經濟部
產業發展署
Industrial Development Administration, MOEA

C2M 資安相關規範說明

112年10月

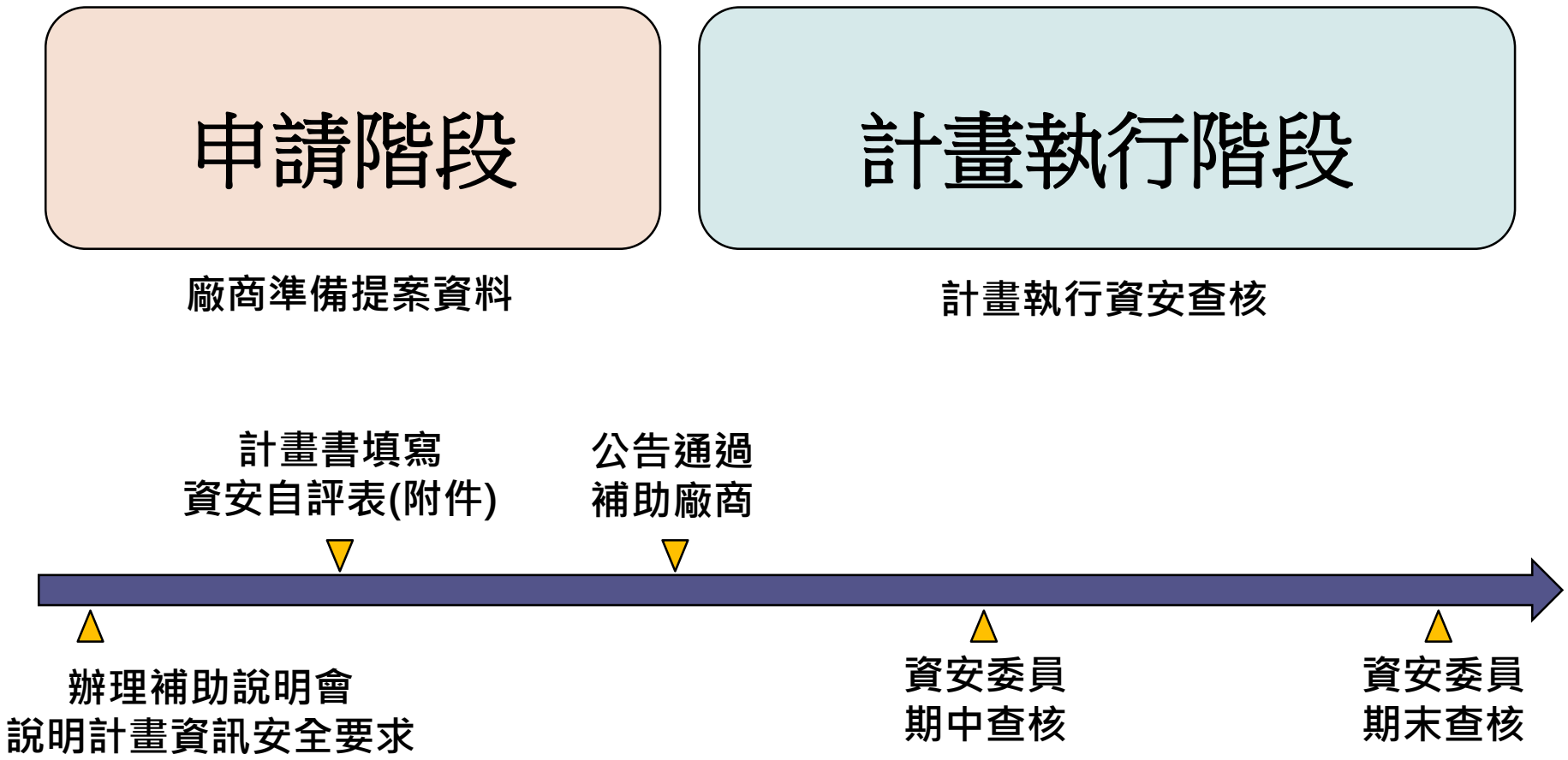
簡報大綱

壹、資安自評與查核流程

貳、「提案階段」資安規劃

參、「執行階段」資安要求

壹、資安自評與查核流程


申請階段
計畫執行階段
廠商準備提案資料
計畫執行資安查核
計畫書填寫
資安自評表(附件)
公告通過
補助廠商
辦理補助說明會
說明計畫資訊安全要求
資安委員
期中查核
資安委員
期末查核

