資通安全管理法修法說明會（北區第 2 場次）

逐字會議紀錄

時間：109 年 11 月 30 日(星期一) 下午 2 時 30 分

地點：臺北國際會議中心 102 會議室(臺北市信義路五段 1 號)

【主席致詞】(略)

【資通安全管理法施行情形及整體修法重點】(略)

【交流討論】

主席林春吟高級分析師：

待會進行的過程我們主要是針對修法，從母法到 6 個子法逐項討論，詢問看看大家有沒有相關建議或看法？那在正式開始之前，就剛才的簡報，有沒有需要我們再加強說明或有不清楚的地方？。

中華郵政股份有限公司：

主席好，我這裡是中華郵政，想請教我們的內部稽核，是要做到全部單位嗎？因為中華郵政有 2 萬多人，而且全台有 1,300 多個支局，而且我們的資安責任等級是 A 級，那每年要做 2 次，我不太確定這個做法有沒有什麼可以提供參考跟建議的？謝謝。

主席林春吟高級分析師：

好，我們提供其他機關的做法給你們參考，我們強調機關內部稽核，是要全機關去做考量，因為我們發現有一些機關的內部稽核，只稽核資訊單位，那個範圍是不對的，因為資安實施範圍是整個機關，所以在你們要做內部稽核的時候，我們的建議是一樣先全部盤點，就像資訊資產要先盤點一樣，把機關裡面的單位先盤清楚，有的機關會做一些分類，然後有一些單位因為有資通系統，所以被稽核的頻率就比較高，有一些單位因為沒有資通系統，可能比較偏使用者資安作業，那被稽核的頻率會比較少一點，或者可以併機關的內稽內控去處理，那都沒有問題。我們強調的是要整個機關去做一個評估跟考量，然後規劃，尤其是有資通系統的單位，稽核頻率跟沒有資通系統的單位是不太一樣的，並沒有說每一個單位都要每年做 2 次稽核，主要的意思是要全盤的去考量，就像行政院對所屬部會的稽核規劃，稽核頻率是 2 年會

稽核完所屬部會，所以今年如果稽核 A 機關，可能就是 2 年後才會再稽核 A 機關。

針對簡報還有沒有問題？如果沒有，我們就先進入法的部分，我們目前擬出來的研修版本總共有 70 條，首先是資安法的部分計有 9 條，主要調修重點就是財團法人的定義那一塊，還有納入上級政府的概念，這一段可能影響的是縣市政府，另外一個就是主管機關稽核的部分，有關母法有沒有要再提供給我們建議？或者是哪邊需要詢問的？

如果沒有，那我們再進入施行細則的部分，施行細則我們目前擬修的條文計有 5 條，主要是上級政府還有實施情形提報的部分，讓它更明確化，針對這邊有沒有問題？

中華郵政股份有限公司：

你好，我是中華郵政李先生第 2 次發言。就是法條裡面，對於「或」這個字有 45 次的出現，「及」這個字有 48 次的出現，那如果就「或」這個字的出現，以第 4 條第 1 項第 1 條，他提到受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施，或透過第三方驗證。請問這個「或」字是兩個都要成立？還是只要 1 個成立就可以審這個廠商的資格？

主席林春吟高級分析師：

以目前舉的例子，受託者應具備完善之資通安全管理措施，或透過第三方驗證，這個「或」原則上是擇一，在我們 FAQ 上有說明。主要就是說，大家必須看一下委託案件規模大小，依委託案去評估，如幾千萬的案子可能就會要求乙方，必須就處理這個委託案通過驗證。但不是說每個案子都要求乙方去得到驗證，因為驗證也是需要成本，還是要回到委託案的範圍，之前也有廠商反應說，1 件 10 萬的案子，要他們去取得相關的驗證，可能會有一些困難，就是請大家在實務上，確認一下資產價值，跟對應合理的要求。

中華郵政股份有限公司：

是，另外還有第 7 條第 2 項的部分，提到什麼叫做核心資通系統，這個「或」字好像不是擇一的意思，是指 2 個都要，是只要其中 1 個符合就是核心資通系統的意思。是不是在法條用字的一致性上，這個「或」字好像有不同解釋？

