附表二

國軍委外資通系統服務安全管控項目查核表

填表日期：　　年　　月　　日

防護需求分級：□普 □中 □高

系統名稱					
計畫申購單位		承辦人		單位主管	

※計畫申購單位應依防護需求分級將相應之資通安全管控措施項目納入契約規範，非相應分級之項目毋須填列；其中適用分級為普、中、高級全部等級者，所有系統均須列入或選擇【部分列入】。

※計畫申購單位若基於預算限制等因素，可接受資安風險而選擇【部分列入】，則需於備註欄註明原因。

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
1. 委外廠商應具備以下要求與資格： (1)廠商辦理委外業務之相關程序及環境，應具備完善之資通安全管理措施（需提供證明文件供甲方審認）或通過第三方驗證(如：CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準)。 **※參考資通安全管理法施行細則第四條第一點。** (2)廠商應配置至少 1 位擁有資通安全專業證照(可參照行政院【https://nicst.ey.gov.tw】公告之證照列表)或具有_____業務經驗（需提供證明文件供甲方審認）之資通安全專業人員。 (3)委外業務複委託情形： ◯不得複委託。 ◯得複委託，廠商應於企劃書說明複委託之範圍與對象，同時廠商對於複委託之受託者應至少有下列要求：(依需求擇項) □資通安全專業證照或具有_____業務經驗之資通安全專業人員 □履約期間內，專案成員至少由甲方（或其代理人）完成___小時資安教育訓練 (4)涉及利用非廠商自行開發之系統或資源者，廠商應標示非自行開發之內容與其來源及提供授權證明。	全部	□列入採購評選（審）評分表 □未辦理採購評選（審）之籌獲案（如小額採購），由計畫申購單位於選商前自行評估廠商資格。	本項目應納入企劃書及採購評選評分表(依需求修訂)

