方式，也就是說相關的資料為什麼你認定它有這樣一個影響機制，業者其實不太清楚說到底是以什麼樣的一個方式，所以在這個的程序裡面有可能再更進一步在核定之前，其實有這樣一個程序可以讓業者去提供相關的資料來做這樣子的認定。

主席徐嘉臨副處長：

我回應一下，在母法第十六條其實已經有，就是剛才比如說剛才這個，各位到說我是不是在它指定之前讓它有陳述的機會？或跟聽更多利害關係人的意見。我們在第十六條其實已經有這個設定，中央目的事業主管機關應於徵詢相關公務機關，民間團體，專家學者意見後，指定關鍵基礎提供者，到期後主管機關核定，所以在他指定之前他就要做這一項相關意見的爭取活動，所以這個在母法裡面已經有規定的。剛剛有幾個律師是說比如說，這個程序，那要不要給它陳述的機會？

我想剛剛我後面這位律師可能比較想著重陳述的事情，我想這個部分，我們再思考看看有沒有辦法，在子法法令說它在這個召集這些公務機關，民間機關團體，專家學者，是不是也可以邀請這個可能潛在的關基礎設施提供者，來做陳述的機會？這個沒有問題。這個在法律上我們可以試著來做這樣的訂定，好不好？好，還有沒有其他？老師，我們這樣子會講不完，好，各位，因為我們必須要Follow我們發言規則，如果沒有問題，我們就要進行下面的子法了。各位法律學者意見都滿寶貴的，我還是要控制時間，謝謝。

華梵大學資訊管理學系：

各位先進等級非常的高， 非常高深的一些解釋， 法律的東西我完全不懂，可是我做了以後，其實這個的問題不一定現在要有答案，今天我們所討論的是關鍵基礎設施還是關鍵資訊基礎設施？ 還是兩個都要包含在內？這個是完全不一樣的東西，它的定義，它的程序等等， 那麼就我個人一些初步的了解，不一定對，因為那資安管理法做了以後比較focus是在

關鍵資訊基礎設施，因為現在關鍵基礎設施這一塊是國土辦現在在handle的，所以是不是在這裡我們先把這幾個東西定義清楚，避免我們到法院要問這什麼東西，當然，就像剛董事長剛講的這只是個原則，我想只是提供給大家做一個參考，先規範清楚清楚，避免大家到時候focus都偏掉的話，今天找大家來的時間都浪費了，謝謝。

主席徐嘉臨副處長：

好，那我們現在接著到下一條資通安全資通責任等級分級辦法草案。

華梵大學資訊管理學系：

這裡面只有一點建議作為參考，不一定堅持要，在資通安全資通責任等級分級辦法草案裡面有提到GCB的部分，然後註明是指公務機關，但是我不知道這樣的想法對不對？如果民間企業承包政府跟專案，他的使用這一個這個設備是不是要符合GCB的要求？

主席徐嘉臨副處長：

那有第二位嗎？

行政院科技會報辦公室：

很多機關都有很多重的資訊系統，資訊系統最核心的部分，現在整個設定比較朝向這個機關的最核心業務和最核心的系統，依照那個部分來做認定，那比方說有一個機關他最核心的部分大約三分之一是A級， 可是其他的三分之二，我比較擔心的部分就是這樣子，其他三分之二的部份，在我們這個分級辦法草案裡面，它其他部分的等級內定有的部分是B級，有的部分是C級，如果以非核心的部分來看，會有B有C嘛，可是我們都把它當作A或者是不清楚界定，很容易讓真正投入的資源浪費。因為你不需要，我想其他的部份也不需要別人來處理也不是C，有的部分可能是B，B的等級的強度，那我是建議這個部分有一部分的說明和處理能夠讓被認定的機關，在非核心的部分的處理的強度也有明確的規範，而不是由他自行認定或處在一個完全灰色的地帶。

主席徐嘉臨副處長：

所以執秘的意思是說非核心的部分還是要一些適度的規範？再重新調整？

行政院科技會報辦公室：

它不知道它是最強的，還是最弱的。

主席徐嘉臨副處長：

OK，好。 那接下來還有嗎？

國立清華大學：

針對這個第三條的部份，第一項行政院應每兩年核定資通安全人員責任等級，新的這一條變成是主管機關？第一個問題就說是當然現在法的修憲行政院都改了主管機關，但是在第二項的時候，還是保留行政院直屬機關。所以這個部分的話要不要整個一併變成主管機關這是第一個問題。

那第二個問題就是說主管機關應每兩年核定自身資通安全責任等級，自己核定自己的責任等級會不會很奇怪？應該就直接用訂定或者制定自身資通安全等級就好。

主席徐嘉臨副處長：

好，好我先統一說明一下，就是剛剛老師提到GCB要不要涵蓋到承包商？好，其實GCB他們現在都按照資通安全管理法，很一套嚴謹針對開發資安設備的一個資安管控的服務模式。原則上我對承包商的專案，還是回到剛剛施行細則的那一條，就是你對委外服務要甚麼安全管理，因為這個你再規定下去其實它的衝擊會滿大。所以我們原則上先不做這樣的處理，因為確實它的衝擊會很大。那執秘這個部分，我回去研擬一下看次要的核心把它們列進去，立法上怎麼去定這樣子。那剛剛那個行政院第三條的這個，行政院可能在第二項的這個部分的，行政院的直屬機關，那個部份還是要行政院，因為它的目標就是行政院的所屬機關，主管機關的這名詞和行政院在這個法規裡面有不同的意義，假設我的主管機關可能換個機關，假設，我只是假設性，那就不是行政院，那只是現在剛好主管機關跟行政院那個東西都是行政院，所以我必須要做替行政院做一個解釋， 一般來講我們行政院是很法當法的主管機關，一般都是不會。但是這個法，原則上是由行政院來當主管機關，所以我再跟法務部說明，但老師的建議剛剛非常好，我們不是自己核定自己，其實可以用行政院制定就好，這個名詞我們可以再來看一下謝謝，好像還有一位。