主席林春吟高級分析師：

有關您對「或」這個字使用疑義，我們回去再請教一下法規會那邊，就

第 7 條第 2 項定義核心資通系統的確有 2 個條件，擇一成立就是核心資通系統，不是擇一條件來定義你的核心資通系統的概念。我們也有發現，有些機關會誤以為那樣，所以我們會再透過各種機會，跟大家宣導核心資通系統的定義有 2 個，只要符合其中一個，就是核心資通系統，不是任選一個來定義核心資通系統。有關「或」這個字是不是有法規上的單一應用屬性，我們回去再請教一下法規會。

國立中興大學：

我的問題應該跟這位先生前面講的是同一件事情，對於廠商的要求上面，如果沒有取得驗證，我們委外的系統其實不大，只是一般的硬體跟維修之類，可能在一定程度上，我們是不是用自評表也是可以行得通？

主席林春吟高級分析師：

所謂的自評表是請那個廠商，就他的資安管理措施，有一個自評嗎？

國立中興大學：

如果是這個系統上面，也許在我們的評估上面，也許它根本就是中以下的，不管在 C(機密性)、I(可用性)哪一個層級，都是在中以下的話，是不是採用自評表的方式，事實上也是行得通的？

主席林春吟高級分析師：

主要就是如何去確認受託者怎麼具備資安管理措施，它的形式我們沒有特定的規定，你們可能有一些檢核項目請他自評，要不要去抽驗？或者是請他交代完以後，實地去稽核，那都可以，那就是看你們在實務上，怎麼去處理？因為有時候你可能覺得說，初步我可能先用自評表，可是後來又有一些情資透露出，這個廠商可能有一些狀況，那你可能會加強確認的力道，在實務上都是可以去彈性運用。

國立中興大學：

我之所以提這個問題，是因為之前提報我們的資安維護計畫執行報告時，教育部給我們的 1 個評論是希望不是用自評表方式，而是要實地稽核，那就牽涉到非常多的系統，若要每 1 個都去稽核，實務上無法負荷。

主席林春吟高級分析師：

好，有機會我們會跟教育部了解一下，大家同步一下看法，主要大家儘量小心為上去處理，但也要注意實務可行性。

好，如果沒有其他施行細則的問題，我們就進到分級辦法的部分。分級

辦法我們目前擬調修計有 43 條，主要是有關 C 級機關的定義，另外大家作業上可能有比較大的不同，是有關 VANS 跟 EDR，其他主要就是防護基準調修的部分，針對分級辦法大家有沒有要提出的問題？

臺北市政府資訊局：

我是臺北市政府資訊局，做第 1 次發言。我這邊有 3 件事需要詢問，第 1 個是 EDR 的部分，我想了解一下這次把應辦事項增加 EDR，說實在 EDR 蠻花預算，再來就是我不曉得這個修正案一旦發布之後，有多少時間研議？這部分對北市府應該不是大問題，但是其他政府機關，我相信可能會是個問題，想詢問一下，EDR 的部分，依法規來講，他的要求是需要全部所有個人電腦 所有伺服器都要安裝 EDR 嗎？還是有什麼樣的要求？因為這邊的 EDR 沒有很明確的講這件事情；另外 EDR 以資安廠商的服務來講，他還有 MDR 服務，所以應該是只要買了 EDR 的軟體，然後他的服務我其實不用買嗎？還是說其實我還是要買 MDR 服務？這樣才是完整的 EDR 導入，就這部分想做一個詢問。另外建議說，以市府這邊導入 3 年 EDR 的經驗，因為導 PC 真的只發現挖礦程式，接下來就沒了，安裝在伺服器的效益比安裝在個人電腦上高很多，所以另外建議，是不是可能列為附表十的要求，可能會比較妥適。因為如果放在應辦事項，可能連 PC 都是需要逐步全面安裝。

