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106年7月28日（星期五）上午9時30分
地　　點：臺大醫院國際會議中心402A/B
出席領域：公務機關

【記錄開始】
司儀：
　　資通安全管理法子法草案座談會會議正式開始，敬請主辦單位行政院資通安全處簡處長為我們致辭。
主席簡宏偉處長：
　　大家好，我在想我們9點半開始，大家在這個時間到，我們就在這個時間開始，我覺得這是蠻重要的。
　　第一個，資通安全管理法已經送到立法院審議，是在上個會期快結束的時候送進去的，在這個期間我們做持續的溝通，今天我們這個座談會並不是就是要把子法就定案了，我們是依照現在我們送到立法院那個版本先草擬子法的內容，如果立法院審議的過程有調整的時候，我們子法也會做相對的調整，所以我們今天並不是討論完就定案，我們到時候還是會實際看立法院條文的修訂，再做適當的調整。
　　第二個，今天為什麼我們要會辦這個座談會？我們後面規劃還要再繼續辦包括對關鍵基礎設施提供者、財團法人，甚至有納入這個法的範圍的組織，我們還會再辦更多的座談會，除了聽各界的意見以外，其實也是做一個溝通，因為我們在母法本身有些地方不會寫那麼詳細，所以很多細節的部分我們是在子法中去明定，我們認為透過這個座談會可以跟大家做溝通。
　　今天這場都大家是公務機關，公務機關大家最關心不外乎幾件事：第一個，有沒有人？我們現在明定要有人；第二個，有沒有錢？機關多也希望可以明定。
　　這邊先跟各位做報告，有關人力的部分，我們跟院長報告過，我們希望在4年之內補足500多人，可是怎麼補？我們現在其實是跟教育部、國發會、科技部，未來可能還會跟勞動部一起談，看以後怎麼去補，在跟行政

院報告的過程中是支持這樣一個做法，所以我們接下來是做人力的培植這一塊，這個先跟各位做報告，到時候我們會根據不同等級，譬如A級機關，我們就會擬定專責的資安人力應該有幾人、B級的機關專責的資安人力應該要有幾人？也會有一些過渡的做法。

目前我們規劃的做法大概會先從派駐資安輔導團的到部會的方式來推動，這個部分原則上也是核定的，所以我們母法過了以後就會組成資安輔導團，依照部會的等級，譬如是A級的，資安輔導團就會到A級機關駐點，比如說2個月，詳細的去確認各項的規範都落實；在關鍵基礎設施的主管機關部分也是，我們這邊會派出專人到機關駐點，希望透過這樣的方式，在機關專業人員還沒有補足之前，對機關有助益。

各位也會擔心派人的人到底是什麼樣的人？跟各位做報告，派過去做駐點的輔導團成員我們會做背景查核，確認他符合安全的規範，這些都是我們在母法送出去以後就開始做這些事，所以到時候派出去的人他的資安查核方式都是有經過一定的程序，我們之所以這麼做，其實也是希望到時候到部會去的時候，不要引起部會的質疑到底他有沒有問題？可以看到那些重要的資料？這個部分我們都有注意到，我們在整個人力的部分會透過這樣的方式逐年去增加，這個是人力的部分。

預算的部分，我們從去年成立以後，在政委、科技會報、院長的支持下，我們有爭取一些經費，所以我們有推動資安的旗艦計畫，每年大概有一些經費，我們在這一塊依照我們資安發展方案、資安發展的藍圖，就會邀集各部會，遵行計畫來推動。

至於縣市政府的部分，我們是在前瞻計畫裡面去做地方政府的區域聯防，所以我們是透過這樣的方式逐漸把人跟錢的部分儘量在這幾年內落實，這個是先跟各位做個一個說明。之所以做這些，就是希望在整個資通安全管理法的推動有一個配套，所以有些未必寫在資安管理法或者它的子法中，但是我們會照這樣去做，這個是在整個資安管理法母法推動還有今天子法的討論裡面先跟各位做報告的。

最後還有一個地方先跟各位做說明，因為受到立法院的要求，所以我們舉辦的每一場座談會都會有逐字稿，所以各位講的任何一個字都會做逐字稿公布，因為這個是立法院要求我們要做的，所以請各位在稍候提問的時候，也麻煩先說明一下自己是那一個機關，這樣我們做記錄的時候會比

較清楚，這個是先各位做一個說明的。至於直播的部分，我們沒有做直播，也沒有現場的文字直播，但是會有現場的逐字稿。

接下來我們會請我們同仁先把整個資安管理法的子法還有相關的細節做個背景的介紹，大概10分鐘，之後請大家盡情討論，不知道針對這樣的程序大家有什麼問題？如果有什麼問題，後面有更多的時間大家可以一起討論，感謝大家遠道而來。

司儀：

接下來進行資通安全管理法子法討論之說明，有請行政院行政安全處賴分析師為我們做子法草案的說明。

賴世榮分析師：

謝謝各位機關的代表參與，今天是第一場的子法座談，後續陸續會有6到7場的座談，我們會針對不同對象，包括邀請各會來這邊討論，原則上第一場是政府機關，所以在座全部都是政府機關，大概主要分成母法跟子法的概述，因為之前母法已經有討論過，而且在4月28日已經函送立法院，所以今天整個重點是針對子法的討論，大綱部分就請參閱。

目前子法有分成5項：資通安全管理法施行細則、資通安全責任等級分級辦法、資通安全事件通報及應變辦法、資通安全維護計畫實施情形稽核辦法、資通安全情資分享辦法。

首先我們針對資通安全管理法與子法概述做說明，這是整個資通安全管理法律的架構，主要是針對資通安全的組織、公務機關、非公務機關的資通安全管理、資通安全產業的發展以及針對委外的部分做一個規範。其中這個周圍有關藍字的部分以子法來單獨的規範；其餘黑字的部分，我們會以施行細則做一個補充。

針對施行細則做一個說明，這個施行細則是由我們資通安全管理法母法第22條授權訂定，主要是適用對象的補充規定，因為我們現在資安管理法有排除軍事機關跟情報機關，所以我們在第2條有規定什麼是軍事機關、什麼是情報機關，我們有針對政府捐助的財團法人做一個定義，原則上這個政府捐助的財團法人是參照財團法人法做一個修訂，原則上財團法人法草案目前也是在這個會期（第九屆第二會期）送進立法院，同時對資安管理法做一個審議。

第二個是針對改善報告做一個補充，改善報告主要是稽核後的改善報

告應包含那些項目，還有一個通報應變調查、處理及改善報告。原則上我們改善報告有兩個，一個是稽核資通安全維護計畫之後的改善報告，還有一個是發生資安事件提出的改善報告，我們這邊改善報告有兩類。還有一個針對資通系統、服務委外辦理注意事項。最重要是我們在第6條這邊有針對資通安全維護計畫目前要包含那些內容這邊做一個規範。

之前我們在開座談會的時候，蠻多人在問，資通安全維護計畫我們行政院會提出一個範本嗎？會，我們會針對這個提出一個範本，目前我們針對資通安全管理法跟相關子法我們規劃提出相關的範本，資通安全維護計畫就是其中之一。施行細則也針對行政檢查做一個補充，這個部分是施行細則一個簡要的說明。

接下來是資通安全責任等級分級辦法，原則上現在各位看到的內容跟現行的規定是一致的，各位與會機關都有收到我們8月1日的開會通知，8月1日我們會再針對資安責任等級的應辦事項做一個檢討，所以原則上如果8月1日那天討論完之後會做一個調修，原則上我們子法有關資安責任等級分級相關的內容也會做一個配合的調整。目前資安責任等級分級大概分成A級別、B級、C級、D級，現行是A級、B級、C+跟C，現行C+對應我們這邊就變成C級，現行C級就是對應到子法的D級，大概是這樣子；有關於分級辦法第3條有針對機關、提出的內容跟核定備查機關，後面我們有一個簡報比較清楚說明；第4條到第9條是針對資安責任等級分級的原則，第9條是一些例外的條件；第10條是針對A、B、C、D級的應辦，其他的注意規範是在第1條跟第11條。