國立中正大學法學院：

謝謝，也就是說剛才講那個說核定等級那個管理事務性質來定，那我

現在講第三條，這第三條大家看的都覺得非常的混亂，也就是說到底要講什麼，是說接受一個，別人通報來的，我是主管機關的，我自己也要訂自己的資安等級。所以這裡的主管機關是包括資通處？包括各個目的事業主管機關這樣子？

主席徐嘉臨副處長：

不是，這邊講的是，沒關係老師你先說，等一下我一起回應。

國立中正大學法學院：

這一條可能真的要整理一下，就是你們到底要講什麼？看的我們看的混亂的地步，完全不知道它想要講什麼，也就是你可能要依機關的那個等級類別來講，就是說中央級的，中央級的那個機關他們是不是就是認證自己的主管機關？那它們是自己人？不是這個意思？那如果是經濟部時麼那些。

主席徐嘉臨副處長：

那個是上級機關。

國立中正大學法學院：

行政院直屬，就是...

主席徐嘉臨副處長：

沒關係老師，這部分我們再講，如果老師覺得有需要的話。

國立中正大學法學院：

大家都看不懂，完全看不懂這條。

主席徐嘉臨副處長：

因為我們這個指定程序在行施有一段時間，所以過去的模式可能，在那個地方，那個部分。

國立中正大學法學院：

也就是你可能講一次哪些單位或者哪個機關自己去決定自己的資安等級？有哪些單位是必須回報請他的主管機關去核定這樣子，好。

主席徐嘉臨副處長：

意思是原則上行政院，等一下我們講的叫二級機關，部會的部分 行政院一定是自己核定自己的，因為他沒有辦法再往上送，那部會和所屬定完之後會送到主管機關，讓主管機關去做最後的核定，原則上是這樣。

國立中正大學法學院：

可是如果說是那個你說，二級的話，它那下面就是有所屬，那所屬就是送還是一起？

主席徐嘉臨副處長：

二級部會裡面，他們還是要去負擔管理下屬機關的責任。

國立中正大學法學院：：

第三項插那個，就是地方自治機關的，然後再來四項又插總統府，這樣完全，寫條文寫的這麼混亂的狀況。

主席徐嘉臨副處長：

好。

國立中正大學法學院：

就是說把那個哪些人，哪邊機關它是自己訂自己等級的寫在一起，然後那一種自己不能自己訂自己等級的，它必須通報他的上級還是哪個機關核定的那一種寫在一起，需要協助去報的又寫在一種，把它這樣子分類來寫條文人家才會看的懂。

主席徐嘉臨副處長：

好，謝謝老師。

國立中正大學法學院：

另外還有剛剛那個程序要講一下，因為我覺得那個就是說這還是因為還是核定，不是自己核定，可能要送核定的情形，因為它還是會涵蓋到那個非公務的特定機關，所以我還是建議說你要把這個，那個整個資安等級的核定，還是需要那個行政程序，因為光你這樣寫完全看不出是有那個行政程序適用，那可能是非公務機關，它可能還是對你這個還是會有意見。再講最後因為之前有去開一個有一個資工的學者他有去講到那個附表裡面，不是指A級，B級那個，他們提到的那個辦理內容，他們說那個ISO系統，它說那個是是20年前提的標準，這個還是沒有改。

主席徐嘉臨副處長：

ISO27001，它的建議有沒有納入其他的標準。ISO27001現在它還是...

國立中正大學法學院：

就是很久以前的東西，我要講說在A級你好像有提到說這個等級以上的也可以，可是以法律規定的這個角度來看就是說，你不能這樣子，因為

1 你拿了一個最低的，就你再寫了之後還可以更高。可是我是業者的立場我
2 只要遵守這樣的規則就好了。對。這是寫這樣的沒有意義的條文了。
3 主席徐嘉臨副處長：
4 老師是指哪裡有以上的？
5 國立中正大學法學院：
6 就是A級嗎。我好像看到有一個就是它的內容裡面
7 主席徐嘉臨副處長：
8 其他具有同等以上效果，這個是不是？
9 國立中正大學法學院：
10 對...這是第10頁是不是，就是說同等級就要，但是法律他附表子法的
11 部分，用這樣規定會沒有意義的，對
12 主席徐嘉臨副處長：
13 好，謝謝，老師原則上我們就做參考好了。會回去做原則上的調整，
14 還有沒有其他的？
15 國巨律師事務所：
16 我看你們有特別去寫，可是看起來又好像差異性好像不是太大，那有
17 沒有可能參考地方自治，用地方自治組織就把那些縣市主管機關之下或者
18 縣市議會，地方什麼所，什麼區，當地代表全部都還含涉在這裡面去做文
19 字上的處理，被讓文字比較簡化，因為我們有個地方自治法，那它有個地
20 方自治組織，我查一下地方組織就有涵蓋直轄縣市的行政機關，就是直轄
21 縣市的政府跟議會，會不會彙整到行政院去核定，或者被查，好像是特別
22 去區分那個直轄市或是縣市的，還有包括可以報告縣市政府和議會，好像
23 不是差異太大，如果統稱叫做地方自治組織，會不會簡化一點，在那個施
24 行細則上面的說明。
25 主席徐嘉臨副處長：
26 好，謝謝，那就這一點，那還有沒有其他的?剛剛其實地方自治組織
27 其實在其他地方有參考過，但在資通安全按照地方組織，但是地方政府，
28 一級機關二級機關是要匯整所屬的往上送，完整送到母法機關，所以還是
29 你在法上要擬定誰幫誰去送？所以他可能沒辦法說要統稱這樣子，所以初
30 步能夠說明是這樣子，不過我。
31 國巨律師事務所：

