資通安全管理法修正重點

114年11月

大綱

一、資通安全管理法增修架構總覽

二、資通安全管理法修法重點

三、資安相關子法修正重點

一、資通安全管理法增修架構總覽

資通安全管理法增修架構總覽

	第一章 總則§1-9	第二章 公務機關資通安全管理§10-15	第三章 特定非公務機關資通安全管理§16-18	第四章 罰則§19-21 第五章 附則§22-23
現行條文	● 目的及主管機關§1-2 ● 推動資通安全產業§4 ● 國家資通安全政策等事宜§5 ● 委任或委託§6 ● 資安責任等級分級§7 ● 情資分享機制§8 ● 委外監督§9	● 資安維護計畫之訂定§10 ● 資通安全長之設置§11 ● 資安維護計畫實施情形之提出、稽核、改善§12-13 ● 資安事件通報應變機制§14 ● 公務機關所屬人員之獎勵辦法§15	● CIP指定程序§16 I ● CIP資安維護計畫實施情形應予稽核§16 ● 其他特定非公務機關資安維護計畫實施情形得予稽核§17 ● 資安事件通報應變機制§18	● 公務機關所屬人員之懲戒(處)§19 ● 特定非公務機關罰則§20-21 ● 施行細則§22 ● 施行日期§23
三讀通過	✚增修 ● 數發部為主管機關§2 ● 特定財團法人定義§3⑨ ● 受政府控制之事業、團體或機構§3⑩ ● 協助民間處理、因應及防範重大資安事件§4 ● 國家資通安全會報§5 ● 依責任等級辦理防護措施§7 ● 主管機關得稽核公務機關§8 ● 委外辦理應建立管理機制§10	✚增修 ● 分層監督管理模式調適：實施情形提出、稽核及事件通報對象§14~17 ● 重大資安事件提供協助及公告§17 V ● 專職人員職能訓練及調度支援§18 ● 專職人員適任性查核§19	✚增修 ● 資安長、專職人員之設置§20、21、23 ● 重大資安事件之行政調查§25 ● 特非人員獎勵§26	✚增修 罰則 ● 特非人員懲處§28 III ● 演練作業罰則§30⑥ ● 行政調查罰則§31 附則 ● 主管機關委託對象§32【註】現行條文§6移列 ● 資安事件涉個資外洩時應另依個資法規定辦理§33

✚增修

共通規範
- 危害國家資安產品管制§11、27
- 應配合演練作業之授權§17IV、24IV

A.C.S 資安是持續精進的風險管理

【註】其餘條文微調，請詳見對照表

二、資通安全管理法修正重點

資通安全管理法修法重點(1/1)

修法目標

修法重點

明確機關權責 定明規管範圍

- 主管機關修正為數發部 (§2)
- 配合財團法人法施行，修正特非機關定義(§3⑨)
- 增加納管受政府控制之事業團體或機構(§3⑩)

明訂委外事項 完善監督機制

- 明定各機關委外權責事項、演練導入第三方協力(§10)
- 強化國家資通安全會報功能(§5)
- 機關權限委託及協調之法規依據(§32)