這個是我們針對整個分級的方式做一個整理，目前大概是分這個三類：依照第一類來說，行政院每年要提出自身資安責任等級，這個是行政院資訊處來函報行政院核定，行政院是我們由資安會報的幕僚，就是我們資通安全處來做一個簽核。第二類是行政院直屬機關、省政府、直轄市政府等機關，一樣是每年提出自身的資安責任等級，還要提出所屬機關跟所管的非公務機關的資安責任等級，彙送行政院核定。第三類就是總統府、國安會及其他四院的部分，一樣是每年要核定自身的資安責任等級跟所屬機關及所管的非公務機關彙送行政院備查。

這個是分級原則，目前大概分成A級、B級、C級及D級，這個跟現行的做法是一致的，我舉例，像臺北市政府就是歸類在我們的A級；經濟部或

交通部也是歸類在A級的直屬前點之機關；像飛安會原則上按照子法的規定，他應該歸類到A級，但實務上它可能可以適用分級辦法的第9條，可能歸類到C級；如果是臺北市政府的民政局、公務局，在這個表裡面是算在那個區呢？直轄市政府臺北市政府原則上是A級，臺北市政府底下的一級機關像公路局，二級機關像新工處、水利處，這邊就是C級或D級的其他公務機關的部分。當然我們還有一個不分級，像果菜市場，這個有可能適用第9條之後就落在不分級。

第9條這個是我們分級原則的例外條件因素，大概有這5項，涉及外交、國防、財政等一些涉及人民財產部分，這個是我們考慮的因素之一，還有涉及關鍵基礎設施提供者、涉及民生資源等等，原則上我們按照A、B、C、D級原則列等級之後，還有一些例外考慮因素在第9條，可以去調整機關的最終分級。

第三個部分跟各位說明，資通安全事件通報及應變辦法，目前我們這個也是由母法第13條、第17條授權訂定，這邊有針對資安事件的分級，依照它的完整性、機密性分成一到四級，第四級是最嚴重的。資安事件的通報流程以及我們的應變流程、程序的訂定、檢討機制等等。這個是我們資安事件的分級，各位如果看這個子法條文可能不是那麼好看，我們這邊用這個表來跟各位整理，針對整個資安事件的分級，依照機密性、完整性跟可用性來區分成四級，我舉四個例子來跟各位說明，像以非核心業務的資訊洩漏的話，這個其實是第一級；如果非核心業務的資訊遭嚴重的竄改，這個是屬於二級；涉及一般公務機密跟敏感資訊遭竄改，無論嚴重程度，都算是三級；如果是關鍵基礎設施的資通系統，無法在可容忍時間內回覆的話，這個是屬於四級，這個表大概是這樣看，如果各位看法條不清楚的話，以這個表來看可以很清楚做一個對應。

這個是針對公務機關的通報流程做一個規範。我們這邊分成三個區域，一個是公務機關、上級/監督機關、行政院責任區，這三個責任區域。在公務機關的部分，我們在公務機關知悉資安事件的時候，公務機關要在1個小時內向他的上級/監督機關以及行政院做一個通報；上級機關跟監督機關收到這個通報之後，要進行事件等級的審核，審核完畢後也要在1個小時內通知行政院，審核完畢之後，我們要判斷這個所屬機關需不需要上級機關跟監督機關的支援？如果是的話，由上級/監督機關做支援；還要

再判斷，如果上級/監督機關支援不足的話，是否需要行政院協助？他要做一個判斷，如果這邊需要行政院協助，我們這邊接獲申請之後，會做一個審議，協助派人處理資安事件。公務機關在資安事件處理完畢之後，要做兩件事情：一個是結案登錄，一個是做改善報告，大概是這樣，這個是公務機關的部分，其實這個流程已經跟現行的狀況是很一致的。

接下來說明非公務機關的部分，非公務機關的通報流程跟公務機關主要有兩個比較不一樣的地方，在中央目的事業主管機關跟地方政府收到非公務機關通報的時候，他必須做一個判斷，這個事件是不是屬於三、四級？如果是三、四級的話，就要通報行政院；在公務機關的部分，其實無論一、二、三、四級都要通報行政院，這個是第一點比較不一樣的看法。第二個主要在結案登錄，結案登錄是由中央目的事業主管機關跟地方政府幫非公務機關去做結案登錄，這個也是跟公務機關主要的差異，其他的整個流程基本上是跟公務機關的通報內容類似的。

第四個部分，我們針對安全維護計畫實施情形稽核辦法，這個母法第6條授權訂定，主要是針對行政院使用，行政院是針對非公務機關的稽核來做一個規範，一樣有針對稽核內容、稽核的配合事項以及稽核後的辦理事項，原則上在完成這個事項之後，行政院要提出稽核結果報告，受稽機關也要針對這個稽核結果報告提出相對應的改善報告。

我們也把整個稽核的辦法做一個流程，有關行政院的部分，我們每年都會訂定年度的稽核計畫，我們在執行這個稽核的時候，也要在1個月前以書面通知中央目的事業主管機關、地方政府以及受稽機關，機關在收到這個通知之後，也必須協助派人協同稽核。在受稽機關收到這個通知，他也要提出相關的說明跟相關的證明文件。在稽核結束之後，行政院也會提出一個稽核結果報告，我們也會把這個稽核結果報告給受稽機關，受稽機關收到這個稽核結果報告，要針對這個稽核結果報告提出改善報告，也同時給中央目的事業主管機關或者是地方政府。提出改善報告後續他也要針對提出改善報告後面的執行情形，中央目的事業主管機關、地方政府或行政院也要針對後續的改善情形做一個管考，這個是稽核辦法的流程。

最後一個是有關情資分享辦法，是由母法第7條訂定，我們也針對情資分享的對象、情資分享的平臺及相關的注意事項做一個規範。情資分享主要分成兩塊：一個是行政院自行建置的平台；還有一個行政院指定中央

目的事業機關建置平台。分享的情資大概也分成三類：第一個是有關資通事件的情資、第二個是產生資安事件之虞的情資、第三個其他情資。這個分享平臺也有國際合作，另外辦法中還有對情資交流做一個規範。有關三個情資的部分，其中資安事件跟產生資安事件之虞者在第6條第2項做一個規範，如果收到這個情資的話，應考量相關分享的限制，但在時間上原則要立即分享，其他的情資原則上我們應適時公開。其他不是適用本法的非公務機關部分，我們也可以申請加入到由行政院指定的中央目的事業主管機關去做一個分享，這個是情資的部分，以上我針對子法部分做一個簡要的說明，謝謝。

司儀：

感謝賴分析師，在我們場地稍做整理後，即開始進行資通安全管理法子法草案綜合討論。

主席簡宏偉處長：

剛才謝謝世榮針對細部的子法跟大家做一個簡要的說明，相關的資料在先前都有寄給大家，看有什麼的意見，我這邊也有行政法規會的參議跟諮議來一起就法規的部分集體說明，有針對現行的做法提出說明，如果各位有任何意見都歡迎提出來給我們做參考，謝謝。

我們原則上採取三個問題，之後我們再一次的回答，誰先？

國家安全局：

你好，我是國家安全局，針對資通安全管理法施行細則草案第2條，對於軍事機關跟情報機關的這一部分，我們的建議主要是法條文字的調修第2條後段：「所稱情報機關，指於國家情報工作法第3條第1項第1款及第2項規定」，這邊建議在法條上文字「所稱情報機關」後面是「指…規定」，後面應該也是「機關」來做呼應，所以我們建議文字修正為「所稱情報機關，指於國家情報工作法第3條所定義之情報機關即視同情報機關」，以上是國家安全局針對文字調修的部分。

主席簡宏偉處長：

好，謝謝，有沒有第二位有建議的？經濟部。

經濟部：

經濟部第一次發言，這個意見大概在會前有提供給賴科長，我們這邊主要的意見或是疑問，最主要是在資通安全責任等級分級辦法的草案，在

第3條的部分，要提供資安責任等級給行政院核定，我不知道這邊訂的「每年」的用意為何？因為其實對於所管轄公務機關所屬比較多的單位來說，其實每年重新做一次這樣的環節也是一個負擔，我們建議在有機關增設、消滅或者是等級變更時，再來做這件事情。