因為我從結構上來看好像沒有那麼大的細緻化的區分。

主席徐嘉臨副處長：

好，沒關係，我了解律師的意思。好，我們來回去看一下好了，不要把文字弄得這麼複雜，好，沒有問題。 各位還有意見嗎？如果沒有我們就往下到第三個資通安全事件通報及應變辦法。

崇錦法律事務所：

主席，我是崇錦法律事務所曾律師，那個資通安全事件通報應變辦法草案，就是我想提供一個建議，就是說在這個辦法裡面，有沒有辦法增列一個辦法內的附件，附件就是把通報這個通報單做成一個格式表格化，我會做這樣建議是因為，對於立法上的一個參法指標的教育部有一個通報的實施辦法，那面有把通報格式列出來，我想對於這個執行事務的公務員或者是第一線的通報者來說，能有效通報的馬上通報有效率的方式，一個很好的方式，那因為像資安通報事件的裡面有一個那個告知單格式，那也用勾選表格方式進行，如果能直接列為電子公文的格式讓發現者直接勾選往上通報出去，我覺得對於那個通報的時機點遵循是有幫助的。這個提供給您參考，謝謝。

主席徐嘉臨副處長：

好，謝謝。

理律法律事務所：

我跟剛才剛順著剛剛曾律師的意見，現在應變辦法第十三條然後它這次的增訂有補了說中央機關指定代理通知業務，我看到這一條的時候有一點疑慮，因為按照原本的辦法十三條內容，其實它是在七十二或三十六個小時要完成所有該通知的處理作業，要事後要在那個月內送交調查及處理及改善報告， 現在又加了一個通知業務，然後通知的方式還要由目的事業主管機關指定，按照這個指定是說在每一個地方都要一個地方事先指定好一般通知的內容，還是說如果沒有指定的話，那我辦理這些通知，通知？通知就通知，坦白講我就想到說，通知的方式還有什麼差異，還要每個事業主管機關通知方式的差別，是不是到時候通知完以後還要被主管機關說明，因為既然叫指定又沒有一定指定的方式和內容，那變成主管機關裁量說有怎樣的通知才符合我的要求，那這樣的正當性可能讓我沒有辦法看

到說法規上的程序， 就是這部分想跟副處長說一下，謝謝。

主席徐嘉臨副處長：

好，還有沒有其他的建議？

國立臺灣科技大學資訊管理學系：

這是剛剛提到的問題，在應變的第八頁每一年什麼時候要辦什麼事情，但是如果時間是這樣訂的喔，那一年會發現到說缺少人手，你每年把那個時間是四月跟九月，這樣寫的意思就是其他時間都不需要，我覺得不需要訂那個日期，如果每年至少要幾次，一般我們在做這個規範是說， 訂一個細節至少，我主管認為很重要，要辦個五次！這樣不行，不然說剛好這個業務比如說報稅，報稅是五月是重點期，這個資訊中心可能要在4月辦兩次這樣也可以。

所以有時候不要讓這個機關變成這樣子，第一個業界找不到人手，到時候你就會發現找了一堆，看到不像人手的人手，這個我講的是實話。第二個就是說在這個時間大家要盡力努力的做，就把事情做，我覺得不要訂時間，甚至上級機關，你要規範上級給你所屬單位辦理這些演練的作業，演練自己演我覺得說，演練一定要找外面的演或是以上，演一下你就知道這樣子程度如何，所以我對當然講要怎麼改我沒有意見，我只是覺得你把這個時間訂下來，人手的問題，演練計劃等等，或者你演練的這個範疇怎麼去定義，這個沒有做相關的規範，沒有辦法達到實質的效果。

主席徐嘉臨副處長：

好，謝謝。我先從後面說，剛吳老師提了這個問題，你知道實務上機關都會把東西放在年底前，全部都在年底前這不要我要的目的，其實演練是希望能夠改成它平常能提昇我們的資安意識，所以它其實在你平常日常工作中就要有資安意識，換句話說演練，如果只是，如果是只是演練計畫，讓他年底執行完等於執行完只是...

國立臺灣科技大學資訊管理學系：

不好意思我打斷一下，那你的意思是說你沒有演練計畫，為什麼它到年底它就把它，就好像預算，在機關比如你的主管機關你上級機關放任它可以這樣做，那是你上面的問題，所以我剛剛才說演練是要有計畫性，針對機關的特性你也可以，你有不同的時間點，把年底我們還有預算我們可

以把它花完，你認為這樣是OK的嗎？

對，但是這樣子你在執行上你有沒有發現到人手也會不足，所以你的演練計畫，就是前面你在講你有很多資安分級，包含你的資安演練的計畫，送那個主管機關那邊你自己去核，自己去定，你自己去做檢討，在用這個地方是卡，而不是你告訴他怎麼做，每一年四月大家來做一次，那當然每年四月大家全國做一趟，九月再做一趟，一樣的道理，跟你年底做兩次不是一樣的道理，跟你四月做，那其他時間都不做，你了解我的意思嗎？