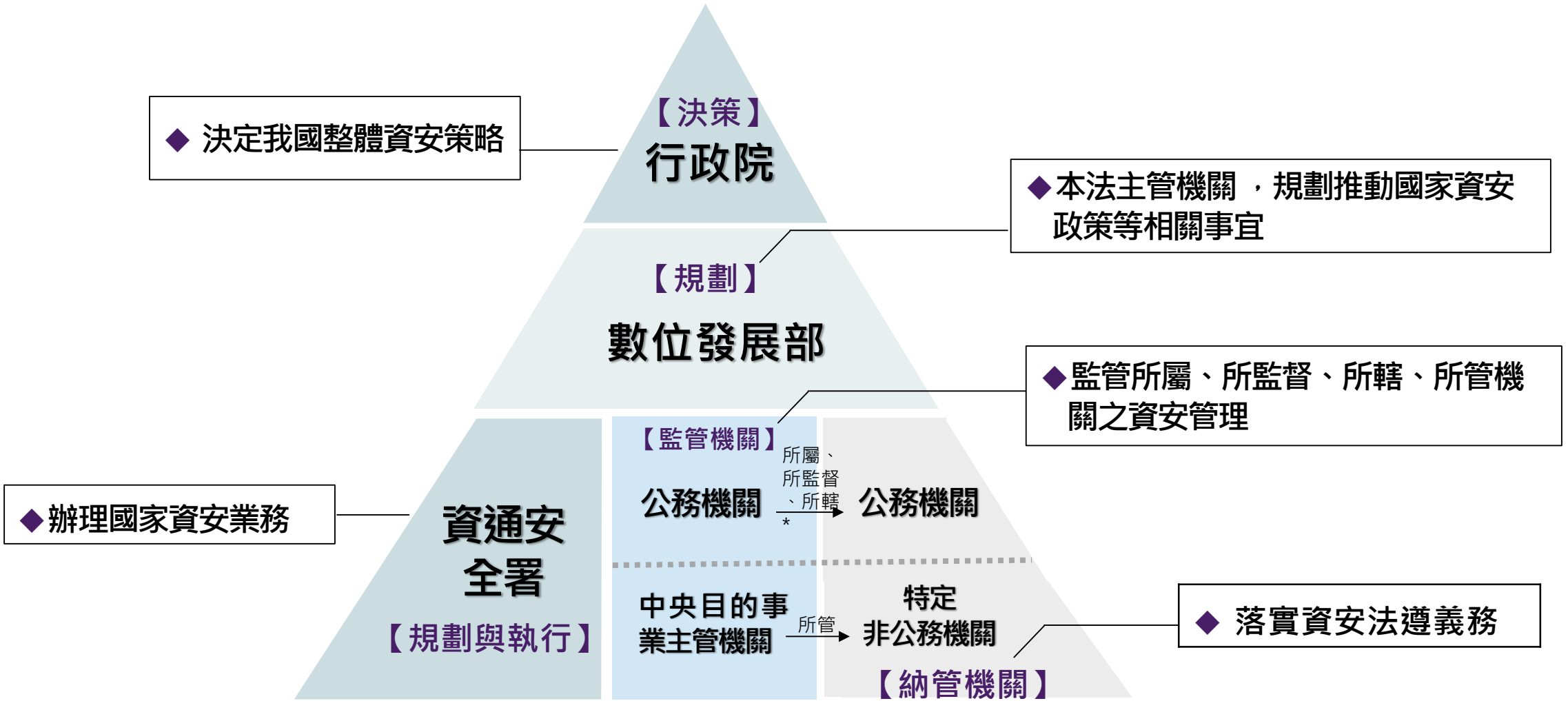
強化資安人力 增訂查核機制

- 公務機關：職能訓練、調度支援、適任性查核(§18、19)
- 特定非公務機關：
  1.設置專職人員及資安長(§20、21、23)
  2.對所屬人員獎懲(§26、28)

擴大稽核範圍 強化資安管理

- 危害國家資安產品管制(§11、27)
- 公務機關：強化聯防體系，分層監督管理模式調適 (§8、14~17)
- 特定非公務機關：重大資安事件調查權限(§25、31)

明確機關權責 定明規管範圍 (1/2)



【註】所轄公務機關：在直轄市政府係指直轄市山地原住民區公所及直轄市山地原住民區民代表會；在縣政府係指鄉 (鎮、市) 公所、鄉 (鎮、市) 民代表會

明確機關權責 定明規管範圍 (2/2)

●修正特定財團法人定義(§3⑨)

修正重點

●為避免各界混淆資安法以及財團法人法所規範之財團法人，並兼顧資安法係以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象之宗旨，修正如下：

特定財團法人
- **財團法人法定義之政府捐助財團法人(捐助比例50%以上) (財團法人法第2條2、3項)**
- **民間捐助財團法人+ 主管機關指定(財團法人法第63條1、4項)**

●增納受政府控制之事業、團體或機構(§3⑩) NEW

修正重點

●新增納管銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之**事業、團體或機構，具資通安全重要性者**。

上開事業、團體或機構，如屬地方政府控制者，為符地方自治及分層負責原則，應經地方主管機關同意後，主管機關始得核定。

【註】銓敘部原則按季公告受政府控制之事業、機構或團體清單

明訂委外事項 完善監督機制 (1/1)