貳、「提案階段」資安規劃(1/3)

一、資安管理：參考 108 年行政院國家資通安全會報技術服務中心整理之「政府機關資安治理評估機制」，依據製造業現況擬訂資訊安全，建置及導入 35%以上應為國內業者產品及服務，計畫驗收至少須達下列要件。

依序	項目	說明
1	人員認知及訓練	經費編列可用於公司內部資安人力，及委外顧問，公司內部資訊人力需取得資通安全通識教育訓練，並定期召開會議。
2	存取控制管理	應具體說明網路安全管理、存取管理、家密管理等機制。
3	通訊與作業安全	應具體說明資安監控、資安防護、惡意軟體防護、遠距管理、電子郵件、安全性檢測，及資料備份等方式。
4	日誌記錄保存	應具體說明資安事件如何應對及日誌管理機制。
5	資安系統開發與安全維護	說明如何落實安全系統發展生命周期。

貳、「提案階段」資安規劃(2/3)

二、資安資源投入說明

(一) 請提案廠商須詳細填妥資安管理自評表

3. 【佐證資料說明】欄位，請填寫該評核項目之具體控制措施內容並檢附證明資料，或說明不適用的理由。

自評項目		項目說明	自我評核					佐證資料說明	顧問查核結果			
			符合	部分符合	不符合	不適用			符合	部分符合	不符合	不適用
人員認知及訓練												
會議召開	資訊安全部門是否至少每年召開 1 次資訊安全管理審查會議。	請受查驗計畫說明資安管理會議招開情形										
人員進用	員工正式任用時，應簽定貴組織制定的聘僱契約，其中應陳述員工對資訊安全的責任，並依規定簽署保密合約。	請受查驗計畫說明資安人員任用狀況				V		如勾選不適用，廠商須說明原因				
存取控制管理												
使用防火牆與 VPN	須有防火牆、入侵偵測等資安設備保護，若透過遠端連線進行管理則必須透過加密通道，登入時必須採用安全的身分鑑別機制。	請受查驗計畫提供網路架構圖，簡述防禦機制是否合理跟恰當。										

貳、「提案階段」資安規劃(3/3)

二、資安資源投入說明

(二)請提案廠商須說明資安支出規劃，資安人力可列入計畫經費，填寫範例如下。

資安項目	項目	內容說明	支出經費(元)	佔總經費比例
網站弱掃	資訊應用軟體服務弱點掃描-IP(數)	弱點掃描服務乃利用高效率弱點掃描工具，針對標的進行安全弱點掃描，評估掃描標的是否存在已知的安全弱點。，針對掃描結果提出相關建議與掃描報告提供統計摘要等報表資訊與相關建議與掃描報告，降低客戶遭受入侵的風險。	以「108年第5次共同性服務契約-資通安全服務」收費標準為例1,679/IP (主機弱掃)	X%

參、「執行階段」資安要求(1/6)

➢ 共同規範(1/3)

一. 提案時應提出完整資訊安全規劃，包含定期檢視內部資安防護流程並持續改 善，以達強化公司營運及臨時緊急應變之目的。

1. 資訊安全規劃，可包含內部人員認知及訓練、網路管理、資料安全、存取控 制、營運規範等。
2. 資安服務及產品功能包含網路及設備安全、資料安全、資安監控與事件回 應、網站安全、身份及存取控管、風險管理與法令遵循、雲端安全、訊息安全、資安教育訓練等。