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
2. 針對承包國軍委外專案業務之相關人員(含分包商）應經單位保防部門完成安全調查，並不得為陸（港、澳）籍人士，經保防部門安全查核未通過者，及大陸地區與港澳地區人民，嚴禁參與專案；另應於相關規定及合約中，規範外部組織設資安管制編組及遵守國防部相關資訊安全管理規定。	全部	第__頁	
3. 廠商應依契約要求提出「專案管理工作計畫書」(含光碟及書面文件)，內容應包括資安防護管控作業之工作項目、參與人員、執行敘述、作業時程交付甲方（或其代理人）審查。人員、工作項目如有異動時，需於3個工作天前主動將異動資料以書面函報甲方（或其代理人）審查。	全部	第__頁	
4. 廠商須於決標次日起 14 個工作天內簽署甲方（或其代理人）「保密切結書」，若須提前參與本案，須於實際參與專案前完成簽署。	全部	第__頁	
5. 應遵循行政院資安管理法及本部資安管控規範等相關規定與要求，強化資訊安全管理，確保資料傳送、儲存及流通之安全。	全部	第__頁	
6. 合約規範或保固期內，定期及不定期配合甲方（或其代理人)實施網站與主機之弱點掃描作業所提之弱點掃描報告，廠商須於甲方(或其代理人)通知日起_____個日曆天內完成弱點改善(完成風險修正或降低至甲方可接收之風險）。	全部	第__頁	
7. 應用系統開發測試階段及版本更新時，應執行原始碼檢測(1 次)，廠商須於甲方（或其代理人）通知日起_____個日曆天內完成弱點改善（完成風險修正或降低至甲方可接收之風險）。	全部	第__頁	
8. 合約規範或保固期內，定期及不定期配合甲方（或其代理人）實施之資安檢測(資通系統屬機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，機關應自行或另行委託第三方進行安全性檢測）、本部及行政院網路攻防演練等作業所提之檢測報告，廠商須於甲方（或其代理人）通知日起 14 個日曆天內完成弱點改善（完成風險修正或降低至甲方可接收之風險）。	全部	第__頁	
9. 原則禁止廠商透過網際網路(民網)遠端維護系統。	全部	第__頁	
10. 系統發生資通安全事件或資安弱點檢測驗證成功(如行政院網路攻防演練、資料外洩、被竊取、	全部	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
駭客入侵等情事)，須主動通報甲方（或其代理人）。另接獲甲方（或其代理人）通知資安事件時，須 24 小時內協助甲方（或其代理人）完成系統修復及損害管制，並於 7 日曆天內提供改善情形及建議報告書。			
11. 系統之測試及正式作業環境應作區隔;正式作業及測試系統，應採用不同的登入程序。	全部	第__頁	
12. 程式變更須於測試環境測試無誤並保留變更前後差異之紀錄，並由甲方（或其代理人）管理人員確認後，於甲方（或其代理人）指定時間安裝程式變更於正式作業，如程式變更後無法正常運作，則須立即恢復原狀。廠商應於更新完成後_____個日曆天(或工作天，不得逾 10 個工作天）內提供相關說明文件，如有必要需安排教育訓練。如程式變更涉及系統文件修正，應於系統變更完成後一個月內修正完成送交甲方(或其代理人）。	全部	□列入 第__頁 □部分列入 第__頁	
13. 程式變更正式作業前應依「國軍軟體發展管理作業規定」針對系統做相關資訊安全檢測，並提交甲方（或其代理人）指定之檢測報告格式，檢測報告須證明系統無中、高風險之弱點。(廠商需於初次檢測時提出檢測軟體能偵測 OWASP TOP 10 項目的檢測報告)。 **※如系統屬單位核心系統，則此項須全數列入**	全部	□列入 第__頁 □部分列入 第__頁	
14. 配合本部資訊安全風險評估及安全管理需求，機敏資料存於資料庫或其他儲存媒體時，採用對稱式或其他加密方式，將機敏資料加密成密文後儲存，若有傳輸機敏資料時，採用 HTTPS 等加密協定，確保機敏資料以密文方式傳輸。	全部	第__頁	
15. 系統須將存於資料庫內之使用者密碼以加密(不可逆)處理儲存，以防止使用者密碼為使用者以外人員知悉。	全部	第__頁	
16. 系統加密方式，應採用公開、國際機構建議安全且未遭破解之演算法(如 AES 對稱式加密、RSA 非對稱式及 SHA-2 安全雜湊等演算法)。並使用該演算法支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。	全部	第__頁	