在第4條的部分，就目前的辦法跟之前的行政規則去對應，辦法是寫得比較簡單，像在關鍵基礎設施的部分，業務涉及關鍵基礎設施，之前我們有提到比較細的部分，想請教的是，這邊的「涉及關鍵基礎設施」的「涉及」是什麼意思？是提供者？還是包含管理者？因為我們如果試著用第4條評定的話，像我們能源局到底是「涉及」？還是落在其他的部分？可能在A級或B級會找不到適用的項目，包括我們的工業局、中小企業處、交通處、管理處等等，其實他們都會有涉及產業，可是他又是一部分的產業，這樣好像不是全國經濟這樣的定義，所以我們在做這樣的事情，變成好像有點模棱兩可，變成不是A就是C了，其實我們也覺得把它放在C，可能沒有那麼適當，沒有一個地方有一個依據去將他們分級很明確的定義下來。

在附表1的部分，有關資通安全的專責人員，附表的部分看起來跟之前行政規則的內容是一樣的，但是之前誠如主席所說的，之前我們對於資安專職人力的部分討論了很久，這個部分還是照著我們討論前的版本去寫，例如我們A級只要配專責2人就好了，而且只是配置專責2人，並沒有「其他」、「至少」等等那些的字眼；像我們之前討論A級是希望應該要配置專職4個人，這個部分其實落差蠻大，在於機關去爭取人力的時候是非常不利的，因為所謂的「專責」只要兼任就好了，我們機關要去跟我們的長官爭取人力的時候，礙於這個規定，反正我們只要2個人兼辦就好了，變成我們很難去做後續的作業，請建議參考。

對於施行細則部分的委外廠商以及非公務機關的查核條件及頻率，後續是不是由各個公務機關跟目的事業主管機關自己訂？這個問題請教。

在資通安全事件通報及應變辦法草案第15條，我們主管機關對於非公務機關的資安事件，必須要提供必要的技術、支援或協助，這個部分到底是要協助到什麼程度？會有一個統一訂定的部分？還是由各公務機關或是中央目的事業主管機關自己去訂？以上問題請教，謝謝。

主席簡宏偉處長：

好，謝謝經濟部，接下來有沒有第三位？

財政部：

財政部這裡有兩個問題請教，第一個問題，在第一級機關應辦事項裡面，在給我們的草案裡面是寫，資通安全職能訓練證書第一機關要有2張，我們同仁是建議維持以前的規定1張，看到今天的簡報資料也是寫1張，所以這邊請確認到底日後要定為2張還是1張？

第二個問題算是文字修正，在資通安全管理法施行細則第4條裡面有寫到一些：「關於本法第6條第3項、第12條第2項、第15條第5項及第16條第2項改善報告」，最後一個「第16條第2項」應該誤植，應該是「第16條第3條」，因為這個比較瑣碎一點，我們會寫成書面意見給你們參考。

主席簡宏偉處長：

謝謝，剛剛有國安局、經濟部、財政部，針對國安局的建議…

張芸參議：

有關於第2條文字的部分，我們說明一下，剛剛也感謝國安局提這樣的建議，說明一些文字的部分為什麼我們沒有寫出「機關」這幾個字？是因為原來國家情報工作法裡面的第3條第1項第1款，就是界定情報機關的定義，它的第2項裡面就是說明「視同情報機關」，所以在條文的文字上我們沒有呈現「機關」2個字。

主席簡宏偉處長：

這樣可以嗎？謝謝。接下來有關經濟部分的意見，世榮這邊可以做回答。

賴世榮分析師：

有關經濟部的意見，林組長前兩天有提供給我，除了現場問題，我這邊也針對她之前提供的來說明回應。有關資安責任等級分級辦法有關業務涉及關鍵基礎設施是否含目的事業主管機關的權責？基本上是以關鍵基礎設施提供者，也就是營運者為主。如果其主管機關，可能會接觸到關鍵基礎設施之重要營運資訊當然也不排除因此列為A級，但如果依第9條規定，認為列為其他等級即可，亦可列為其他等級。

另外在附表的部分，我們目前是寫「專責人員」，經濟部這邊建議是改成「專職人員」，依照我們現在資安管理法母法，其實我們是講「專責」，所以目前我們建議還是維持「專責」。證書相關的規定，指的是機關

內部須有的證書數量，至於為了持有證書所受訓的課程，日後如果符合職能訓練課程的要求，也可能算列職能訓練時數。

經濟部也提出來有關資安管理法施行細則第5條第2款的部分，他們建議如果受託者多半已經具備ISO 27001國際資安證照，也同時提出第三方稽核報告等一些佐證資料，是不是進一步不需要重複稽核？這個部分我們還是建議，雖然對方已經有委託第三方做一個認證，原則上我們資安管理還是要有相關對應的說明，因為我們也要判斷他稽核的頻率來做一個調整。

另外一個是有關資安責任等級分級辦法第4條業務涉及基礎關鍵設施，他們建議可以強化關鍵基礎設施對象各項資安的措施，而非直接將機關列為A級，明訂關鍵基礎設施的定義。這個部分他也提出來，如果是規模不大的診所跟瓦斯行，會不會是未來的規範對象？原則上不會，現在目前資安管理法分成兩塊，一個是公務機關、一個是非公務機關，非公務機關的部分又分成三塊，一個是關鍵基礎設施提供者還有公營事業跟財團法人。經濟部說，如果這些規模不大的診所跟瓦斯行，未來會不會是我們的規範對象？不會，因為如果是規模不大的診所或瓦斯行，就不會落在CI提供者，原則上CI提供者必須由中央目的事業主管機關去指定，然後報行政院核定，規模不大的診所或瓦斯行原則上就不是CI提供者，更不是公營事業，也不是財團法人，所以應該不會有這個問題。

主席簡宏偉處長：

可是我們在規定裡面，其實在B級機關有涉及個資的，譬如診所雖然規模不大，可是它有涉及個資，這樣算不算B級？

賴世榮分析師：

主要看它是不是關鍵基礎設施？它不是關鍵基礎設施就不會落在A級到B級的範圍裡面，因為大家這個一定會常常誤解，我們資安責任等級目前的分級，公務機關當然沒問題，非公務機關的部分，有一些診所、瓦斯行，這些都不會是A、B、C、D的規範範圍，原則上一定要按照我們非公務機關的範圍，CI提供者、公營事業跟財團法人，針對這三類對象做一個分級。

主席簡宏偉處長：

這個部分我補充說明，剛才世榮在講的所謂關鍵基礎設施提供者，其

實以目前來說，我們這個部分是跟國土安全辦公室一起合作，所以其實他那邊有一個列冊，所以是他那邊有一個列冊的才會是所謂關鍵基礎設施提供者，剛才在問假設地方診所、地區性的診所有涉及個資，如果這個診所他並沒有在關鍵基礎設施提供者的名單內，他就不會落入剛才的A、B、C、D級，就沒有這個問題，基本上範圍會取決於在關鍵基礎設施提供者我們有一份名單，這個跟國土處的名單控管列冊內的才是，這個跟大家做一個說明。請問這邊有沒有要補充？

吳啟文高級分析師：

我想補充責任等級這一塊，其實目前在公務機關責任等級這一塊是蠻明確的，第一個，機關的層級；第二個，涉及到的業務；第三個，關鍵基礎設施；第四個，個資。剛剛問的比較多的是非公務機關，特別是CI這一塊，一般非公務機關CI會被列為A級，我剛剛看分級辦法裡面的說明有提到，主要是在維運跟提供這一塊比較會列為A級，這邊有做CI的維運跟提供，這一塊可能各機關比較需要補充，謝謝。

主席簡宏偉處長：

我這邊再補充一個，就是針對剛剛經濟部有提到幾個問題：第一個包括附表專責或專職這一塊，這個部分我們回去再確認一些跟會報分配的數量，讓它一致，另外依照母法的話，這個部分是由行政院訂之，所以專責人員的設置跟專責人員的定義，我們到時候會把「專責人員」的定義定義進去，基本上我們母法是寫「專責人員」，我們在定義把裡面專責人員的定義儘量是以專任為原則，不要兼任，兼任是例外，用這樣的方式，這個也要配合整個推動的期程，所以這也就是為什麼我們當初會寫「專責」，因為如果法過了，大家現在都沒有專職的人員，其實大家就是違法了。也不可能為了請專職的人員，不管他是不是有符合資安人員的要求，立刻就補，其實這個也會造成大家困擾。我們到時候在施行的過程中會再做解釋跟說明，把期程也納進去，因為我認為這樣比較合理，世榮這個部分可能要注意。數量的部分會回到當初跟院會在報告的是一致。