我剛提的意思就是我在意的是，你要有plan，要有計畫，你們演練的那個計畫，那個範疇，還有你這個演練的你的主管機關配合你的下屬機關會演練的，要求！我是提這個重點，而不是你要做幾次，你要做什麼議題，你現在做這個什麼電子郵件社交工程演練，我不曉得不知道這個跟資安從我們的技術角度，我們認為主要資安問題不是在這個地方，那個是資安認知，資安意識而已。認知不是演練這種東西，資安議題一定要找陳董，找一些hitcon這種，查一下那才是真的資安議題。

主席徐嘉臨副處長：

我跟老師說明一下老師剛剛講那個，演練演練課程是有不同的程式，

國立臺灣科技大學資訊管理學系：

是阿。

主席徐嘉臨副處長：

我們在這個法條其實有寫主管機關，我們必需要做演練，就個是老師剛提的，行政院我們實際上現在做完也是這樣，行政院每年本來都會做攻防演練，老師也清楚我們對課程觀察都會做攻防演練，但是我們會做比如特別關鍵業務的或未來基礎設施部分的我們也會做情境演練，這個方案是行之有年，所以這是屬於大型的可能需要跨很多機關部門，甚至每個關鍵基礎設施的主管或是中央目的主管機關甚至是上級主管機關都要一起來參與，那整個大概就是用比較國際型發生的資安事件來去作情境模擬來去演練他們的程序，這是在法律是有規範的，這是我們的角色，那另一個是部會管理所屬機關，所以它也有它的角色，這一條是在管制這個東西。

國立臺灣科技大學資訊管理學系：

是，我知道，我理解。 所以我才說這個，你要底下規範每一個，規

範到市公所都要去做？市公所演練是什麼時候年底還剩一些錢，我們找人來演一下社交工程，我覺得這沒有效果，你懂我意思嗎？就是說它演練是需要有plan，當然各不同的層級的機關，它要滿足的資安等級要求不一樣。你應該是要從那個管理的角度，我記得我以前在談論資安管理只用八個字在談這個論題，就是你要第一步管理，你要高度自治，什麼是第一步管理，就是你訂的很多大原則從你的主管機關，對於你plan的工作，你現在是好像是要把從上面的這個機關每個人都要做業務性的工作，做到三級機關做到四級機關去，人手真的會不足，我覺得這樣不是一個組織運作有效的方法，組織運作有效的方法是；你上面會訂立很多的政策，達成的標的，讓他就從上一直分流下來，如果你從上面就要開始規範到三級機關，甚至四級機關。

未來要怎麼去運作我想，相信這個一定會很亂，你們會覺得很累。以後也沒人願意去扛說，我今天去擔任這個資安工作人員，為什麼？最後壞的都換到我。你懂嗎？你所有責任的歸屬到最後都是所有資安的，都是資安業務做的，不是資訊人員，不管他是什麼資訊背景，所以我，這個還是不要那麼的去談到細度，你要從規劃的角度去對他有要求，跟規範和管理，這樣就ok了，以上。

主席徐嘉臨副處長：

好，謝謝老師的建議，那我想。

元培醫事科技大學資訊管理系：

吳老師，不好意思我想提問這個第八條第二項：作業內容「得」，「得」的意思就是option，所以它裡面，它把第二項的第一款，第二款，其實寫這個計劃很難，那你不寫它又不知道要做什麼，前面第二項第三款有提到必要，它的前面的施行細則，所以我個人同意用這樣做，在基層好像比較好做，那剛才吳教授也有提到它可以請那個機關一起做，所以能不能加兩個字？把那個第二項第1款的至少，至少一次，用「得」的，有寫比沒有寫好，我的個人意見。

主席徐嘉臨副處長：

謝謝，好，董事長。

中華資安國際股份有限公司：

我講實務面，我申請這兩個自然憑證，申請自然憑證只有它會，我們都不會。在辦公室等20幾天，結果他去渡假三天，他也不告訴我。

國立臺灣科技大學資訊管理學系：

休假，渡假他怎麼會告訴你？

中華資安國際股份有限公司：

我要特別強調是說，這時候你們應該是思考，怎麼樣可執行？那不然我最頭痛的事情就是要哪個中央單位來制定？我到現在都不知道中央單位是誰？因為我們經濟需要對不對，我們現在個資法你看他都照他的去玩，可是現在我們的業主因為他們都要外銷，他必須要面對它，你懂嗎？所以我的建議是說，是不是思考一下這個資安管理法真的很重要，但是希望是可執行，不要到時候被轟被罵說不可執行，這我講真的，拜託。

主席徐嘉臨副處長：

資案事件通報，現在已經在處理了，現在已經在執行了，剛剛大家提的問題我充其量就先做這一下解釋這樣，那兩位律師提到通報的表格，公務機關通報的方式是上網通報，所以大概覺得這個表格的必要性我們討論一下，應該是是沒什麼必要，但是一般的特定非公務機關對於它的中央目的事業主管機關需要通報這件事情，這件事情要不要用格式去做表達？我現在想得比較麻煩是說，因為現在每個關鍵基礎設施的領域也不一樣，比如通信領域它電信網路的領域跟金融領域它所要通報一件事情，但通報內容會有點差異，是不是可以通過一致性的表格去登記我不確定，所以可能要再去了解一下再去做思考。法律是不是要把這個執行面的文件附上去，未來修改是否都做去做處理這也在考慮的問題，先做這樣的回應。

通報的方式，通報的方式其實有很多種，有電話，網站，即時通訊這些通通都是通報的方式，所以在這個現在裡面並沒有明確的要你要用哪一種的通報方式，目的是要讓通報機關有它的彈性空間可以去做決定，所以大概是這個樣子。好，再接下來。