那第 2 點的部分就是之前其實市府這邊給的修法建議，就是資安專職人力數量需求，以臺北市政府資訊局來說，我們統籌了很多機關的資通訊系統及，資安應辦工作，包含使用我們的機房，協助處理了相當多技術面跟管理面的部分，做了所謂的資訊向上集中之外，也做了所謂的資安向上集中，那在人力要求的部分好像還是要求，B 級 2 位，C 級 1 位，對於這樣的狀況，不知道說資安處這邊有沒有比較彈性的做法？而不是有些機關其實已經由資訊局這邊幫忙做了七、八成的資安，他還是必須要配置 2 個專職人力，對他來講也是一個蠻艱困的事情，因為他們就真的有 1 個核心系統，他就被定義為 C 級，但其實以資安能量來說的話，我們盡量集中由資訊局這邊協助各機關來辦理資安工作，也希望做一些人力比較彈性化的校正，這是第 2 點的部分。

那第 3 點的部分是有關附表十的部分，有一塊就是針對高等級防護的資通系統，有要求內外部使用者識別與鑑別，好像多了多因子認證的部分，且牽涉到外部使用者，針對外部服務要求，這一塊的影響幅度還蠻大的是不是

還有一些彈性，可以做一些調整？謝謝。

主席林春吟高級分析師：

謝謝。臺北市政府的資源相較比其它縣市政府多，所以也嘗試過不少資安的防護，剛才給的建議非常好，大家執行時可以做為參考。目前我們 EDR 的部分，就是放在應辦事項，那至於您剛才說是不是放附表十，我們回去再討論一下。有關它的執行範圍，因為會跟機關爭取到的資源有關，所以我們目前規範的方式是比照資安健診。剛才臺北市政府有提供 1 個建議，就是在主機端布建可能是他們比較建議的，有關 PC 端，,如果資源沒有辦法在一時之間到位，PC 端可能可以就一些系統管理者，或者是比較重要特定的 PC 去布建。原則上買了 EDR，要不要再買 MDR，主要是整體機制要有效，如何在機關裡面去布建才能達到效果。目前我們定義的 EDR 實施時間是在修法版本頒布後的 2 年內，大家可以先做預算籌編的作業。

再來就是你剛剛講的附表十，內外部使用者識別與鑑別的部分，在高防護等級要求多重認證技術，您的建議是說，外部民眾端的那一塊可以不用嗎？

臺北市政府資訊局：

對，民眾端的部分。

主席林春吟高級分析師：

好，這個我們回去再討論看看，是不是還是把內外部使用者識別拆開來規範，謝謝。

中華郵政股份有限公司：

您好，我是中華郵政第 3 次發言。附表二的地方，特定非公務機關有一些資安教育的要求，特別是針對資安專責人員，因為在 FAQ3.15，有特別提到所謂的資安專業課程訓練，或是資通安全職能訓練，有幾種方式可以取得。其中第 4 點是說要參加國內外公司及訓練機構，然後第 1 點是由貴處認證的資安訓練機構。另 108 年 11 月 28 日，貴處有發布 1 個資通安全自主產品採購原則，鼓勵透過自主產品採購來帶動整個產業發展，還有資通安全能量。這個部分中華軟協自主能量登錄 108 年第 1 梯次，3.9.3 資訊安全技術教育訓練有 5 家，第 2 梯次有 8 家，然後在今年上半年 1.13.3，資訊安全技術教育訓練有 17 家，合計有 30 家。但好像跟 3.15 的 FAQ 好像沒辦法 meet，因為 FAQ 所提的是 4 種類型的訓練機構。這部分有點造成我們在遵循上面的困

擾，就是說我們公營事業，想要透過軟協提供的服務機構地圖，找裡面有能提供資訊安全教育訓練的這些公司，但是很可能這些公司並不符合所謂的公私立大專院校或者是依法設立 2 年以上的職業教育訓練，或者短期補習班，學術研究機構，行政法人，財團法人等等的這些相關要求。請問這個部分要怎麼去認定？謝謝。