第二個，剛才有提到，受稽的機關或組織本身已經有通過ISO 27001，是不是要再去做稽核？會不會重複稽核的問題？這個取決於第一個，他的等級；第二個，他取得ISO 27001的範圍跟我們認定的核心業務範圍是不是一致？舉例來說，假設一個機關是列為A級，但是ISO 27001只針對機

房，我相信兩者是不能畫上等號的；如果ISO 27001的驗證範圍是全機關，原則上這個就可以接受，這個也是剛才世榮有在提的，它的驗證範圍還有驗證頻率。

第三個，對有些部會可能會有這個情況，關鍵基礎設施提供者數量很多，不可能在一年之內就全部稽核完畢，這個部分我們當初在母法裡面有提到，由主管機關提出資通安全維護計畫，是可以在維護計畫裡面把稽核的頻率還有稽核的時程做詳細的說明，因為這個簽核計畫其實是由主管機關送行政院核定，假設要稽核有100、200個，我們這邊也不會要求一年內執行完畢，這也不可能，我覺得一件事情要讓它實際可行，所以這個事情其實是可以在稽核計畫裡面去做說明；但是如果這個主管機關、主管部會所管轄的機關或組織其實只有10個，那也要分2年，我覺得這個也說不過去，所以這個部分原則上我們是由這個部會他依照實際上的能力、執行的情形來做提報，但是我們這邊會再看過，大概是這樣子。剛才有提到如果有不一致的部分，我們再確認讓它一致，還有再補充嗎？

賴世榮分析師：

財政部的部分有提出兩個，一個是第一級機關應辦事項，應該是1張；另外施行細則的部分，這個是發文出去我就發現錯誤的，不好意思，第4條的「第16條第2項」應該改成「第16條第3項」，這個提醒我，謝謝財政部。

主席簡宏偉處長：

謝謝，接下來？

環保署：

主席、各位長官及各位機關代表，大家早，環保署第一次發言，想就教一些在資安事件通報及應變辦法草案第2條，資通安全事件分成四級，但是好像沒有明確規範屬於個人資料洩漏是第幾級？希望各位再補充說明，或者在這邊明確。就像簡報第14頁只寫到資訊竄改或系統竄改，我會提出這個疑問，因為我們的應用系統發生一個小問題，就是在漏洞上沒有處理好，結果遭外面的搜尋工具把我們個人資料屬於內部使用被收走，而且讓外面的民眾查到，我們雖然在很短的時間把系統都補正、調好，但這個資源已經在外面讓很多透過Bing或其他搜尋引擎處理，我們再要求他，他也處理的比較被動，所以未來在這一塊應該在個人資料去明訂，它是屬於

廠商之間造成後面持續被洩漏，不曉得在整個策略管理上有沒有對應的辦法？以上。

主席簡宏偉處長：

謝謝，接下來那一位？

中央銀行：

主席、各位長官大家好，中央銀行有問題詢問，在資通安全責任等級的各個機關要辦事項裡面有提到核心系統，在另外的資通安全事件通報及應變辦法草案有提到，核心資通系統，請問這兩個草案裡面的「核心系統」跟「核心資通系統」到底是不是一樣的？還是有什麼區別？

主席簡宏偉處長：

謝謝，接下來有沒有第三位？沒有，好，我們先就這兩個問題回答。

賴世榮分析師：

環保署有關個資，原則上各位可以看到我們現在通報應變辦法草案第3款，如果涉及個資的話，我們按照第3款處理：「各機關發生資安事件，有下列各款情形之一者，我們都一律視為三級」，第一個是有關一般公務機密或敏感資訊遭洩漏或竄改，個資可以算是敏感資訊，如果有涉及個資，原則以第三級為考量。

有關中央銀行剛剛提到「核心系統」跟「核心資通系統」，這個應該都是一致的，就是核心系統，以上說明。

主席簡宏偉處長：

我們就把文字統一，看是要「核心系統」還是要「核心資通系統」。剛才環保署還問了一個，如果這個是廠商所造成的，這個部分我們在那一個地方有這樣的規範？

賴世榮分析師：

廠商造成這個部分應該是要由機關來判斷這個是內部造成的還是外部，如果是機關的話，目前這個應該涉及機關的委外管理，這個部分到底是一級還是四級，就由機關自己來判斷。

吳啟文高級分析師：

我再補充說明一下，第一個，針對環保署提的問題，一般個資算敏感資料，敏感資料外洩是算三級資安事件，我想這個很明確。

第二個，有關廠商這一塊，只是一般我們給廠商，不是這個意思嗎？

可不可以再說明一下？

環保署：

對不起，補充報告，內部資料被Google或是Bing把它搜集，搜回他們家，只要上網就可以查到，我們家這一段早就防止了、都改善了，所以他一直在外面讓人家持續找到，就算我們行文通知他，他也置之不理，我們能夠應盡的責任都做了，第一時間或許不是他收走，是我在官網洩漏，後續民眾可以在他的搜尋引擎上找到，被曝露在外。

賴世榮分析師：

可是為什麼會被收走？

環保署：

因為資安上有一個漏洞，在網路上被人家收走。

吳啟文高級分析師：

其實我們有類似的事件，這種情形也可以跟我們做聯繫，如果資安處有管道的話的，如Google、Yahoo我們也儘量去處理，至於案例，其實是跟醫療有關的，一些特種個資，我不曉得別的單位，一般是報三級，我可以報告，如果查得到，一般是報三級事件。

另外剛剛央行提的，一般我們都會統一，「核心系統」跟「核心資通系統」我們再統一，一般是這一塊是談資訊系統分級以後，高等級我們把它訂為「核心系統」，我再做補充說明，謝謝。

主席簡宏偉處長：

好，謝謝，接下來還有那一位？後面那一位，然後接下來中間這一位。

臺南市政府：

臺南市政府資訊中心第一次發言，有關於資安責任等級，目前如果從C+變更變成C，事實上這裡面以現實來看，就是公所，公所這個部分如果變更之後變成C，因為這個責任等級應辦的事項裡面，原則他們是不需要去做ISMS機制的建立跟完成第三方的驗證，這個部分是有增加進來，但是有增加進來的話，其中核心系統至少一項需要通過這個認證，但是在專責能力的部分卻沒有明訂，裡面是寫「如有」，等於並沒有明訂。再來，國際的資安證照這一塊也沒有列進來，這個有一點好像沒有對上的感覺，如果他需要去做ISMS的認證，結果他沒有這樣的證照，這個兩個好像是要搭

配在一起的。

另外A級、B級都要做SOC，這是所謂監控管理機制的建置，這個部分A級、B級都有，在我們剛剛的簡報35頁，C級的部分是沒有勾選，但是在之前提供的附表3裡面，卻是有資通安全監控管理機制的設置，也就是說，SOC事實上是在變更後的C級還是要做，但是這個可能不一致，跟剛剛簡報第35頁，這邊是沒有打勾的，這個部分會有不一致的地方，不曉得那一個為真？可能要再確定一下。

因為以目前的公所發現的狀況，事實上是沒有專責人員的，譬如研考來兼代，等於研考要做研考業務，也要做資訊業務，這樣的狀況，如果未來變更，變成他必須要做ISMS，他又對於資訊的這些認知事實上是相對薄弱，這樣的話又沒有專責人力來支撐這一塊，他又要做SOC，又要做ISMS，等於他具有B或A級的這種水準，這樣的話沒有專責的資訊人員，也沒有辦　法要求獲得國際的證照，這個部分恐怕未來有幾個狀況，也許公所會避開，他們全部都要求列為D級，就是第四個等級，比較符合目前的現況，因為這是原來沒有的，現在變成有了，他們要怎麼去避開這一塊？一種是避開；一種是就是公所原來兼資訊的他可能就會有一些心裡的反彈，可能他就不要兼，這些就變成一些困擾，這個部分可能要因應，以上。

