

資通訊委外安全管理要求

113.07.16

購案標的：大容量儲存系統及周邊設備

一、本次購案標的是否為會內自行或委外開發的網站、APP 或其他資通系統的建置、維護？

是，本購案標的資通系統的防護等級是：普級 中級 高級。

否

二、廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本會資通安全管理及保密相關規定。

三、廠商履約人員國籍不得為中國籍，且所使用之資通設備、服務、軟體及元件不得為中國所有（大陸品牌）。

四、廠商辦理本專案之相關程序、人員、設備及環境，應具備完善之資通安全管理措施或通過第三方驗證。

廠商應通過第三方驗證（ISO 27001 最新可被驗證版本）。第三方驗證機構須經財團法人全國認證基金會 TAF 認可。

廠商辦理本專案之相關程序、人員、設備及環境須具備完善之資通安全管理措施。

五、廠商於本購案履約執行之專案成員或履約人員應具備該領域之專業證照，以保證履約交付內容之品質，並配置「資通安全專業人員」，以及提供資通安全專業人員擁有之資通安全專業證照（數位發展部資通安全署公告之資通安全專業證照清單之一）或具有類似業務經驗證明。

六、本專案不得複委託（分包或轉包）；本專案得複委託，複委託之受託者應具備與本專案廠商相同之完善資通安全管理措施或通過第三方驗證。

七、本專案業務涉及國家機密，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

八、廠商應提供本專案資通系統（客製化）之安全性檢測證明，其檢測工具不得為自由軟體，且需提供檢測工具名稱、版本及原始報告，以及確認檢測時之弱點資料庫已更新至最新版本（檢測報告必須載明檢測日期及檢測工具名稱、版本，以及弱點資料庫更新日期）。

檢測項目如下：

系統主機弱點掃描

網頁弱點掃描

滲透測試

原始碼檢測

- 九、承前項：本專案資通系統為本機關核心資通系統或本專案金額達新臺幣一千萬元（含）以上，應由第三方進行安全性檢測及提供檢測報告，第三方機構應為現行「電腦軟體共同供應契約」之資通安全服務暨資訊服務廠商，且檢測項目須與廠商「電腦軟體共同供應契約」合格項目相符，所提供之檢測報告規格、要求亦須符合「電腦軟體共同供應契約」要求。
- 十、本專案資通系統開發與維護如使用第三方軟體或元件，應提供第三方元件清單（包含版本及是否可以持續更新等資訊），並說明其來源與授權證明。
- 十一、廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性。
- 十二、本專案標的涉關鍵基礎設施(或本機關指定之設施)，廠商及分包廠商之履約人員於進場或參與工作前，應提出 6 個月內核發之「警察刑事紀錄證明」(外國人應提出該國籍政府核發之類似文件，並經公證或認證。但申請入國簽證時，已備行為良好之證明文件者除外)；其證明內容應記載無犯罪紀錄，並經機關審核同意，始得進場或參與工作。屬臨時性進場者(例如送貨司機及其隨車人員)得免提送上開證明文件，但應接受本機關或其指定之單位或人員(例如但不限於專案管理單位)全程陪同或監督管理。
- 十三、廠商於執行本專案及保固服務期間，若知悉或發生資通安全事件時(含本專案範圍及廠商內部管理範圍)，應於 1 小時內通知本機關及採行補救措施。
- 十四、本專案(含保固)終止或解除時，廠商應確返還、移交、刪除或銷毀履行契約而持有之資料，並提供切結書與說明資料之刪除或銷毀方式。
- 十五、於本專案(含保固)期間，本會得視需求或發生可能影響本專案之資通安全事件時，對廠商及分包廠商實施現場實地資安稽核，稽核範圍為本專案相關之程序、人員、設備及環境，廠商不得拒絕。稽核結果若不符合本專案約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本會通知後應於期限內完成改善，未依限完成者，依契約違約條款辦理。