主席林春吟高級分析師：

好，目前這兩邊是脫鉤的，因為在資安法上，要求的是專業訓練，原則上我們會比較扣合在訓練機構，比較有機制在做訓練，當作基本要求。軟協辦理的主要是經濟部委託的自主能量登錄，揭露重點在於這個廠商有提供這個服務的能量，兩邊的定義其實不太一樣。您剛才提可能會讓你們在執行上，有一些不是太一致的地方，後續我們會再跟經濟部那邊討論看看可以怎麼樣去做一個處理，謝謝。然後剛才臺北市的問題，我好像漏答 1 個，就是人力彈性運用的部分，目前我們推資訊/資安資源向上集中，集中之後，機關等級調降，依法就沒有人力配置要求。那剛才您舉的例子，比較像是你們將七八成的資訊/資安往上集中，可是機關自己還有兩三成，因為還是有需要去保護的資通系統候，如果機關的等級沒辦法往下調成 D 級，還是要去處理 C 級機關的應辦事項。

臺北市政府資訊局：

因為這樣在資源上會有蠻大的差異，以資訊局來講，我們有五六十個系統，我們是 B 級，另外如圖書館，他只有 1-2 個系統，也是 B 級，依法規 B 級都會要求是 2 位資安專職人員。

主席林春吟高級分析師：

圖書館可能掌握圖書借用人員的一些個資，像臺北市的跨機關服務又做得很好，所以可能又涉及非臺北市市民的民眾資料，像新北或桃園的民眾都有可能去借書。原則上還是依責任等級，若他沒有辦法調降的話，在法遵上，還是依等級要求辦理，就是要有專職人力去協助做資安作業，去看有沒防護上的缺漏，或可以再評估有無可能調降等級。

臺北市政府資訊局：

好，謝謝。

教育部：

大家好，教育部第 1 次發言。就是剛剛提到責任等級分級，行政院所屬

機關每2年要提報1次，因應本次修法，我們可能要配合修法後的內容再去調查1次責任等級，建議作業時間能否拉長一點？謝謝。

柯旻圻助理設計師：

我今天剛好發1個公文，請大家說辦理資安法2年1次等級核定作業，請上級機關回復的日期是110年2月5日，調查函的附件，即請大家填註機關資安責任等級有沒有要調整及依據。

主席林春吟高級分析師：

等級調查公文的附件，我們有加入可能會影響等級的一些屬性欄位，要麻煩大家協助填寫，我們會再做後續的處理。目前提交時間是110年2月5日，大概有2個月的時間，再麻煩大家協助。好，那邊。

行政院環境保護署：

您好，我姓蕭，請教一下剛才提到的資通安全責任等級分級，如果資安法最近修法，我們到底是依照新的資安法去做核定提報還是依照原來的資安法？

主席林春吟高級分析師：

原則上在沒有完成修法前，就是依現在的資安法規定去做，你們提報後，主管機關會核定等級。新的等級核定下去後，就是依新的等級去辦理，還沒變更前，還是要依現行的等級去做處理。

文化部：

午安，這是文化部第1次發言，有關那個分級辦法的第6條，也就是有定義C級機關，首先我想要說明的是說目前版本裡，那個「或」的前面跟後面比率原則，好像有點不太對等。因為原本是說要維運自行或委外開發的資通系統，現在「或」的後面加上使用系統的話，可能是沒有維運，也要算成C級。這樣子或的前後兩邊的對等好像不太對等。那我要舉1個例子，譬如說如果很多機關其實都有用財管系統，那是雲端方案，機房相關的資安防護措施，都不是機關在維運，如果因為這樣就把機關調成C級，這樣的比例對好像不是很對等。所以這個文字內容是否可以再調整？或是再規定使用什麼樣規模的系統，如金額或使用人數，達到什麼樣的範圍，才納為C級，不然的話，有些機關甚至只是使用1個電子看板的管理系統，或者是停車場的管理系統，的確不是客製開發，只是買1個套裝軟體，這樣就會被調成C級，那C級的納管對象可能會瞬間提升蠻多的。然後我也想要說明，現在一直都