●強化國家資通安全會報功能(§5) NEW

修正重點

- **國家資通安全會報由行政院召開，明定所有公務機關之協力義務**
  - ✓ 原為行政規則，現將規定入法。
  - ✓ 各政府機關、中央及地方間，應致力配合推動執行國家資通安全措施。
  - ✓ 決議事項，相關政府部門應予執行，由主管機關定期追蹤管考，並得辦理績效評核。

●權限委託及特非監管機關之協調(§32)

修正重點

- **權限委託：明訂主管機關得委託事項 – 原條文§6、施行細則§12**

  主管機關辦理資通安全整體防護、演練、稽核、國際合作等事務，得委託其他公務機關、法人或團體。

- **明定主管機關得協調指定中央目的事業主管機關辦理特非監管業務**
  - ✓ 現行資安法施行細則§12提升至法律位階。
  - ✓ 特非之業務涉數個中央目的事業主管機關權責時，主管機關得協調指定單獨或共同辦理應辦事項。

強化資安人力 增訂查核機制 (1/2)

公務機關

NEW 調度支援職能訓練(§18Ⅱ)

資安署

- **調度支援，以戰代訓:** 遇有**重大資通安全事件**，得調度各級機關資通安全人員支援，並視為在職訓練的一環
- **推動專職人員之職能訓練**

NEW 適任性查核(§19)

函請法務部調查局辦理

主管機關：任用考試人員
用人機關：所屬現職人員

- **主管機關查核**：得於資通安全人員任用考試榜示後，對錄取人員之適任性進行查核
- **用人機關查核**：得對所屬資通安全專職人員適任性進行查核
- **效果**：拒絕查核或查核結果經用人機關認定未通過者，不得辦理涉及國家機密、軍事機密及國防秘密之資通安全業務

強化資安人力 增訂查核機制 (2/2)

特定非公務機關

應設置專職人員及資安長(§20、21、23) NEW

✓強化特定非公務機關資通安全能量，比照公務機關應設置資安長及資安專職人員。

增訂對所屬人員之獎懲規定(§26、28II) NEW

✓特定非公務機關對於所屬人員之資通安全維護績效優良者，應予獎勵。

✓特定非公務機關所屬人員未依本法規定辦理，情節重大者，依機關規定予以懲處。

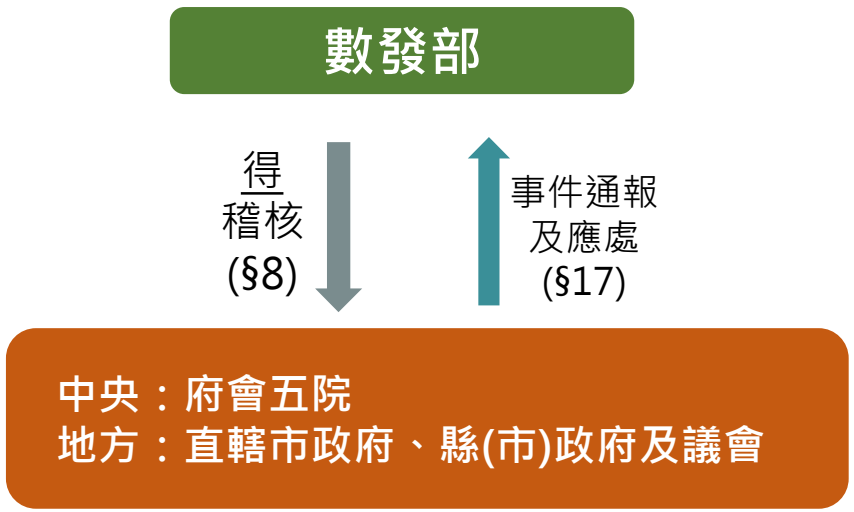
擴大稽核範圍 分層監督管理 (1/1)