二. 相關產品如已有國家資安相關檢測標準，須採用通過資安驗證(資安自主產品認證/能量登錄)之產品。

三. 提案廠商應由高階管理階層指派具決策主管人員負責協調資訊安全專案之計 畫執行及資源配置。

四. 資訊軟硬體不等同資安軟硬體，下列產品不可列入：虛擬主機、伺服器、雲端 服務、路由器等資訊類產品。

五. 若涉及個人資料收集、處理及利用，須符合工業局訂定之「製造業及技術服務 業個人資料檔案安全維護管理辦法」(詳見網站)。

參、「執行階段」資安要求(2/6)

➢ 共同規範(2/3)

六. 資訊安全組織：請指派公司之專責人員負責資訊安全計畫、執行、查核及 改善，並由管理階層指派高階人員負責協調專案資源。

七. 資訊安全計畫：請規劃資訊安全風險評估，可透過但不限於第三方單位執 行原始碼檢測、黑箱檢測或滲透測試等，並針對重大威脅及脆弱性必須規 劃資安防護解決方案。

八. 為配合審查流程透明化，計畫內所運用、分析、存取之資料及金流須落地。

九. 補助計畫簽約時，若委託資安服務業者應提供與資安業者簽訂之「合作意 願書」或「合約」等佐證資料。

十. 資訊安全項目經費應占總經費合理比例，驗收時應提供支付資安廠商之給 付證明、說明於該案中所提供之產品及服務、解決哪些資安需求等。

十一.資安業者不應有過度再外包的情形(不得超過資安經費的 50%)。

十二.使用的資安軟、韌、硬體產品，不得為中國大陸生產或開發。

參、「執行階段」資安要求(3/6)

➢ 共同規範(3/3)

十三.計畫內資安軟、韌、硬體產品，非國內(台製)之資安產品佔比不得超過資安經費的 50%；若有特殊情形，須於計畫書審查會中明文說明。

十四.列入資安人力核銷項目，相關員工必須具備以下至少一項(1)取得資安證照、(2)碩博士論文與資安相關、(3)曾在資安專業公司/機構從事資安相關工 程、服務等滿一年、(4)其他可資舉證之資安專業服務。(註：資安專業不同 於資訊專業。)

參、「執行階段」資安要求(4/6)

- **必要要求(1/3)**

一、人員認知及訓練

(一)每年召開一次資訊安全會議。

(二)應陳述員工 對資訊安全的責任，並依規定簽署保密合約。

二、存取控制管理

(一)網路安全：使用防火牆與 VPN。

(二)權限管理：保存核心系統存取管控及日誌紀錄。

(三)加密管理：

- 防竄改機制。
- 機敏保護資料之傳輸，使用及儲存。

三、通訊與作業安全

(一)實體環境控制

- 公用之個人電腦或終端機應設定登入控管。
- 密碼保護級強度設定之規範。

(二) 安全性檢測

- 定期更新電腦作業系統及與軟體。
- 保持軟體/韌體更新(安全性更新機制、失敗回復至前一個版本)。

參、「執行階段」資安要求(5/6)

- **必要要求(2/3)**

三、通訊與作業安全

(三)遠距工作管理

- 對於遠距工作場所規範。
- 限制遠端對安全網路的存取。

(四)資安防護

- 各個主機應安裝資訊安全防護軟體。
- 強制使用強密碼。

(五)資通安全監控

- 自我監測：資通訊系統應建立自我檢測功能。
- 監控及偵測容量使用情況 (CPU、記憶體、存取空間等)。

(六)資料備份「321 原則」(3份備份、2種不同形式、1份異地)。

四、日誌記錄保存

(一) 具備日誌與稽核機制，且須存查至少一年。

(二) 紀錄存取機敏資料。

(三) 密鑰管理的職責分離。

(四) 異常日誌紀錄。

參、「執行階段」資安要求(6/6)

- **必要要求(3/3)**

五、資安系統開發與安全維護

(一)生命週期維護

- 進行安全檢測：資通訊系統須於上線前及營運期間定期進行弱點掃描或滲透測試。
- 進行備援或備份之復原演練：應建立業務持續運作計畫(BCP)或災難復 原計畫 (DRP)，定期進行演練並持續改善。

簡報結束
敬請指教