在推資訊向上集中，很多所屬機關開發的系統，如網站，我們都希望他的主機可以放在我們的共構系統裡，統一由上級機關或共構機房來維運。那如果說那他的機器，或者資安的都已經向上集中，由共構機房來提供機關使用，依調修的內容就變成 C 級的話，反而會讓機關向上集中的誘因喪失了。即不管我是放在本地的通訊機房，或者是放在上級機關那個共構機房，我一樣都會落成 C 級的話，那我向上集中的動力到底在哪裡？這是我想要反應。再來就是「或」後面的那個字眼，的確一開始看到叫做非自行或者委外開發系統，真的有點看不懂，這樣的字眼可不可以落成括號，使用一些比較白話，譬如說套裝、商用還是市售，來輔助非自行或委外開發系統。以上，謝謝。

主席林春吟高級分析師：

好，謝謝文化部的意見。因為 C 級的定義，也是我們現在還在研議，還沒找到一些比較好的用詞。如果您有想到其它，也歡迎提供給我們。目前的研擬版本的確如剛才講的，我們也發現有一些問題，我們會再修，您剛才的意見，我們再納入參考。然後要跟大家強調一點，我們的向上集中並不是說那個系統，這個機關建了，然後放在上級機關的機房，就叫向上集中；因為那個系統還是由本來的機關在管，不是共構了就叫向上集中，我們主要是看資通系統是誰在維運，就是誰要去注意系統的資安議題，不管是弱掃、滲透測試，或系統該修補的弱點，有沒有去修補，主要是那些維運的作業，還有系統相關的一些防護，我們強調的重點是在這邊。因為有些機關覺得，請所屬把系統都拿到上級機關的機房，就可以降低等級，但那些系統只要是你的所屬在做維運，他其實只是放到某個機房，你把它想像成是把主機放在中華電信商的共構機房，是比較相似的。所以我們要強調的是，原則上就是相關的管理和維護責任，也要向上集中。為什麼要向上集中？就是因為每個機關都有辦法配置那麼多，不管是資訊人力，還是資安人力，因為那個人才的訓練是要成本，大家應該在實務運作上會有這樣的議題。那剛才提的那些套裝、商用的，我們也有考慮過這些用詞，那後續我們再看看說有沒有一些比較好的。因為我們查了一下，目前在資通系統的，不管是定義用詞上，其實有各種說法，比較難有一個比較一致性的。那在這邊也是歡迎，萬一你還有想到其它的，再提供給我們。因為在上面寫一些什麼一定規模，這個可能也會又變成一個，就是法規的不確定性了，那個我們法規會也會有意見的，好，謝謝您。然後好，分級辦法這邊還有沒有要給我們建議的？好，那邊，謝謝。

財團法人國家實驗研究院：

大家好，我是國家實驗研究院，第一次發言。關於那個 VANS 的部分，我們是特定非公務機關，那請問一下那個關鍵基礎設施的部分，去導入 VANS，是只有關鍵基礎設施的部分呢？還是全單位？以上謝謝。

主席林春吟高級分析師：

我們導 VANS 應該都以全機關為一個範圍，對，我們目前是這樣。

財團法人國家實驗研究院：

不好意思，我再說明一下。因為我們有單位他的關鍵基礎設施，其實是跟我們的網路所有東西全部都區隔的，所以他的設施其實是比較特殊的狀況，其實就是微型的操控站，那他其實是特殊的一個服務，跟我們其實是完全網路全部分開的，所以假設我們要全單位，因為 VANS 我們去上課，其實它不是太容易執行的，老實說，然後因為有那個成本的考量，所以如果說是只有關鍵基礎設施部分的話，或許我們導入是可以做，可是如果說是全機關要我們導入系統，實際上有困難，以上。

主席林春吟高級分析師：

好，你們的狀況可能我們會後再了解一下，好不好？到時候跟我們的同仁留一下那個聯絡資訊，我們可能就細部的部分再討論一下，因為特定非公務機關，尤其 CI 提供者那邊，的確是比較特別一點，好，謝謝。還有沒有？那邊。