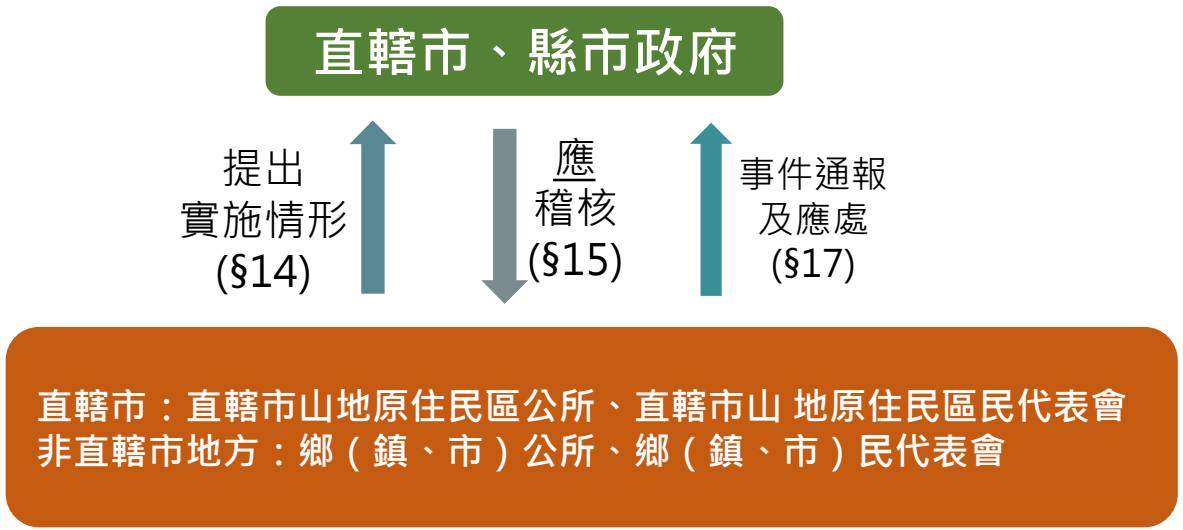
●強化公務機關聯防體系，分層監督管理模式調適 (§8、14~17)

現況問題

- 無上級機關之**公務機關**，依現行法無外部稽核機制*審計部109年總決算審核報告指出
  - ✓ 中央：府會五院
  - ✓ 地方：直轄市政府、縣(市)政府、地方議會、直轄市山地原住民區公所、直轄市山地原住民區民代表會，鄉（鎮、市）公所、鄉（鎮、市）民代表會。

修正重點





強化危害國家資安產品管理 (1/3)

01 行政規則

發布日期：108 年 4 月 18 日

依「**危害國家資通安全產品限制使用原則**」，倘因業務需求且無其他替代方案，應具體敘明理由，經**機關資安長**及其**上級機關資安長**逐級核可，**函報數位發展部核定**後，以**專案方式購置列冊管理，及遵守以下規定**：

1. 指定特定區域及特定人員使用
2. 使用理由消失應立即停止使用
3. 以**不含個資及資料的電腦單機**將其**下載並以斷網或非公務網路之獨立網路使用**較為安全

提升至法律位階

02 行政函釋

函文日期：109 年 12 月 18 日

為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，行政院秘書長109年12月18日院臺護長字第1090201804A號函知各機關，**公務用之資通訊產品不得使用大陸廠牌(包含軟體、硬體及服務)**。

納入子法內訂定

強化危害國家資安產品管理 (2/3)

- 危害國家資通安全產品(§11、27)

公務機關

公務機關 ✚ 場所提供公眾視聽或使用之傳播設備及網際網路接取服務 ✚ 公務人員

- 不得下載、安裝或使用
- 但書：因業務需求且無其他替代方案者，專案使用*

【註】雙資安長核可，函報主管機關核定後，專案使用並列冊管理。

獲配之公務用資通訊設備

- 不得下載、安裝或使用

特定非公務機關

特定非公務機關

- 特定非公務機關
  - 中央目的事業主管機關得予以限制或禁止

【註】機關資安長核可，函報中央目的事業主管機關核定後，得以專案方式使用，並列冊管理

  - 但書：因業務需求且無其他替代方案者，專案使用*

【註】管控措施由中央目的事業主管機關報主管機關備查

- 場所提供公眾視聽或使用之傳播設備及網際網路接取服務，於維護資通安全之必要時

強化危害國家資安產品管理(3/3)