主席簡宏偉處長：

謝謝臺南市政府，接下來該中間那一位。

臺中市政府：

臺中市政府第一次提問，有關於簡報第9頁分級方式，現在有載明「省政府、鄉（鎮、市）公所、直轄市山地原住民區公所、省諮議會及各級地方民意機關…」這些民意機關，請教一下，以後民意機關是由他們自己每年提出嗎？因為目前實務上的做法，如果有資安事件的話，是由我們縣市政府代為審核，但是這一方我們的主管在很多的資訊主管會議上就有提到，我們對這些民意機關沒有一個強制力，所以以本府來說，我們目前的社交工程演練跟資安通報應變演練，我們無法納入他們來演練，這個方面可能以後會是一個問題，謝謝。

主席簡宏偉處長：

謝謝兩位，接下來有沒有第三位？來，中央銀行

中央銀行：

主席、各位長官好，有關於剛才提到，資安等級C級的機關如果要辦理SOC，依我們行裡在推動，基本上如果所屬機關，我們目前因為礙於人力的關係，如果要推動SOC的話，可能也會面臨到有這個問題。

主席簡宏偉處長：

有三個問題，請世榮回答。

賴世榮分析師：

剛才臺南市政府提出的問題，其實都是說簡報跟現行的法規不同的地方，這個我們再檢視之後確認如何調修。

臺中市政府剛剛說的有關一些民意機關，現行是由地方政府協助彙送給行政院，未來如果資安管理法三讀通過的話，未來可能會依照規範辦理，看到簡報第9頁，原則上如果像市議會，就是要由他自己提出來資安責任等級，彙送行政院核定，現在市議會是由市府協助來提報，未來法制化之後，是由市議會或者區域代表會，他們就是一個單獨的機關，自己來提。

吳啟文高級分析師：

我想再補充說明一下，目前我們C級機關是原來C+，最早我們的等級A、B、C、D，為了簡化A、B、C，後來又多一個C+，後來又多一個C，C各位注意一下，下面是表列，但是這些機關第一要具有自行跟委外開發資通系統，而且要設置有伺服器。所以我說明一下，其實不是每個公所都會列到C等級，他還是要這個情節的先決條件後，他才會列到C，這個說明一下，不是所有公所都會列到C級，我想很多公所還是D級，重點是他資通系統有沒有server，這是第一個。

剛剛也提到，目前C級這個規定也是參考之前C+的規定，就是要導入ISMS，因為要做這個事情，我們在訓練這一塊，倒是沒要求有ISMS的證書這一塊，要有這個經驗，我是覺得這一塊訓練部分我們資安處可以再考慮要不要加入，目前我們資安處在推動資安聯防的概念，包括六都帶一些周遭的縣市，我們希望以縣市為單位，去cover他自己所屬的，所以在這一塊的驗證還有包括提的SOC這一塊，我希望可以搭配區聯防的觀念，或者是以縣市政府為核心，去帶動，不是他真的要去做，因為他可能只有一個系統或者核心的地方，去cover到這一塊，我們希望用這樣的做法，不見得每一個一定要去做這樣的事情，我倒是覺得證書那一塊的訓練，我覺得

可以適度的調整，謝謝。

主席簡宏偉處長：

譬如我們在附表3責任分級第7頁這邊，C級的部分我們有提到，資通安全監控管理機制，初次受核定或等級變更後之一年內要完成監控機制的建置，並持續維運。回過頭來問，我們的想法裡面這個部分並不是你要自己建才叫做完成，像我們現在跟六都推動聯防的概念裡面，其實我們就是希望由六都去帶領各自的縣市，縣市也是整合所屬，當然也包括公所，部會我們也是這樣的概念，這個也回答中央銀行這邊講的，你們所屬裡面並不一定他自己要去建SOC，而是你中央銀行要去把他納為你SOC的範圍，我知道這個有，但是我們現在方向上就是這樣推動，這個也配合國發會機房整併，所以其實都是環環相扣。所以在C級裡面要完成這個機制，不一定是C級自己去建這個機制，而是他的上級機關建的SOC機制把他納入，所以是用這樣的機制。包括剛才在說的核心系統要導入ISMS也是一樣，他要導入ISMS，就是你的上級機關要去協助他，而不是上級機關說這個所屬機關要自己去處理，不是這樣。

跟各位說明長期以來我們要推的概念，部會要整合所屬，縣市也是要整合所屬，進一步是縣市的部分我們希望做區域治理，所以我們目前原則上是由六都各自協助周遭的縣市、離島或者是花東地區，六都目前都有提報計畫上來做建置，包括SOC部分的資訊分享，還有包括事件的處理，國發會這邊也有在推動部會機房整併，其實這個都是一起的，長期以來可能部會都是由所屬自己在處理，我們希望現在其實是逐漸去落實以部會為中心。

甚至跟各位報告，整個在GSN的調整上，國發會有發文，在5月底之前DNS改用GSN的DNS，接下來我們會再進一步調整GSN的內網化，這個以前國發會也有在推動，未來的出口其實是透過部會出口，這個我們會跟國發會合作，再進一步去強化，希望把GSN的部分做適度的調整，這樣的好處也是未來在一些公用的資訊系統可以做到私有雲的服務，這都是一步一步配套去推動的。

包括剛剛臺南市跟中央銀行的部分也是一樣，並不是一定就自己去建，可能是他的上級主管機關或者是市府要去做聯防的協助，謝謝，接下來還有那一位？

內政部：

主席各位長官、各位先進大家好，內政部第一次發言，因為內政部預計在8月初的時候會舉辦資通安全通報演練，因為在演練說明會的時候有很多C級機關反映，因為內政部的C級機關大部分都是警察跟消防單位，他們反映他們的資安人力大部分都是兼辦，譬如像這次的資通安全事件通報及應變辦法的草案第4條上面有規定，其實這個跟現在的規定一樣，1個小時內要依上級或監督機關及行政院指定的任何方式進行通報，雖然第4條第2項有說，如果有事故無法為前項通報，可以依其他的適當的方式進行通報，但是因為他們的狀況，只要有特殊的勤務，可能全部的單位人力都會抽乾，所以我們部裡面也沒有辦法去了解到底他們發生什麼事情，他們也沒有辦法去了解他們自己的單位系統發生什麼事情，消防他們兼辦人也是需要出勤務的，針對這個情況，有沒有什麼適當的方法可以協助他們？謝謝。

主席簡宏偉處長：

謝謝，還有沒有第二位？

交通部：

主席、各位長官、各位先進，交通部這邊做第一次發言，剛剛有提到關於資安證照的訓練，這個地方我有一些建議提出來，目前我感覺上好像各單位的資安證照大概都是以ISO 27001 LA證照為主，這個證照取得的方式可能是配合ISMS的認證廠商，由他們去提供這方面的訓練，再去補助三位內部人員取得這個證照，我個人的想法覺得這個證照可能比較偏管理面的，管理面可能對管理制度上有幫助，可能對資安事件發生的時候，要去看一些log或是看封包，可能對單位人員還是沒有辦法去看關於這方面的東西。

我有一點建議，例如由資安處辦一些技術方面的證照訓練，像CEH或是CISSP，這類的證照比較偏技術方面，可能對單位內部的資安能力比較有提升的作用，但是因為這方面的證照在外面來說，可能它的上課費用都蠻高，可能單位也沒有這方面的預算去支應，個人花這個錢他可能也不願意，所以我建議是否可以由資安處類似團體訓練，可能也比較好去請講師，這是我的建議，謝謝。

主席簡宏偉處長：

謝謝，有沒有第三位？後面那一位。

監察院：

各位長官、各位先進大家好，監察院這邊是第一次發言，有關施行細則草案裡面第6條第3款，我不曉得剛剛前面有沒有提過，這邊有提到「配置適當的資通安全專業人員」，我建議還是一樣比照母法，改成「專責人員」應該比較恰當，不然什麼叫資安專業人員？這個可能要定義一下，這個是第一個，。