國巨律師事務所：

通報的部分，就是剛有老師提到通報部分我們用電子郵件社交工程演練寫在子法裡面，確實是太過於，就是該怎麼說，很累！對，因為未來很多時候都會用電子郵件因為大家可能都是用即時通訊，所以這種情況用含

涉的範圍，應該是只有演練計畫有一個核備管理的機制或辦理追蹤考核的，應該就可以把它去做管理，不會要去針對特定的那個什麼社交工程，電子郵件去做限定，這是一個情形。

第二情形是說因為我剛才有聽到執秘提到是說，我本來以為這個通報應變應該是跟我們現在資安會報，應該兩個會整併在一起，應該不會有建立重複的匯報，匯報應該整個通報就一起指定，只會有一套系統，不會再有另外一套資安會報的情況，因為剛剛執秘有提到說，我們還有一個資安會報，另有一個通報機制，還可以去做行政命令的處理，我想這兩個應該是合在一起的。

所以假設是這種情形的話，我的認知是通報跟應變應該是把以前的行政命令提升授權明令的一個概念，但是這件事情會呈現的差別像剛才副座這邊所提到的的，確實在NCC那邊本來就有一個資安應變的通報機制，那它的資安應變的通報機制以往通報作業的時候，其實有很多的束縛，或者是管理上的一些問題，那我不知道這一次的細則是不是有針對以前通報上的一些問題去做處理？還是單純的只是把它以前的行政程序，把它無法變成一個母法授權的方式做應變？ 這是請教的一個狀況，謝謝。

主席徐嘉臨副處長：

好，那這邊還有沒有意見？

元培醫事科技大學資訊管理系：

報告，我對子法的第9條第10條，我從兩個角度公務機關怎麼來做。第九條通報的內容規範，當然每個人的意見不一樣，到底要不要寫？我說第9條這個樣子，那未來有個參考的範本，那不然們再回溯20年前，公務機關做好的時候，大家都抄，那內容哪有什麼差別？我這邊能不能夠提一個建議是說第9條通報公務機關應變的這個內容，出自哪邊沒有講，我能不能提一下，我去美國，英國有相關的標準機制在所謂的通報、應變的內容我們都可以做個參考，是不是在哪邊補充做個說明？在第九條第十條未來這個支援下去以後公家機關就要做了，那商機一定會出來，商機出來最大的可能是很多資安廠商，可是它這樣沒有一個標準，那以後一定又有爭議，那這個涉及到最後的懲罰，懲罰的部分，所以我是說第9條第10條能不能訂的比較細膩一點，然後細膩用在子法裡面，請不要用補充的附件來，這樣大家以後比較，這未來涉及到諮詢，因為你有沒有通報，你沒有通

報就三百萬，那我們細節作法是哪幾項？這個我是覺得未來，因為涉及到公共面而且一定要處罰它，這個法條能不能做細膩一點，像第十條事件發生之後之復原、鑑識、調查及改善機制，這個機制的話可大可小，可以是十個字，可以一千個字，一萬個字，未來這個部分的話我會希望中央機構能夠協助幫忙我們推動，這個機制是要拿來落實、提昇我們的資安能力，不是來打擊我們公務員，謝謝。

主席徐嘉臨副處長：

好，謝謝。

華梵大學資訊管理學系：

我補充一下，我們現在還在講通報，我們第五項是情資分享，那分享跟通報這兩個是不是有關連性？通報請裡面是不是應該包含的情資分享面，這個情資應該是威脅情資分享，像這些東西是不是可以把他明確的定義出來，這個錯在哪裡？必免到了基層，到了實務那邊，真正執行的時候會有變質，好，謝謝。

主席徐嘉臨副處長：

我先從後面回答上來，就是通報跟情資辦法本來就不一樣，通報它其實講的就是在線上通報這件事情，原則上就是資安事件的通報程序，我知道，但情資分享就是剛講的威脅情資，那我們在情資分享辦法裡面其實有定義，有對分享和對應，相對就是把它區隔開來，這是兩個是不一樣的東西。 那剛有提到那個，老師有提到說這個第9條跟第10條，未來的應變的規範，裡面應該要包含，訂定應變規範。這裡面要有一些國際標準要參考去設計，我想國際標準那應該會非常的細，大概不太適合訂在這邊，但是目前可以做為參考跟指引的，再去做個細部的規劃。那接下來要說的是電子郵件的演練計畫， 這還是回到剛才規範就是比較細，不一定，這件事情，我會回去思考一下，這確實有這樣的問題，搞不好十年後這些就都沒了。 其實我們在公務機關已經都包含進去了。

國立臺灣科技大學資訊管理系：

對阿。演練規劃要有那個完整的演練規劃，OK?

主席徐嘉臨副處長：

好，老師，謝謝。因為這個場地我們只約到12點半，是真的，那我必

須要加速了。請問剛才還有誰要發言？

開南大學資訊管理系：

我這邊跟剛才一樣，因為一個是所謂的通報，另外所謂的就是情資的分享， 那我看完這些法條之後，比較好奇的是，因為我通常通報的時候是用事件類別去做定義，可是實際上通常有資安事件的時候，通常是一個感染途徑的過程，所以其實感染途徑是要比較容易去做分類的，事件其實是被感染大爆發之後群聚的感染事件的行程，所以其實在通報的時候是用事件類別來，因為通報的時候過程需要即時性，發生事件馬上通報，可是後續分析完了這個發生原因之後，應該是一個分析感染途徑的過程，那它感染途徑的過程應該要列入情情資分享的部分，然後那些感染途徑過程應該要列出來設備上面哪些風險點上面？哪些是軟體上面風險關鍵點？直接給相關的廠商，然後做相關的申請計畫。