危害國家資通安全產品限制規定(§11、27)

限制範圍

- **公務機關**
  - 中央機關(構)
  - 地方機關(構)
  - 公立學校
  - 行政法人
- **特定非公務機關**
  - 公營事業
  - 關鍵基礎設施提供者
  - 政府捐助之財團法人
  - 受政府控制之事業法人或團體

於維護資通安全必要時，各機關自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服務

事件行政調查 瞭解脈絡根因(1/1)

- 公務機關：回歸適用行政程序法
- 特定非公務機關：重大資安事件調查權限(§25、31) NEW

調查機關

中央目的事業主管機關

調查時機

限於「重大」資安事件發生

受調查者

特定非公務機關
(當事人)

受託之資訊廠商
(關係人)

調查程序

1. 通知到場陳述意見
2. 通知提出獨立第三方機構出具之鑑識或調查報告
3. 前往應受調查者之處所實施必要之檢查

證件出示
調查人員應出示執行職務之證明文件

保密義務
受任或受託調查者，不得洩漏獲悉秘密

三、資安法相關子法修正重點

資安法各子法草案修正重點

序號	類型	法規名稱	修正重點
1	修正	資通安全管理法施行細則	1.定明母法第14條無上級機關提出稽核改善報告執行情形 2.增訂委外廠商應增加「曾犯刑法妨害電腦罪章」經有罪判決確定或通緝有案尚未結案之查核項目
2	修正	資通安全責任等級分級辦法	1.修正責任等級提報流程及核定依據 2.特定類型防護基準擴大適用 3.附表修正、應辦事項法遵期限調整
3	修正	公務機關所屬人員辦理資通安全事項管理辦法	定明調度支援、適任性查核、職能訓練規定
4	新增	危害國家資通安全產品審查辦法	定明危害產品審查作業及情資分享程序

(一)資通安全法施行細則

委外廠商之適任性查核項目

細則 §4 委外機關之適任性查核

NEW

- 曾犯刑法「妨害電腦罪章」經有罪判決確定或通緝有案尚未結案
- 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案
- 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處
- 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事
- 其他與國家機密保護相關之具體項目