第二個是我的問題部分，有關第7條的部分，因為大家知道資安人員現在都很辛苦，如果出了事情要寫改善報告，目前條款的第3款是寫要有損害控制跟復原作業之程序，第4款要有事件調查跟處理作業的歷程。我想問一下，損害控制及復原作業的歷程跟第4款裡面事件處理作業的歷程有沒有重複的地方？因為我不想到時候出事情的時候，為了寫符合標題裡面的報告內容，要去生出差不多一樣的東西，這樣可能也不是很好，這個是我問題的部分，可能你們定義有不一樣，這只是我提出來一個問題。

另外有關資通安全責任等級分級辦法草案裡面的第2項有提到：「資通安全責任登記為A級、B級、或C級者，應依照附表5所訂資通系統防護需求分級原則，完成資通系統的分級」，我們看一下附表5，它裡面完全都是文字，都是用非常嚴重或災難性、嚴重性等有限的形容詞來區分高、中、低，因為每個人對這種嚴重的程度的感受不一樣，所以我會建議是不是比照目前的資訊系統分級與資安防護基準作業規定的安全等級設定原則，裡面有提到很多的範例，把這些範例一樣納到附表5裡面，供以後真的有出了事情以後，大家就要按照這個表來區分到底是那一個等級，不然單純從形容詞來看，很難看出等級的區分。

另外，在現行的規定裡面有說，通過ISMS驗證的機關，準用已採行之風險評鑑方法，對照到新的辦法裡面的補充，我在新的辦法裡面好像沒有看到，我建議也是納進去在附表5做註記，如果已經有透過ISMS的，是不是就不用再引用新的辦法來做一次風險等級的分級？以上報告，謝謝。

主席簡宏偉處長：

謝謝，請世榮針對剛才監察院第6、7條的部分，這兩者之間有什麼不同？

賴世榮分析師：

這個我們應該不是專責，是專業人員沒錯，因為其實也包含非公務機關，如果我們用「專責人員」，這個可能會不適當，應該還是維持「專業人員」，因為這個還涉及非公務機關。

第7條第3項我們再確認一下，第7條第3款、第4款的部分，我們再做一個釐清，如果我們討論以後覺得這兩個是一樣的，就把它合併在一起，有關內政部跟交通部的部分請吳高級分析師做回答。

吳啟文高級分析師：

第一個，有關內政部的問題，通報演練這樣C級機關的簽章問題，目前我們在通報應變辦法第4條規定1個小時內要通報，其實我們最近也在檢討這個通報應變的網站這些提報的資料，因為以往在通報的時候，其實對於某些狀況要有適度的掌握，但是有時候1個小時他內掌握程度有限，所以目前我們區別成兩塊，第一個是通報部分可能是你發生的時間，但是事件有分兩種：一種是你主動發生，但是我想這個比較少；大部分是上對下，如果我們上對下，一般他的電腦已經被移清，所以我們希望他至少1個小時內通報，但是只後續對通報結案這一塊，你的處理、損害管制這一塊會要求填的比較細，但是通報的時候會比較簡單，大概是對一些細節我們有做這樣的調整。

一般在通報的時候其實會做初步的處理，你剛剛講協助部分，目前有提供技術資源，他自己要決定要不要技術支援，一般分兩段，一個是我們主管機關、一個是我們資安處的技術中心。所以我們適度去調整這個通報網站的內容，讓通報的工作不會大家覺得很複雜、要填很多的資料，我想C級大概是上對下的通知，這一塊部分可能要特別注意。

第二個，交通部談到資安證照跟證書部分，剛剛談的證照，在我們目前資安責任等級分級的一些作業辦法裡面確實有規定，不是只有ISO 27001有證照，你剛剛談了很多CEH、CISSP都有，所以我們不是只有ISO 27001才是證照，只是目前機關大多都是以那個為主，我也跟你報告，目前我到機關很多都有CEH，但是我們目前主要在推證書這一塊，目前我們雖然有10個課程，但是我們以後會希望用領域別，你是處理那一個領域要具備那一樣證書來發，這一塊反而是我們的重點，我會加強這一塊實作訓練。

比如我們最近辦SSDLC的實作課程，就是教你怎麼去Secure coding，

而且這個課程都是我們自己開發，甚至請老師我們自己來上的，反而那個是我們自己要去加強，而且那個課程是根據政府機關的實務上經驗怎麼去實作，可能是我們的重點。以往我們也開了不少國際證照的課程，其實這一塊處理非常困難，因為還牽涉到考試的問題，我舉例來說，像CISSP考試是事後才考，考試非常貴，這個錢是誰出，我都覺得很爭議，你考過要出給你多少、考不過要出給你多少錢，那個其實我們都處理過，非常困難。所以國際證照後續希望各機關納入你們的訓練，但是我們會對公務人員職能訓練這一塊加強，甚至有領域方面的證書出來，這個一塊是我們需努力的地方。

另外我再補充一個，剛剛監察院談到有關資通系統防護需求分級原則，這一塊的重點是我們希望透過機密性、完整性、可用性去區別資訊系統等級，但是你剛剛談到可以準用ISMS的一些分級，我覺得沒有問題，但是要看ISMS的範圍，範圍有沒有cover到你所有的資訊系統？我們這一塊是所有的資訊系統都要做，但一般ISMS只有做核心系統的風險評估分析，所以你要去看看有沒有cover；如果沒有的話，系統分級還是要做出來，不是只有做你範圍那一塊，但是你可以準用那個方法，我們沒有意見，你自己有一個風險評估方法，你不是CIAL我們沒有意見，但是你還是要全部做出來，以上，謝謝。

主席簡宏偉處長：

謝謝，另外有一個剛才監察院有提到，是不是可以在附表5加範例？其實這個範例我們後來是把它拿掉，因為我們本來加範例的意思是給大家做參考，可是很多機關在通報產生爭議的時候就拿範例來跟我們談這個是屬於還是不屬於。各位也知道，以個資來說，譬如個資洩漏10筆算那一級？可是個資內容本身是不一樣，比如有的洩漏是非常完善的個資，跟他可能部分個資的洩漏要不要算同一等級？或者是特種個資，所以後來為什麼我們在細則裡面把那個範例拿掉？我們本來是希望加一個範例讓大家了解，結果大家變成拿這個範例回過頭來說它是或不是，反而造成困擾。

我們會把嚴重或災難性用形容詞，其實這也是回到剛才監察院所提的，機關本身風險評鑑，既然我們這邊有定義「非常嚴重」或「災難性」等等，在你們導入ISO 27001的時候會有一個風險評鑑的方法，就可以用這樣的方式來對應，我認為這個部分可以給機關做這樣的彈性。如果各位到

最後還是希望我們把範例加回來，我們可以加範例回來，但是我還是要強調，加了範例以後，可能有些機關就會認為只有這個範例才叫這個等級，那反而失去範例的意義，所以這個部分也聽聽看大家的意見，我們自己也會評估要不要把範例加回來，也不希望造成大家的誤導，大概是這樣子。接下來還有那一位？

財政部：

財政部第二次發言，剛剛有同仁提到在責任等級C級機關一般事項裡面，現在是規定要導入ISO 27001以外，還要進行認證，現行C+的公版裡面是說，應該是要有以下核心系統導入ISMS，並沒有說要得到認證，因為我們在現場有討論一下，考量有些機關他的確是有伺服器、有系統，但是他本身沒有資訊人員，比較算特例，我們替他考量，因為他可能也沒仔細看這樣厚厚的一本，他不曉得這個差異性，這邊是不是可以再請資安處再考量一下，而且導入是可以上級機關輔導，但是驗證這件事情的確需要經費，需要比較足夠的支援，可以再討論一下，謝謝。