那這是所謂通報出來之後，知道的攻擊的途徑之後，那時到該做自動化的分析跟攻擊的策略，而這些演練的過程不應該是等到每年的年底，或者是每個一陣子才去做這個自動化的，每年才去做風險的分析，而是應該做全自動化的依據的風險點之後，其實我覺得國家應該可以有單位負責專門去做資通安全通報層級的單位的風險點，那個自動產生的過程，那這個過程產生了以後，其實並不是要去懲罰任何一個廠商，而是就算當是一個腸病毒的爆發的時候，你可以在家自主管理，你也可以就是先知道這個說傳染途徑之後，你可以做各個落點的分析，那這個部分我相信都可以產生的話，應該會造成實際上的資安法通過之後，會對整個國家的資安的這個效果是會產生，而不是只是每個人覺得有法之後依定要遵循，因為實際上因為機器跟機械之間的工作工程遠遠比人類的溝通效率差很多，那我當初我覺得定這個法就沒有什麼意義。

主席徐嘉臨副處長：

好，謝謝。就先到這邊，因為等一下還有其他，謝謝老師提的這個意見，其實這個，確實本來現在就有在運作，我先說明一下為什麼通報這個個第一個時間是很快速的，所以必須一下子發生資安事件馬上就要通報，通報之後呢，你必須開始做你的損壞，好，一致，因為病毒感染或者是操作攻擊的去做損害管制，做損害管制之後，你就要接下來就是開始找出你的原因，那這幾個步驟其實就是在講一般事件處理面幾個主要的一個步驟

，我是這麼粗略的這樣講，在這個步驟裡面這個，一般的公務機關跟主管機關的角色是什麼，應該是事件發生就要通報這是第一個，後續當然它可能在資安系統需要做個提升，那就再續報，再往上提昇。

接下來呢，必須規定處理完這個損害控制之後，接下來他就要提他的改善報告，改善報告就是後面你要去建置完成；針對比如說這個攻擊來源攻擊手法，感染途徑是什麼，去做一個解釋跟檢討，接下來要針對這個為什麼會被感染，會被攻擊，會被入侵，這樣的改善報告，在這個法裡也有明確的規定。

所以這就不必就是在現在我們這個資安事件通報辦法裡面都有做規定，它整個這個辦法的主要邏輯和訂的主要規範內容是這樣子。你剛剛有提到是說，未來是這些資訊 之後會做分享，情資分享，沒錯，其實在資安的情資分享辦法裡面，當某一個機關假設 他是被攻擊，其實就要到情資分享的管道 去通知其他的公務機關，某個公務機關有一個落點遭到這樣做，你們收到的情資就要趕快做因應，這是情資分享簡單的目的。大概是這樣子。當然這兩個子法是相輔相成的，大概是這個樣子，不知道那還有問題嗎？

開南大學資訊管理系：

那有幾種是比較偏後面的傳染途徑的過程？那事實上傳染途徑每一個被傳染的弱點每一部分不一定每一定都會相同，讓我覺得其實事件歸事件，因為事件會變成新聞，傳染的過程實際上可能是真正的重要的部分，因為傳來的部分後面會有設備的弱點，有軟體要升級的部分，一定是它有相關的這些漏洞會再造成一個風險的發生，而且這個東西出去之後，我覺得國家可能要有一個單位，像教育部現在沒有弱點分析的單位，但教育部有事件異常的通報單位，那所以，因為說我一直覺得覺得少一段，整個國家在做這一段的時候少了一段就是我們都會知道我們被攻擊了，因為教育部會通報，但是教育部不會告訴我們說你們可能哪裡有問題，那實際上在開始在ISO 27001做資訊攻防演練的時候，攻防演練的時候其實我們會做，但是我們自己本身只按造我們自己知道的專業等級在做，那實際上就是少一塊。

主席徐嘉臨副處長：

OK，我了解你的問題，原則上是這個樣子，機關自己發生資安事件一

定是有事件才會去追究，往回追溯他的來源或者攻擊方式，這個原則上是要主管機關 每個公務機關或特定非公務機關，它必須自己要能夠這樣做，因為這個對象非常多一定要這樣子自己做，但母法裡面有規定一條行政院「得」提供協助，換句話說行政院主管機關它會提供協助，那目前運作機制來講，是這樣子沒錯。政府機關果如果發生資安事件，他們都會做第一層級的處理，甚至做後續的鑑識，或者委外服務這樣子，但是他沒有辦法達到這個的時候，他會向上求援，到行政院那邊，那我們可以協助他們去做建置，原則上現在的機制是有的，所以現在跟老師說做一下回應。

國立臺灣大學管理學院：

我還有一個問題，現在這個資安問題已經不是只有行政上說，你被攻了會是怎麼樣？我是覺得說我們在向上求證也沒有什麼辦法來解決問題，我贊同剛剛吳教授這邊說的，每次都修補不完，那每次我們的行政單位要看文字來決定，重點方法要有依據，從源頭開始就是說，現在的安全管理最大的方法就是說，所有台灣人管得到的，我們政府管得到的，任何人不能拿個植入程式到我的電腦裡去，這我們台灣法律規定我們就比較好管，不然你再怎麼管也沒用，因為你電腦被人家被人家植入很多程式，任何公司都可能盜，甚麼管制都沒有。公家機關比較好，反正出事就大家都看你，私立機關就很慘，就是出事它也不負責，要怎麼玩，所以說任何人不能隨便支付給人家，你家不能給人家跑,那個法令在憲法應該要有它的基本要求，那個中華民族那個地方有任何交流的地方都不能來跟我蒐集資料！那什麼意思？那你到網路上弄個爬文程式，你辦法找，因為我們本來就不可以給你看，你讀不到資料。你們只要誰進去，你們都是侵犯，因為什麼事？因為保護外面的人，所以，現在狀態就是說，我們應該放進所有的人，責任就不會這麼多，因為被安全侵入這件事情，大家都維持穩定的，所以我們應該輕鬆一點，讓每一個人壓力少一點， 出事找專家。希望這樣法令可以改少一點，不然搭配的快死掉了，我只能建議這樣。