辦理適任性查核**前**，應經當事人**書面**同意

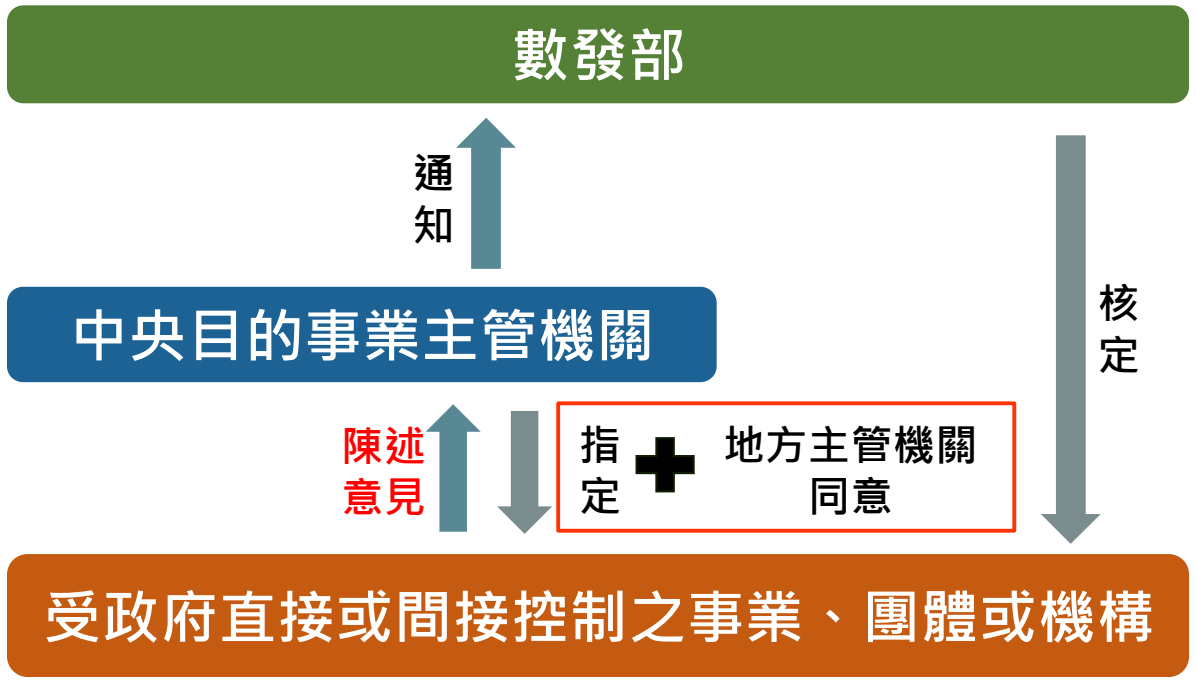
受政府直接或間接控制對象陳述意見機制

- 配合母法增納受政府控制之事業、團體或機構，細則第9條增訂定陳述意見機制

母法條文

- 指銓敘部依公務人員退休資遣撫卹法第七十七條第一項第二款第三目及第四目公告之事業、團體或機構，**具資通安全重要性者，經中央目的事業主管機關指定**，並經主管機關核定者；**其受地方政府控制者，應經地方主管機關同意後，主管機關始得核定。**

指定流程



(二)資通安全責任等級分級辦法

特定類型資通系統防護基準之適用

修正前

第11條第2項:

特定非公務機關之**中央目的事業主管機關**就特定類型資通系統之防護基準認有另為規定之必要者，得**自行擬訂防護基準**，報請主管機關核定後，依其規定辦理。

修正後

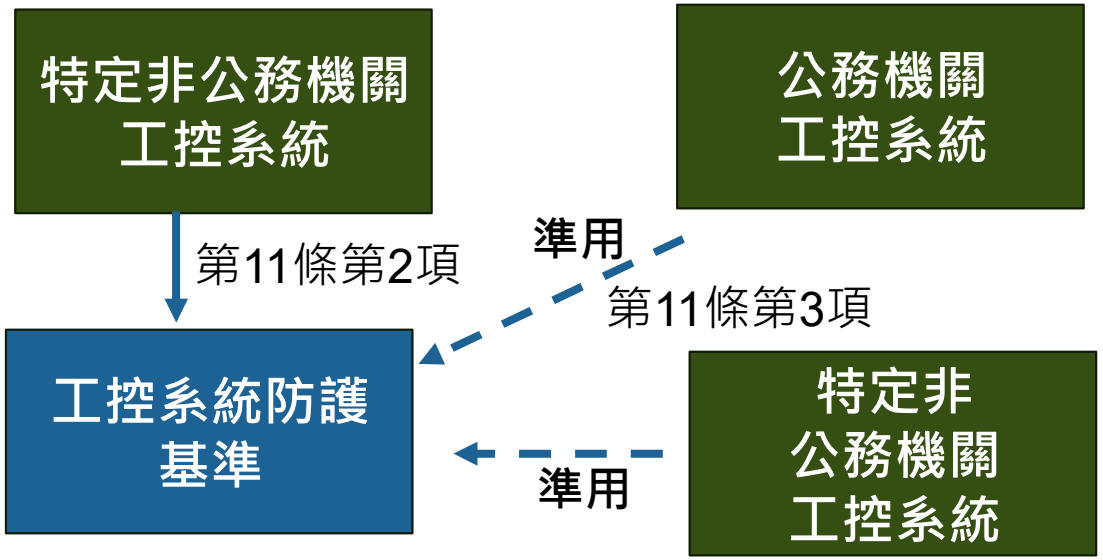
第11條第3項：(本項新增)

公務機關經其**上級機關或監督機關**同意者，**準用**中央目的事業主管機關依**前項所定防護基準相關規定**辦理，其他**特定非公務機關經其中央目的事業主管機關同意者，亦同**。