審計部：

這次有 1 個 EDR 導入，那之前譬如我們的資安的那個廠商跟我們介紹，那介紹到 EDR 這個部分，我不知道是不是其實他就是那個，就是主要做 APT 那個會先防護這樣子，本來就有 APT 這個部分，我們又加了 EDR，2 個到底有什麼不同？

主席林春吟高級分析師：

好。他們兩是不一樣，建議要不要找一下那個臺北市資訊局那邊請問一下，因為 APT 跟 EDR 的部分，其實防禦的點就不太一樣，然後他的整個行為模式應該也是有一點不同。這個技術面的東西，我們可能就不在這邊去做一些討論，好不好？那有一些 EDR 的產品，就是共契上的，其實我們可以至少提供共契上的一些資料，你們可以再跟廠商確認一下產品的差異。我相信他們講得可能會比我們講得更清楚，可是它們是不一樣的東西，這是肯定的。

好，還有沒有？這邊。

新北市樹林區公所：

您好，這裡是樹林區公所第 1 次發言。就是一樣是針對責任等級第六條的修正，這個 C 級機關，像是我們新北市政府，各個機關都使用市府他們建的那個 mail server，若依照新的那個條文，只要使用的話，是代表讓全市府所有機關都落到 C 級嗎?

主席林春吟高級分析師：

不是使用。你有點出就是本來 C 的那個用詞的問題，像新北市府統一建一套 mail server 給他的所屬機關用，那所屬機關沒有另外再架 mail server 的話，你就不會因為你使用市府的 mail server 而變成 C。你如果會變成 C 的話，應該是你們自己又架了 1 個什麼系統，才會因為那個系統變成 C，不會因為使用。所以那個目前 C 的寫法勢必得調整，但目前沒有找到 1 個比較好的調整方式，還是先用這樣的文字。那的確目前的文字會有一些問題在，一定不會用此版去定版，重點絕對不是要把 C 的數量拉上去，其實我們的期待是大家最好是可以是 D 或者是 E，然後系統儘量地往上，縣市政府一定是 B 級機關，儘量讓他提供服務給他的所屬機關去做使用，這才是我們的目標。好，分級辦法的部分…那邊。

連江縣政府：

連江縣政府第 1 次發言。因為連江縣在離島那邊，那真的是交通上非常的不方便，所以離島資源是非常缺乏的，那因為現在推向上集中，我們有想要把連江縣鄉公所的等級調降到 D 級，所以他們現在在考慮把他們的鄉公所網站移到縣府部分。可是當初聽主席您說向上集中不只是把他們的網站移過去我們縣府的地方，還要幫他們做弱掃，滲透測試那些什麼的部分，那這樣的話，我們的預算跟資源光靠縣府的部分，是完全無法去負擔的。有關離島的部分，還請幫忙考量一下。

主席林春吟高級分析師：

好，目前大概有 40 幾個機關，他從 C 級調降成 D 級，那很多的確就是網站，網站等於是最好向上集中的。目前那幾個案例，大家就是上面的機關，他是用網站 1 個平台跟框架，所以其實是在共同的運作基礎上，幫那一個公所開 1 個網站在那邊，其實你會對那個系統做弱掃還是什麼，你是對那個平台，你不會說因為公所的網站，在你的平台上多開 1 個網站多掃 1 個網站，

可是你增加的工其實不會那麼多，公所負責就是內容的維運，對於說連到你的網站平台去，可能就放資料或更新資料，這樣他是可以往下降的。所以其實要回到你們縣府那邊網站的，是不是有 1 個平台框架？如果是的話，建議你們可以讓他們就是直接在你們的平台框架上，開 1 個網站，讓他們維護就好。那如果你們有達成這樣，做好的時候，就發個文過來給資安處說明，這樣是可以順利的往下降。對比剛才的 1 個說法，如果是他自己建 1 個網站，然後把那個機器放在縣府那邊，這就是我剛才講的，因為他網站整個的平台，還是他要維運，因為這種情況就變成 2 個網站平台，那不是我們所謂的集中，我們期待的集中就是有一個平台框架。好，那大家還有沒有？暫時沒有的話，那我們就接著往下，好。