主席徐嘉臨副處長：

我們當然也希望駭客少一點這樣，但是回到剛剛 。

元培醫事科技大學資訊管理系：

怎麼可能！那很多公司不能生存，駭客。

主席徐嘉臨副處長：

原則上現在的刑法第36章就已經在規範網路上的攻擊行為，其實現在已經有一些行政的規範。好，我們要趕快去辦理接到第四章手續，一定要趕快 ，接下來我們第四個特定非公務機關資通安全維護計畫實施情形稽核辦法。

主席徐嘉臨副處長：

第四個 我們這次的內容主要就是增加稽核的組成，稽核小組的組成和迴避原。

國立中正大學法學院：

當初的檢查拿掉， 這個公務稽核這個措施，有沒有強制性？

主席徐嘉臨副處長：

什麼意思？

國立中正大學法學院：

之前它會有那些強制性檢查，可是你現在這個稽核的話…

主席徐嘉臨副處長：

老師就這個意見嗎？在母法裡的規定是中央，不管你中央機關。中央目的事業主管機關本來就是會稽核，那我們現在其實也一直是這樣做，那因為公共安全部分就是中央目的事業主管機關是「應」稽核，主管機關是稽核，在母法是這樣的部分。後續這部份我們再釐清，好不好？那我們會請我們法務部，請問各位這邊還有沒有？

國立交通大學科技法律研究所：

第5條第5項關於 稽核小組成員應該主動就下列主管機關，那按他第一項提到說，受稽核的機關財產上利益之利害關係者，這個部分我是覺得範圍怕過於抽象，比如說，我今天購買了某一個機關的股票 它可能是就是比如說財務上的利益，他有多大？才構成他的事由？我覺得這個是要去根據母法的釐清，因為財產的利害關係可大可小，很小的利害關係其實不見得會構成事由，但是標準如果不清楚，多少錢下定，才需要受到財產法保護，現在講到的利害關係，是什麼樣的業務？比較難想像 盡可能加註明，謝謝。

主席徐嘉臨副處長：

OK，謝謝 還有其他的專家要給我們意見的嗎？

親民黨立法院黨團：

主席，我只是要問延續問題的一致性，就是我幾句淺白的話來講，第四條有要求主管機關通過稽核的辦法對不對，那第十六條第六項有說目的事業主管機關對於關鍵基礎設施，他去訂立一個稽核辦法，這是一個應辦事項嗎？那到底目的事業主管機關他要不要訂？

第二個，它定的體制要絕對參考？因為它定的那個地方沒有第七條那個，那以後個目的主管機關它的法制定作業是怎樣？是要送給你們核定嗎？還是他自己做就算？沒關係，你可以晚點回答我，這個問題可以再討論很久。

主席徐嘉臨副處長：

好。母法第十六條跟十七條最後一項，針對他們中央目的事業主管機關的資通安全維護計畫他們實施的情形，然後稽核的頻率、內容、方法報告主管機關核定，所以它還是要訂定後核定，對，原則上這在法理面就有規定了。

發言人十三：

你只是在解釋後面法制作業程序的問題。

主席徐嘉臨副處長：

這就是。

發言人十三：

對，我知道我知道， 你在討論的是後面法制作業程序的問題，但是，那個要另外再訂一個子法，顯然要嘛，對，沒關係。

關於這個內容的話，我們下午再討論好了。

主席徐嘉臨副處長：

那接下來，還有沒有意見？那剛剛那個老師說的是裁定大小是不是可以依國外標準訂定一個數字？這個我們這個再來考量看看好了。因為這個又是另外一個學問了。我們可能需要時間來思考一下，好，那大概就先針對這兩個問題我先做一下回應，還有其他的嗎？就到，那我們就兩個一起好了：資安安全請辭分享辦法跟公務機關所屬人員資通安全事項獎懲辦法草案，好，董事長。

中華資安國際股份有限公司：

第五，第五條，裡面有各機關通辦事項，

主席徐嘉臨副處長：

老師哪個第五條？

中華資安國際股份有限公司：

情資分享，你裡面有安全性檢測，有講網路安全弱點檢測，然後缺針對防護缺乏網路主機程式的弱點，建議修改那個主機跟網路弱點掃描就可以了，就是主機沒有去考量，

主席徐嘉臨副處長：

那你講的是情資的第五條？

中華資安國際股份有限公司：

對，第五項裡面。

主席徐嘉臨副處長：

哪一條第五項？

中華資安國際股份有限公司：

第二條第五項，因為我是寫在去沒有對應，所以我想沒有關係？還有一個就是說，裡面寫的，你看，第一銀行報時候並不是你講的那個，裡面現在有寫說，資安事件發生疏於管控的主機，在經由內往橫向入侵，所以我現在意思是說，是不是不見得是核心系統？因為現在資安事件變成串接在一起，所以我的意思是說是不是將所有系統弱點掃描，因為像第一銀行他其實是透過電話錄音主機做跳板跳進去的，可是按照你的核心它並不是。你懂我意思？因為他們現在都是用橫向在串的，我是說所以建議這邊稍微注意一下。那剩下的部分是寫在那建議上面，好嗎？