現況問題

OO醫院
(公務機關) ✗ → 衛生福利部醫療領域資通系統資安防護基準

OO公司
(經濟部所管) ✗ → 交通部交通領域工業控制系統防護基準



資安專職人員

修正前

公務機關

需置
「資安專職人員」

特定非公務機關

需置
「資安專責人員」

修正後

公務機關
特定非公務機關

需置
「資安專職人員」

資安專職人員

每人每年接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練

特定非公務機關資安專職人員需取得至少一張資安職能證書

資安專職人員以外之資訊人員

每人每年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

資訊人員每2年接受通安全專業課程訓練或資通安全職能訓練改為每年

一般使用者及主管

每人每年接受三小時以上之資通安全通識教育訓練

附表1-7新增及修正應辦事項

項目	公務機關/特定非	辦理內容
資安治理成熟度評估	特定非	A、B：特定關鍵基礎設施提供者每年辦理一次
核心資料庫安全檢視	公務機關 特定非	A：每年辦理一次　B、C：每二年辦理一次
物聯網設備安全檢視	公務機關 特定非	A：每年辦理一次　B、C：每二年辦理一次
政府組態基準檢視	公務機關	A：每年辦理一次　B：每二年辦理一次
端點偵測及應變機制	特定非	A、B：完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料
資通安全威脅偵測管理機制	特定非	A、B：完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料
弱點管理	公務機關 特定非	A~D：適時進行軟、硬體之必要更新或升級，並於修補前採行緩解措施
資料外洩防護機制	公務機關 特定非	A、B：完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級

(三)公務機關所屬人員辦理資通安全事項管理辦法

適任性查核

查核主體	查核對象	查核時點
用人機關	所屬資安專職人員	必要時
主管機關	資安考科錄取人員	得於榜示後

拒絕查核或查核未通過者，不得辦理機敏資安業務

查核基準項目

- 公務人員消極資格
- 對國家忠誠度
- 受外國勢力影響
- 犯罪資訊(妨害電腦使用罪)

資安職能訓練

資安職能訓練制度
訂定及實施

評量及證書制度
訂定及實施

訓練機構
遴選及查核

調度支援

目的

為強化公務機關資通安全人員實戰經驗與應處能力，並發揮共同一體之行政機能。

規劃方向

1. 調度支援應尊重機關意願，需事先徵得機關同意。
2. 調度支援以短期3日內為原則，至多再延長3日。

適用對象	公務機關
參與機關	主管機關、事件發生機關、支援機關
啟動時機	發生重大資安事件，事件發生機關請求支援或主管機關認有必要時
機關意願	調度支援應事先徵得事件發生機關及支援機關同意
支援內容	事中損害控制及事後復原鑑識等資安事件應變相關事項
調度時間	每次以3日內為原則，至多再延長3日

(四)危害國家資通安全產品審查辦法

「危害國家資通安全產品」修正重點

現行規定

- 現階段請各公務機關依照「各機關對危害國家資通安全產品限制使用原則」與「行政院114年函」，禁止使用危害國家資通安全產品、大陸廠牌之資通訊產品(含硬體、軟體及服務)。

✓ **以行政規則、行政命令要求各機關遵守規定。**

資安法修正重點

總統公布日期：114 年 9 月 24 日

1 **相關規定提升至法律位階**

依資安法授權，建立危害國家資通安全產品之風險評估、情資研判、情資分享辦法。

2 **提升機關應處效率**

以資訊化方式，將經相關領域機關所綜合評估、研判後之情資，分享給資納管機關，以利各機關及時應處。

提報機關與情資分享

提報機關定義：

- 納管機關對所使用之資通訊產品，**經自評疑似為危害產品**者，得敘明**理由及提供相關情資佐證後，由其上級機關確認所提情資，送交主管機關。**

◆ **得向主管機關進行提報之機關：**

一、總統府、國家安全會議、五院及其直屬機關。

二、直轄市政府、直轄市議會、縣(市)政府及縣(市)議會。

三、如為特定非公務機關，則應由其中央目的事業主管機關提報。

情資分享簡介：

- 透過**情資分享機制**，將各機關所提報並經本辦法評定為危害國家資通安全產品之情資，**以發布警訊之方式分享予納管機關。**
- 若屬**重大風險情資**並透過**N-ISAC分享予非本法納管之機關（構）。**
- 為搭配前揭情資分享方式，規劃修正**《資通安全情資分享辦法》**，將危害國家資通安全產品情資納入該辦法之「資通安全情資」，據以分享危害國家資通安全產品情資。

資安是持續精進的風險管理