17. 系統採用之加密金鑰或憑證，應配合加密金鑰或憑證週期，於到期前進行更換。	全部	第__頁	
18. 系統應具備帳號管理相關功能，包含帳號之新	全部	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
增、停用、刪除及使用者權限建立控制機制，且帳號權限應以最小權限為原則，以確保系統安全；資訊系統應具備唯一識別及鑑別使用者，不應有共用帳號之行為並應識別及鑑別非機關使用者。			
19. 若應用 ActiveX 與 Java applet，應採取相關防護措施(如：加註警語提醒使用者將下載之相關元件為何)。	全部	第__頁	
20. 系統發生錯誤時，使用者頁面僅顯示簡短訊息及代碼不包含詳細的錯誤訊息，且系統管理者介面需限制存取來源。	全部	□列入 第__頁 □部分列入	
21. 系統檢核使用者產生之密碼，系統應確保一般使用者密碼長度至少 8 位字元、特權帳號密碼長度至少 12 為字元，且均應包含大寫英文字母、小寫英文字母、阿拉伯數字及特殊符號等至少 3 種組合，系統須提供密碼最短及最長之效期限制，且要求密碼最短效期限制為 1 天，最長之效期限制要求使用者至少 3 個月修改一次密碼，且密碼不可與前 3 次相同，並於畫面上提示使用者如何產生強化密碼。	全部	□列入 第__頁	
22. 系統須建立將使用者異動情形記錄於稽核日誌之功能，且系統應提供查詢系統帳號之建立、修改、啟用、禁用及刪除動作、授予權限功能及異動紀錄。廠商非經甲方（或其代理人）同意不得新增或刪除系統帳號及異動權限。另系統須提供資訊系統管理者帳號所執行之各項功能稽核日誌，稽核日誌不得由管理者刪除，須由特定授權之人員才得以進行稽核檔之異動、刪除作業，並留軌跡紀錄。	全部	□列入 第__頁 □部分列入 第__頁	
23. 應用系統伺服器上之應用程式不可以賦予資料庫及作業系統最高權限帳號，應給予最小需用權限，以免惡意人員透過資料庫管理系統破壞內部資訊作業。	全部	第__頁	
24. 廠商如接獲系統異常無法正常運作通知，應配合甲方（或其代理人）訂定系統可容忍中斷時間，於 4 個小時內（依合約規範調整）做緊急處理，並於系統可容忍中斷時間（　　）內回復系統運作。 **※（）內請填入可容忍中斷時間（含時間單位）**	全部	第__頁	
25. 廠商應配合甲方（或其代理人）訂定之可容忍資	全部	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
料損失時間（　　），建立執行系統源碼和資料備份機制。 **※（）內請填入可容忍中斷時間（含時間單位）**			
26. 廠商應配合甲方（或其代理人）主機移機或汰換，將系統原主機資料(包含應用系統、資料庫及檔案等)移轉至新環境，進行相關網路連線設定和系統測試，以確保系統運作正常。	全部	第__頁	
27. 開發或維護系統時，廠商應配合甲方（或其代理人）要求，對於所開發(維護)之應用系統之系統運作環境(如：作業系統版本、資料庫系統版本或軟體版本...等) 之更動，協助進行事前評估及協助轉置，且於前述更動前、後，須進行系統測試，以確保系統運作正常及符合甲方（或其代理人）伺服器端及用戶端構型相容性。	全部	第__頁	
28. 維護(保固)期間內甲方（或其代理人）因軟硬體設備異動，因而涉及原系統環境變更時(如版本變更或安裝 Patch)，廠商應提供技術服務及辦理變更前、後系統測試，並依甲方（或其代理人）需求協助關閉軟硬體中不必要之服務及埠口。	全部	第__頁	
29. 維護期間內如因故終止服務，廠商應於甲方（或其代理人）要求或合約規範之期限內，將甲方（或其代理人）存在於委外廠商處的資料或設備移轉至甲方處或甲方（或其代理人）指定單位。	全部	第__頁	
30. 系統需符合 IPV4 與 IPV6 協定。	全部	第__頁	
31. 配合甲方（或其代理人）委外稽核作業之查核，廠商（含分包商）應配合接受甲方（或其代理人）或委託單位之稽核或查核等業務，其範圍包括本專案開發環境、設備、人員及系統之管理機制等；另專案如有允許複委託項目，廠商應針對複委託項目督管分包商資安檢核。 **※開發、測試及正式環境均須符合本部「專網專用、實體隔離」政策，且開發人員活動區域(空間)應有明確限制。**	全部	第__頁	
32. 資訊系統應就涉及機敏資料部分建立稽核日誌，並確保資訊系統有稽核特定事件(至少包含更改密碼、登入成功及失敗、資訊系統存取成功及失敗)之功能，採用單一日誌紀錄機制，確保輸出格式的一致性，且僅限特定授權之使用者能存取稽核日誌。	全部	第__頁	