主席徐嘉臨副處長：

好，謝謝，朱老師？

華梵大學資訊管理學系：

這個，我不曉得這裡的開頭可不可以改？假如可以改的話，我建議資通安全情資，應該是個威脅情資，不是一般正常的情資。如果都可以改這一定得改！那第二個談到分享，事實上分享的東西威脅情資，是分成三個，事前、事中、事後都有問題，威脅的事情是事前，那我們不是提到緊急

通報是事後，事情已經發生了，要威脅的東西是事前，是事情已經規定已經發生了。

所以它事實上，資通安全情資分享包含兩件事情。我跟你講你有沒有能力去接受這個東西能不能沒能去Flowed它？發生資安事件，我今天發現剛剛就像董事長講的，你的主機有漏洞發給第一銀行技術人員看到，他不知道是怎麼回事，這次我發台大中文系系辦所，他看了看，沒有一人可以處理這些，今天不是說要真的要訂的那麼細。但是我想要說他是一個威脅的情資，第二個就是在情資分享的第三頁第二列第七條，裡面下面講到說書面傳真，電子郵件，資訊系統或其他適當方式，各位你也聽到我們在講什麼，緊急通報的提到的那些，我想建議的就是，如果可能的話我們可不可以換成我們如果用書面通知的時候，怎麼樣的東西我可以用書面？第二個按照ISAC裡面的分享的話，他有很多細節的東西，那麼這邊簡單講就是說是傭difine出來,就是說我什麼時候東西可以用書面，什麼樣的情形用傳真，什麼樣的東西可以用email ，因為已經知道邏輯，現在就看你們要不要這麼做，回去考慮一下，謝謝。

主席徐嘉臨副處長：

好，謝謝。原則上那個意見我們先帶回去，其實，剛剛老師提到那個情資希望我們後面做個處理，這個我們已經有把他訂在子法理面，就是後續會把這個納進去，那就先這樣那還有沒有其他的。就是下面的第五條第7款的，獎懲辦法，好。

國立中正大學法學院：

就是獎懲辦法裡面就是說像那個記獎的第五條裡面，這個裡面它有講到說辦理通報跟應變，可以被計獎，可是不是他的義務嗎？公務員盡義務還要給它嘉什麼獎？ 這是我覺得有一點一個，要不要這樣子訂？另外就是裡面有提到他主動發現所謂的資通安全的弱點，甚麼入侵之類的，但是當他發現這個這樣他們系統有這些有問題的時候，是不是就意味著說，公務員，他處理資安業務的人，是不是意味著就是說他當初辦理這個業務時是有疏忽的 所以會變成是 應該是要懲罰的。所以這是一體兩面 就是說哪有獎勵他把它講出來他發現這？ 可是當他講出來：有漏洞，他可能會追溯到說當初他去承辦這個業務，採購這樣的系統，它為什麼他不會變成當初是他執行公務在上面他恐怕是有它過失存在，所以反而是要受罰，是

不是要去追他的責任，他會被懲處這樣。

主席徐嘉臨副處長：

OK，好。

國立臺灣科技大學資訊管理系：

按照這樣講，這樣計，如果我刻意要附和這個獎懲辦法，我每次都辦資安講習，所以我一直記嘉獎一直累積，其實我們這個獎，我們都很知道這個獎懲我們都知道用意在什麼的地方？

公務員，你本來就應該執行公務，你為什麼會有獎？第一是因為你工作做的很好，做得很好然後你說為什麼，我本來就是辦這個人事，我本來就是做人事的，但是我做得很好，它的獎這是在你的主管機關裡面對你的「做」來對你做不同的獎項。第二個是，本來這不是你該做的，或著是你做了這件事會影響讓其他的機關。

跟著做來，比如你發現了一個資安的漏洞，你解決了那個問題然後分享了很多的機關，這個獎是這樣你看你們都把什麼什麼記功，那是學校的獎懲或是規則，那已經不是規則，我們訂一個法的時候就是讓大家依據這個法來訂一些規則，你們都把規則定好的話，大家執行下去。所以我覺得在獎這個部分，不需要寫的這麼細，一次、兩次、三次，不用，但是這個「懲」的話，是什麼就是剛剛，這就叫懲罰該你做沒有做 對不對，那懲就是公務機關該你做的你沒有做，應該你負責的你沒有把事情做好，這樣就會應該受到一些懲處，或者你主動利用你的職務之便，這一定是一個很嚴重的問題 你利用你的職務之便，知了這個法，那你又要去犯，這個才要去懲，你說什麼記大過什麼，那個其實因為他符合條件，甚至他那個犯法要送到公務人員懲戒委員會辦理，你知道這個本來就不是你該做的 所以我覺得這個辦法你應該再精簡一點，精簡一點，不用去把那個規則性，把規則性入這個辦法。

主席徐嘉臨副處長：

我同意吳老師的看法，因為訂的這個其實裡面規定還蠻細的，其實只要規定一些原則性，讓我們的工作人員想辦法去做那個精神跟那個原則和那個資安法的原則精神拿出來這就可以了，好，這個部分原則上我們會照這樣。

國立臺灣科技大學資訊管理系：

就像你還抓知法犯法的理由，有民法，有刑法，還有公務人員服務法等等。這類的，都可以去比對相當bases，不需要在這裡再寫，到時候人家還以為有兩個法，對不對？

主席徐嘉臨副處長：

好，謝謝，那還有？時間差不多了。好，那我們今天會議就到這邊，非常謝謝各位老師，還有法律專家給我們意見和建議，謝謝。

司儀：

謝謝各位踴躍的發言，如果有其他的意見要補充的話，再寫在名單上交給工作人員， 謝謝。