主席簡宏偉處長：

謝謝，接下來那一位？文化部。

文化部：

主席、各位與會先進大家好，文化部第一次發言，事實上我是一個問題請教跟建議，我們現在資通安全責任等級，不管是A、B、C、D，認為它訂一些應辦事項，覺得是立意良好，但我想說先針對有關於認知跟訓練這一塊制度的構面提一個建議，事實上人對了，事情就對了，所以我們針對我們的人員去做一個資通安全教育訓練的應辦事項，這個立意真的很好，這個應辦事項很好，但是對於我們在執行單位來說，KPI怎麼去做達成的統計對我們來說是困難的，怎麼說呢？比如現在資通安全關於訓練有分兩類：一個是專責人員、一個是一般人員，專責人員畢竟數量少，統計上沒有什麼太大的困難；但針對一般人員來說，我們機關人員晉用種類非常繁多，人員進出很頻繁，這些同仁是不是每個人都有接受3個小時以上的教育訓練？事實上我們每次辦的各項資安課程，他們會不會來？有沒有來？這個統計都非常的累，所以我們每次在開一些資安管理會的時候，我會覺得對於這個KPI達成率非常覺得為難，不曉得其他的機關有沒有這個困境？我們怎麼樣來了解，到底機關內的同仁有沒有每年接受3個小時以上的

教育訓練？如果這件事情是重要的，用什麼樣的統計方式可以達成這個KPI？這是一個問題請教。

第二個問題，專責人員對我們來說就是所謂的資安專業人員，政府機關的資訊人員流動率也很高，我們覺得如果資安就是國安，將來是不是有所謂資安專業人才資料庫？有沒有這樣的統計平臺？讓資安專業人員、資訊人員受過那些資安的專業教育訓練跟證照的取得？在這樣的平臺上是一個開放的資訊，各個政府機關在人員在晉用，請他執行所要的任務的時候，這樣的平臺都可以讓我們取得相關的資訊。所以我們是想有關於人員的訓練，是不是有相關的統計平臺可以讓我們做登錄跟查詢？以上建議。

主席簡宏偉處長：

謝謝文化部，還有沒有第三位？

內政部：

主席、長官、各位先進大家好，內政部第二次發言，因為我們在說明會的時候，警消有熱烈的回應他們的問題，所以很感謝剛剛各位長官的回答，我是想可不可以針對警消在通報部分可以更彈性一些？比如他們如果真的有特殊勤務，只要在事後提出舉證之後，我們可以放寬特點的通報時間？因為他們是反映有時候在特殊勤務的時候，他們真的沒有辦法去看手機，了解到底發生了什麼事情，我們本部這邊因為他們的資訊人力都被抽出去了，我們也沒有辦法了解他們的系統發生了什麼事情，而且未來警政署好像規劃中也沒有要併入本部的資料中心裡面，所以對於這個部分不知道可不可以放寬警消通報的時間？謝謝。

主席簡宏偉處長：

謝謝，這個我先回答，第一個財政部問的驗證部分，我的想法是這樣，即使之後要驗證，有沒有可能在上級機關驗證範圍加入多場域就可以解決了，不一定是他自己要去驗證，納入你的多場域驗證就可以解決了，這個你們再想一想，這個是針對財政部的部分。

文化部的部分，有關你的建議我們可以評估看看，因為我們再跟人事部門這邊討論看看，相關的資料我們再想一下，我們有這樣的想法，可是我們目前並不會優先來做這件事情，未來我們可以考慮看看要不要這樣去處理。

至於應辦事項一般人員部分我再請啟文回答。內政部的部分，基本上

我並沒有那麼贊成所謂的放寬，最近有一個案例，歹徒是用聲東擊西的部分方式，譬如在某個地方製造假事件，讓保全或是警衛跑到那個地方去，原來地方就空了，他就進去偷東西，這個是這兩天的一個新聞，所以我認為這樣的部分，如果照你剛才提的，他可以不用在這樣的時間，會不會到時候有類似的情況？這樣在整體的資安上會不會造成一個漏洞？這個部分現階段我們會認為可能朝不放寬的方式，但是你提到如果有實務上的困難，也許我們跟警政署這邊溝通看看，如果是依照我們向上集中的概念，因為警政署是屬於業務特殊、又有全國性，他是可以設立資訊部門的職權機關，照例說警政署就要去統籌他所屬，就不是由內政部來統籌警政署，這個是當初在組改的時候根據資訊單位的設置原則已經有這樣的規定，所以這個部分也許我們再跟警政署討論看看，有沒有這樣的方式來處理，目前我們比較朝向不放寬的想法。

至於文化部剛才講到應辦事項，那個部分行政院的看法？

吳啟文高級分析師：

我再補充一下剛剛財政部提的問題，因為你剛剛談到C級，我們之前談到是比較C+級，我想回去我們再確認一下，我印象C+好像只有導入，沒有通過驗證，如果確實是這樣的話，我們回去再修正，我剛剛看好像也是沒有通過，我們回去再比對，謝謝你提醒。

第二個，文化部提到認知訓練這一塊，這一塊每個機關做法不太一樣，剛好我有機會受邀去機關作講習，在一般人員部分，其實我去的機關有不同的做法，一般比較不好的，我一去，還沒有到的同仁就改成簽到，我開始講的時候有些同仁很委屈，留下來跑不掉，撐到結束才走，這種情形我是覺得最不好。另外我最近剛好去一個機關，我覺得還不錯，因為我們現在規定，除了講習以外還要做評量，從評量就知道他有沒有來上課，像這次評量機關自己出題，以前是叫我出，出5題是非、5題選擇，甚至我去講習的時候，他們單位還有準備一些紀念品讓我發問。所以我是覺得可以用很多方式來鼓勵同仁參與。

你剛剛提的有關資安人才的資料庫平臺，我們中心確實有這樣的平臺，但是沒有開放機關查詢，所以你們想了解這些同仁有上過什麼課，其實都可以跟我們同仁聯繫，我們確實有keep這樣的資料，從一開始辦理公務人員資安職能規劃的訓練到現在我們都有。只是現在遇到比較大的問題是

機關人員流來流去，譬如原來有一個同仁有1張或2張，他走掉了，這種情形也可以讓我們知道，我們會再安排機會讓他們調訓一下，我想這個機會是比較多，因為我們紀錄裡面可能以為你都通過了，真的有移動可以透過反映，這個部分我們都可以協助，以上，謝謝。

主席簡宏偉處長：

謝謝，還有那一位？監察院。

監察院：

各位長官好，監察院第二次發言，有關資通安全責任等級，A級機關應辦事項裡面第一個，資通系統分級及防護系統裡面有規定，初次受核定或等級變更後之一年內應依附表5完成資通系統分級，並完成附表6之控制設施。我現在的問題想請教，有關完成附表6之控制措施的「完成」定義是什麼？以監察院為例子，我們大概有30到40個資通系統，有是所有的資通系統都必須完成附表6很多的這種安全防護措施嗎？還是高防護需求等級完成就好？這個地方可能請長官給我們一點回答跟建議。

主席簡宏偉處長：

好，謝謝，接下來還有那一位？如果沒有的話，世榮這邊針對監察院所提問題回答。

賴世榮分析師：

我們資安責任等級第一級，現在我們是寫初次受核定或等級變更後一年依附表5完成分級，這個沒有問題，監察院同仁這邊問，是不是要完成附表6的控制措施？目前我們確實是這樣寫，可是目前附表6有臚列這麼多的項目，當然還是按照高中普來去做一個判斷，完成的定義是什麼樣。按照我們專案管理最小權限的大概有3頁這麼多，原則上按照高中普來做一個控制措施的判斷。什麼是「完成」，就是按照我們臚列這麼多項逐一去完成項目，不曉得有沒有回答到你的問題。

監察院：

我這邊補充，很多系統要達到所有高中普裡面所定義的安全防護基準的話，有些是要花錢去改系統的，有些是要花人，如果是自行維護的話，就要投入人力，所以在這個辦法通過以後馬上要適用，我覺得很多機關會有問題，到時候針對資通安全處如果有對我們一些管考的時候，這一項我的回答，我相信很多機關應該都會答「完成」，你打死我都不相信，我不