33. 稽核日誌需具備以下項目:	全部	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
(1)識別使用者之ID，不可為個資類型。 (2)時間應記錄至秒等級。 (3)執行的功能或存取資源名稱。 (4)執行結果或事件描述。 (5)網路來源與目的位址。 (6)其他本部要求之項目。			
34. 廠商應評估及配置適切之稽核日誌所需之儲存容量，並至少保留1年（含）以上之稽核紀錄，如發生稽核日誌處理失效時(如儲存容量不足)，應自動採取適當之因應措施，如覆寫最舊的稽核日誌或經甲方（或其代理人）同意之措施，並於(　　)小時內主動通報系統管理者及其指定人員。 **※含個人資料之應用系統紀錄資料應至少保存5年以上；未含個人資料之應用系統紀錄資料應至少保存1年以上。**	全部	第__頁	
35. 應用系統主機須建立時間同步機制。	全部	第__頁	
36. 本部監控資訊系統如偵測到攻擊或異常情形，廠商須協助對事件進行分析和說明，以釐清不尋常之活動。 針對資訊系統所使用的外部元件或軟體(含開源軟體)，廠商應注意其相關安全漏洞通告(如技服中心公告訊息)，定期評估更新，且不得使用預設密碼。	全部	第__頁	
37. 系統除允許匿名存取的功能外，所有功能都必須於已通過身分驗證後才允許存取。網站除公開區域外，其他網頁皆需於身分驗證登入成功後，才得以存取。系統傳遞身分驗證相關資訊(如：帳號、密碼等)應採用加密傳輸，不以明文傳輸，以避免資訊被攔截或監聽竊取。	全部	第__頁	
38. 系統需提供稽核日誌查詢介面，供特定授權之人員得以進行稽核檔查詢作業；甲方(或其代理人)有審查稽核事件需求時，應依需求協助產出稽核事件之紀錄，供承辦人員審查。	中 高	第__頁	
39. 廠商應提供應用系統重要程式完整性定期驗證機制，偵測未授權變更特定軟體及資訊，如採用版本管控程式(如 SVN)比對機制或其他同等效益之替代方式。當發現違反完整性時，應協助進行資料回復作業。	中 高	第__頁	
40. 系統應禁用閒置帳號。亦即使用者帳號連續	中	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
(　　)日未登入，系統即予以鎖定或禁用。 **※（）內請填入系統可容許未登入時間**	高		
41. 系統應設計連線閒置時自動登出或自動連線中斷(Session Timeout)功能，其中含敏感資料之系統不得超過 15 分鐘。	中 高	第__頁	
42. 稽核資訊應運用雜湊或其他適當方式確保其完整性	中 高	第__頁	
43. 身份驗證機制應防範自動化程式之登入或密碼更換嘗試。	中 高	第__頁	
44. 密碼重設機制應對使用者重新身分確認後，發送一次性及具有時效性符記。	中 高	第__頁	
45. 廠商應協助建置備援設備以取代原服務中斷時，可於容忍時間內提供服務。	中 高	第__頁	
46. 系統應配合甲方（或其代理人）所定之情況及條件(如上班時間或指定 IP 來源)，限制使用系統。	高	第__頁	
47. 系統應提供監控系統帳號違反正常使用狀況之記錄功能(如：半夜連線執行特定功能)，並於發現違常使用或嚴重錯誤時提供回報機制(如：email 或簡訊通知)。	高	第__頁	
48. 廠商應建立機制每日備份稽核日誌到與原系統不同之實體系統，並運用加密機制，保護稽核資訊之完整性。	高	第__頁	
49. 廠商應配合提供重要資訊系統軟體與其他安全相關資訊之備份資料，以便甲方（或其代理人）儲存在與運作系統不同地點之獨立設施或防火櫃中。	高	第__頁	
50. 對帳號之網路存取，應採取多重認證技術(如：鎖 IP、採用動態密碼認證)；在使用者建立連線前，應識別允許存取之特定來源(如：IP)。	高	第__頁	
51. 加密金鑰應採取安全管理措施。	高	第__頁	
52. 系統之服務水準，經甲方（或其代理人）評估須滿足高可用性需求者，應採取分散式或叢集伺服器架構，以使當系統發生錯誤情況或硬體毀損時，服務仍能正常運作。	高	第__頁	
53. 系統應定期執行軟體與資訊完整性檢查(如：同位元檢查、循環冗餘檢查、密碼雜湊函數)。	高	第__頁	

資通安全管控措施項目	適用分級	列入RFP（依需求修訂）標明頁數	備註欄
54.應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	第__頁	
資訊(安)部門審查意見			