接下來就是通報應變辦法，這邊我們擬修條文是 5 條，主要是針對那種多發型的，就是短時間內可能在某個領域，或者是屬性相同的發生類似的資安事件，這邊主要就是因應可能性的那種組織型攻擊。如果說他的上級機關有發現到這樣情況的話，我們在這邊就是賦予上級機關可以另外通報 1 個資安事件，來統籌這些可能相關的資安議題，主要是就這邊；然後另外一個就是說在我們實務作業上，有一些比較重大的資安事件發生之後，他的上級機關或主管機關，我們會進去幫忙，就不會說只是到結報的時候才進去。那也是因應實務上運作，所以我們把那個相關的處理彈性把它放進去。那針對通報應變辦法這邊，大家有沒有什麼？好，那邊。

臺北市政府資訊局

請教一下，2 個問題，其一是因為近期我們也收到說通報資安事件的狀況，想釐清在第六條所謂的 1 小時內知悉之後要通報，那我想了解一下，就是公務機關知悉這一塊有沒有比較詳細的定義？因為我們這邊有遇到 1 個情境是，譬如說負責資訊網路設備的人員，他可能在換設備的時候，他弄斷了，斷線了，結果他們可能忍受的時間是 4 小時，結果到第 6 個小時，第 7 個小時都沒有回覆，那接下來是隔了 1 天，然後我們這邊資訊局就會通知那一個機關，你趕快通報，那他們隔了 1 天才通報，就是這種類型的案件，結果後來他們可能會說，因為我資安人員沒有知悉，所以我是你講了我才知悉，所以是我知悉的那 1 天那 1 個小時開始算，才算 1 個小時。因為那個定義有點模糊，就是什麼叫做公務機關知悉？因為所謂的公務機關知悉指的是，上級機關通知他，還是技服中心通知他？還是說他們機關裡面的，只要有人知道

的那個時間點，就是知悉？還是說要有資安人員收到才算知悉？對，這個是我們實務上面的 1 個問題。

那第 2 部分，有關那個關聯性的資安事件，我們可能要再額外做通報的部分，因為市府來講，我們總共管轄了 140 個機關，那數量讓我們不見得可以立即發現，我說實在的，今年資安處有給那個資安事件的數量，那應該臺北市府貢獻不少，我們這邊都有依法通報這樣，那因為我們數量這麼多，然後是不是在這個系統上面，能夠給一些輔助？就是譬如說在短時間之內，有類似說疑似關聯的，還是怎麼樣的話，也許在系統面的部分可以提供給我們一些提醒或者是提示，那由我們主管機關會比較、判定，然後我們也願意主動辦理通報關聯事件這樣子。以上建議，謝謝。

主席林春吟高級分析師：

好，謝謝，就是有關那個系統提示的部分，這邊我們會帶回去，看看系統那邊可以怎麼至少先預警或提醒你們注意，這樣的確大家就會比較提高警覺。那有關那個逾時知悉，我們法規上的文字是公務機關知悉，所以我們沒有去指說要資安人員知悉，還是誰知悉，原則上是以公務機關知悉，來定義的。然後這邊也是提醒大家，就是有一些法遵，像那個事件通報，他時效上有 4 個階段，每 1 個階段都有一些時效的規定，這邊就是提醒大家一定要特別注意。因為我們在系統上，是會做統計的，目前每個月我們也會針對，就是上個月，如果逾時，會發信給當事的機關跟他的上級機關。那每 1 季我們會把它統計起來，就給他的上級機關，所以這一段就是大家如果有不小心，或者遇到資安事件的話，務必要依法規上的 1 個時效，去做對應的處理，這個就是再次提醒大家。好，那大家還有沒有？那邊。

中央銀行：

中央銀行，敝姓林第 1 次發言。就是針對通報應變辦法裡面第 2 條的事件分級，那像資訊系統我們照責任等級分級辦法附表九那邊，其實都有對三個構面都有補充，可是在我們事件分級的時候，就是依著是非核心、核心、涉及關鍵基礎設施，那其實就算是核心資通系統，他的可用性這一邊的衝擊，他可能還是普，那他發生事件，其實影響也是有限的，那一下就跳到二級事件甚至三級事件的話，感覺上好像也不符合它的比例。所以在他的事件分級的部分，是不是可以回到，就是系統的分級，用普中高來做命名？謝謝。