曉得在座各位先進是不是跟我有同樣的問題？

吳啟文高級分析師：

我說明一下，這項規定是從我們資訊的分層，以資安防護基準作為規定搬過來的，其實那時候是從104年7月開始有這樣規定，我們104年7月推動當初有提到，因為很多系統已經有一段時間，我們是希望第一個，配合新系統開發，系統改版的可以優先做；第二個，涉及到有些管理規定的部分，也可以優先做，但如果涉及到要花很多經費，我們希望是改版以後再做，我們當初有這樣的前提，這裡面的規定其實不是新的規定，他規定高中普有分四大類、29項的規定，這一塊我們也希望逐步來修正，機關達成這個規定，所以我們也辦一個說明會，協助各機關怎麼去提RFP，甚至後續驗收怎麼去確認這些有符合相關的規定，甚至還寫到委外的文件，我們都有這樣的說明，甚至我們最近開課是教你怎麼去實作，特別是針對SSDLC這一塊，這一塊我們會逐步輔導各機關來達成，雖然之前規定已經訂了1、2年的時間，後續配合法可能會更主動、嚴格的要求，但是我們還是會協助各機關逐步完成，以上謝謝。

主席簡宏偉處長：

像這個部分我的想法是這樣，其實在104年就已經有公布，那時候我們想法是在系統更版或是開發的時候就必須要依照這樣逐漸去推，我也理解有些機關的系統沒有那麼快的更版。到時候施行的時候，我的想法是各位可以先去盤點，把時程列出來，有一個很重要的重點，依照風險的管理，那一些是屬於比較高等級的，那一些先處理，之後就是按照這個時程逐項、逐項去做，如果有這樣的時程，我覺得在提報計畫去做更新，或是去做預算的爭取，其實相對就會比較可行，我們實務上看到大概都是用這樣的方式處理的。

接下來？不好意思，因為剛才有一些人比較晚進來，所以我再跟各位做一些說明，對於比較晚進來的，今天各位的發言都有逐字稿，這個逐字稿都會做公開，這個是立法院要求我們必須要有逐字稿，所以在提出問題的時候，可能把你的單位做一個說明，這樣的話，我們在記錄上會比較簡單，謝謝，麻煩。

工程會：

謝謝主席，工程會提供幾點意見，目前之前資通管理的相關法規已經

相當完善，但是就執行面部分我們會遭遇一些問題，想要提出來。現在管理法草案第14條已經有明訂，這些執行的過程中如果有一些故意或過失造成相關違反規定的時候要懲戒或懲處，因為我們現在相關子法項目不多，可是執行的人力，這個可能是每個機關會遭遇的問題，還是可能只有我們工程會遭遇的問題。譬如像目前A級機關要有2個專責人力，目前我們工程會只有5個資訊人員，我們又有很多主要的核心業務在做，所以在實務上、人力的配置上真的是會有困難。

另外像之前推動資安的時候，包含軟硬體升級、很多系統要改寫、要通過ISMS這些的認證等等，就像剛剛主席、各位長官有說了，還需要有預算，我們工程會從103年開始，就有兩個核心系統一直要導入驗證，我們每年編的預算每年都被砍掉，我們會遇到如果像這種要3年內完成，通過第三方驗證，可是事實上因為這種情況而造成無法驗證的時候，實際上執行上會變成我們違反這個規定而受到懲處。在執行上有沒有比較變通的？可能是因為工程會過去一直要組織再造，所以很多委員在看預算的時候，都會認為我們要組織再造了，如果這些執行的過程確實是因為這種預算爭取不到，或實務上真的沒辦法做到的時候，造成執行上的困難，可能會影響到違反規定，我想沒有一個公務人員會希望遇到這種情形。

上次在院裡面開會的時候也有提到，有沒有可能由資管處或是資安處先盤點，或是統一編列一個資安預算，依照各機關來分配，不然有時候在推動一些業務上面，我們業務單位或是我們資訊人員他們確實是會有一些困難，會先反彈，以上也請主席這邊可以納入考量，謝謝。

主席簡宏偉處長：

謝謝，還有沒有其他的建議？沒有？我先直接回答，其實我認為預算資訊部門還是要有爭取的義務，因為我覺得必須要講得出一個道理，通常人家就會願意推動的預算，當然工程會可能有因為主管的關係，但是也不只工程會目前有主管的問題，其他有幾個部會也有，可是這幾個部會這樣的問題好像沒這麼嚴重，他們有爭取一些計畫在處理，這個是我先講的。

第二個，如果到時候真的有問題，我們這邊也會一起想辦法，看怎麼樣必要的協助，但是基本上我並不是那麼認同由資安處或是國發會的資管處爭取一筆預算幫所有的政府機關把這些都做了，其實依照以往的經驗，這樣的效果不會太好。也先提醒大家，這算是我私下的提醒，當我們有經

費的時候，希望大家不要拿到經費就開發新系統，之後沒有錢維運就變成是，提報計畫要維運的經費，我們看到很多的部會都有這樣的情況，到最後系統在那邊，可是沒有維運的經費，變成用計畫的經費來做維運的事情，這個計畫本身的目的是不一樣的，像我們資安處提供的旗艦計畫裡面都要求一件事，提報計畫裡面，必須要把當計畫結束以後要怎麼維運講清楚，譬如六都的前瞻計畫裡面，我們也有加一個，當這個計畫提出來的時候，要把永續營運的做法講出來，列入評分的項目之一，我們的目的就是希望所有的這些系統的開發跟維運想清楚怎麼做，剛才也在講，我們希望做向上集中或做資源整合，目的也在這。其實整個預算就這麼多，如果大家能夠共享，能夠省出來的經費會很多，這時候我們可以去做更好的服務。

再回答剛才工程會另外一個問題，當這個法過的時候，相對也是給你一個依據可以去跟內部爭取這個經費，大概是這樣。還有沒有其他的？各位還有沒有其他的建議？國發會。

國發會：

主席好、各位先進好，國發會第一次提問，有關於資通安全責任等級分級辦法，在這邊有說要每年提出自身或所屬的資安責任等級，不曉得這個部分可不可以說明一下原因？其實在這個分級方式已經定義的非常清楚，像我們本身是A級機關，原則上沒有太大的異動，會是一直維持在A級的部分。

主席簡宏偉處長：

大家知道在資安的推動上其實是PDCA的循環，為什麼我們希望整個在管理法跟相關的細則我們都是抱這樣的概念，也就是說，雖然機關是A級，可是你還是要定期去review自己，包括到你每年應該針對整個情況的變遷、技術的進步，定期做相關的風險的評鑑，也重新檢視自己，這樣才能夠讓整個資安一步一步變好，所以我們才會有這樣的一個想法，雖然可能以國發會來說，你會一直都是A級機關，但是並不表示你不用每年重新去review自己作業的環境有沒有需要調整的，這樣可以嗎？有回答到你的問題嗎？

國發會：

不好意思，再補充說明一下，我想其實大家都會每年review，不管是辦法出來之後，我們要做的事情很多，就算我們依據這個規定做，我相信

大家都是有在做PDCA這一塊，會問這個問題的原因，是因為每年提出就會有一些行政上的程序，我只是在想大家會不會跟我相同的問題。

主席簡宏偉處長：

這個部分我們希望每年提出也是希望去落實這樣的循環，但是如果大家認為這樣的頻率太高，這個我們再想一下看是不是做適度的調整，是不是在一定期限內，不過我們還是會比較期望每年，可能國發會相對的所屬只有一個，可是對有些機關來說，他的所屬可能有很多個，在這種情況之下，每年的循環這個部分我們可以再納入考慮看看，謝謝。

還有沒有其他問題？還有沒有其他問題？還有沒有其他問題，基本上我會問三次，如果沒有其他問題，就代表大家都沒有問題。這個部分我們並不是今天開完座談會以後大家就不可以再提意見，不會的，所以大家如果有任何意見的話，歡迎mail給我們，原則上我們會把會後mail的方式再跟大家做說明，如果各位不介意的話，我有一個想法，大家提的問題是不是也可以公開在網站上？這樣大家也可以知道別人問了什麼問題，還有我們的回答，作成一個類似Q&A這樣子，如果各位不介意的話，我們大概會用這樣的方式，這個先跟各位做說明，如果各位回去有其他的問題，再告訴我們說一聲，再次謝謝大家今天撥空前來，今天非常謝謝各位，你們的意見該修正我們會修正，該納入評估我們會再納入評估，謝謝各位。

司儀：

謝謝各位長官的蒞臨，我們在會議資料裡面有夾一張意見單，如果各位長官對於資通安全管理法這個草案還有其他意見的話，歡迎寫下來交給穿有綠色背心的工作人員，謝謝各位。