

資安驗證與資安檢測服務採購規範書

購案名稱：資安驗證與資安檢測服務

一、工作項目及產出文件

1. 工作項目、具體成果與完成日期

編號	工作項目	具體成果	預計完成日期
*1	資安驗證評估規劃報告	● 內含細部執行規劃甘特圖。 ● 遵守行政院所頒訂之各項資訊安全規範及標準(如行政院國家資通安全會報技術服務中心所頒訂之共通規範)，並遵守機關「資訊安全管理系統(ISMS)」等相關資訊安全管理及保密規定。 ● 完成指定場域依照 ISO27001 或 CNS27001 產出資安驗證評估規劃報告。	10 月 30 日
*2	資安驗證文件	● 完成依照 ISO27001 或 CNS27001 資安驗證文件。	11 月 28 日
*3	網站資訊安全弱點檢測	● 完成指定之 URL 網站弱點掃描檢測，測試標準為 OWASP Top 10。 ● 於檢測完成後提供檢測報告，修復期間提供 E-Mail 弱點諮詢服務。	12 月 15 日
*4	程式源碼檢測	● 完成指定之網站程式源碼檢測，測試標準為 OWASP Top 10、SANS TOP 25。 ● 於檢測完成後提供檢測報告，修復期間提供 E-Mail 弱點諮詢服務。	12 月 15 日
*5	網站滲透測試	● 完成指定之 URL 網站滲透測試。 ● 測試標準：OWASP、OSSTMM。 ● 於檢測完成後提供檢測報告，修復期間提供 E-Mail 弱點諮詢服務。	12 月 15 日
*6	資安驗證執行報告	● 遵守行政院所頒訂之各項資訊安全規範及標準(如行政院國家資通安全會報技術服務中心所頒訂之共通規範)，並遵守機關「資訊安全管理系統(ISMS)」等相關資訊安全管理及保密規定。 ● 完成指定場域依照 ISO27001 或 CNS27001 產出資安驗證規劃執行報告。	12 月 15 日
*7	臨時交辦工作。	完成臨時交辦工作。	12 月 15 日

2. 產出文件、時間與配合事項

- (1) 115 年 12 月 15 日前繳交執行報告，報告內容提供 115 年 12 月 15 日完成之工作項目具體成果的相關佐證資料與報告。
- (2) 本案依招標文件規定不允許大陸地區廠商參與，並不得採購大陸品牌產品，且避免採購具資安疑慮之資通訊產品或服務。

二、廠商條件

- (1) 承接本案之廠商須具備以下條件，並請提供證明文件
 - ✓ 參與國際資安演練競賽作品。
 - ✓ 共契服務評鑒與輔導合作單位/公司與政府單位經驗與實績。
 - ✓ 公司通過 ISO 27001、ISO 20000 及 ISO 22301 等驗證。
- (2) 承接本案之廠商所需使用合法之軟體，不得違反智慧財產權、著作權及專利法之規定，如有違反事情發生，須承擔所有法律責任。需提供檢測工具合法之軟體商業使用授權證明，並提供不違反智慧財產權、著作權及專利法之承諾書。

三、權利歸屬：凡因執行此購案所產生之智慧財產權均屬於工研院所有。

四、付款方式：付款方式分兩期，115 年 10 月 30 日交付編號*1 的產出報告後，支付本案金額之 40%為第一期款；交付編號*2~編號*7 的執行報告，驗收後支付本案金額之 60%為第二期款，結案完成日期為 115 年 12 月 15 日。

五、其他：須配合工研院至指定地點進行相關工作事項，並配合出席相關資安稽核、諮詢與討論會議，因配合交付項目所衍生出之工作與費用由得標廠商負責。

六、結案驗收：結案驗收時按上述有關條款辦理，交付檢索資料之內容經請購單位確認，合於需求者方可完成驗收，廠商須配合進行檢索資料說明。

七、保固：保固期間為結案後起計一年期，期間如有因本案範圍內之需求產生之服務工作，由得標廠商配合完成，並負責衍生之費用。