主席林春吟高級分析師：

原則上他2個的切入構面不太一樣，您剛剛講得就是你的核心資通系統，他如果是核心資通系統，原則上就會落到二級事件。可是這樣會對你們造成什麼樣的議題嗎？因為如果它既然是你們的核心資通系統，在整個定義上，目前我們法令的精神，對你們在實務執行上，會有造成什麼樣的一個執行上的困難？

中央銀行：

我們實務上是有1個系統，因為個資的問題，所以他在可能機密性法令，我們把它分為高防護需求，但他的可用性這一個構面，其實他可能一個禮拜、兩個禮拜不運作，其實都不會造成什麼樣的影響。那就會變成說，他萬一不小心什麼中斷了，那就要二級事件起跳。

主席林春吟高級分析師：

這邊我們帶回去研究一下，就是說其實你們的那個核心資通系統，你的重點其實在機密性高，而不是可用性那一段，你要表達是這個，那這樣是不是有可能是在一級的範圍裡，對不對？沒關係，這個我們回去再研究一下，好不好？謝謝你，好，大家還有沒有？這邊。

新北市樹林區公所：

新北市樹林區公所第2次發言，針對通報應變辦法，就是在貴處舉辦說明會，很常看到投影片都講說呼籲各機關不要以那個資安事件發生數量當作KPI。只是放在簡報上，是沒有什麼約束力。然後是否可以建議把它直接放在那個辦法、修法裡面？因為現在很多機關還是以數量當作KPI去做評分的。

主席林春吟高級分析師：

在法裡面要求事件不要納KPI，好像跟法的結構不太相符合，我們目前的做法，除了在一些高階主管會出現的場合去做宣導之外，那我們就是像行政院出去的稽核，我們也會特別看。當他的指標有把資安事件納進去的話，原則上我們都會幫他寫1條待改善事項，我覺得這件事情是可能需要一些宣導，因為大家對資安事件的觀念其實要做一個扭轉。資安事件對我們來講是一個情資，是一個重要情資，我們會鼓勵大家就是通報，反而你不通報，才有可能會造成更大的危害。那您講那個，我們在看可以怎麼落在相關的文字裡？不過目前依法的體例可能比較很難融進去，謝謝。

好，如果沒有的話，我們再往下，就是特定非公務機關的實施情形稽核辦法，這邊我們的擬修條文是4條，主要就是因應那個不可抗力，可以去處

理說本來已經規劃好的 1 個稽核計畫，大家有沒有問題？那目前我們還是強調稽核，我們還是採實地的方式去進行。因為有一些機關有在想說，是不是可以視訊稽核，可是就目前來講，我們還是以實地稽核這種模式為主，所以我們就是以在時間去做一個調整的方式來處理。

好，我們就再往下，再來是情資分享辦法，主要我們要擬修的條文有 2 條，主要就是中央目的事業主管機關有在反應，特定非公務機關其實是這次資安法把它納進來的，所以他們需要更多的鼓勵，去分享一些有用的情資，所以我們就在法裡面，把這一條修進去，讓中央目的事業主管機關，可以在處理作業上有一些彈性。

好，如果沒有，那就進到最後一個獎懲辦法的部分，那這邊也是一樣，原則上我們盡量不走懲處的部分，我們會希望是以鼓勵的方式在處理這件事情。可是如果有一些應辦未辦，情節又重大的，有時候還是得去做一些檢討跟評估，目前我們就是把整個評估的對象範圍，把主管跟上級機關一塊納進來，畢竟他們還是有一些督導的責任，把它明確的訂出來，這就是修法的一個重點，好，那針對這個大家有沒有問題？好，如果沒有的話，那我們今天的修法的部分，原則上到這邊，今天謝謝大家，謝謝。