附表三

列管軍品廠商 資訊系統安全查核基準表	
辦理項目	辦理內容
資訊安全管理系(Information Security Management System，ISMS)之導入及通過經濟部標準檢驗局授權委託之「財團法人全國認證基金（TAF)」認證之機構之驗證	專案有關資訊系統（含使用乙太網路之工業自動化控制系統）導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準（如行政院資安處「關鍵資訊基礎設施資安防護建議」所列)，並通過我國 TAF 認證之機構驗證(如標準尚無 TAF 認證者則依經國際標準（ISO 或 IEC）認證之系統驗證機構，且經本辦法主管機關認可)，應持續維持其驗證有效性。
資通安全專業證照	專案有關資通系統導入 CNS 27001 或 ISO 27001 或 IEC 62443-2-1 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，並完成上述系統或標準的中立公正第三方驗證，驗證範圍應包含資訊科技(IT)安全與作業科技(OT)安全，且持續維持其驗證有效性。
限制使用危害國家資通安全產品	1、除因業務需求且無其他替代方案外，不得採購及使用行政院核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 2、必須採購或使用危害國家資通安全產品時，應具體敘明理由，經行政院核可後，以專案方式購置。 3、已使用或因業務需求且無其他替代方案經行政院核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。
資訊資產管理	1、資產清冊：機敏辦公室內應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之資產清冊。

	2、可移除式媒體之管理：機敏辦公室內電腦應運用軟體管制可移除式媒體存取作業。
實體與環境安全	1、設備安全應依安置地點、環境之特性設置適當防護措施，以降低因環境不安全引發的危險及避免未經授權存取系統的機會。設置在外部以支援業務運作的資訊設備，亦應遵守資訊安全管理規定，維護其實體與環境安全。 2、含有儲存媒體的設備項目（如：硬碟、磁帶），應在報廢、維修、汰除、移轉等處理作業前移除或完成實體破壞，並詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經清除或無法加以讀取。 3、應律定人員辦公處所之個人電腦使用及桌面安全管理政策與規定，以防範文件或資訊被未經授權的人員取用、遺失或被破壞。
資訊作業安全管理	1、專網電腦應使用防毒軟體、防火牆及相關電腦系統資安設定及措施，專屬網路內應依任務特性參酌使用相關資安防護設定及措施，單機電腦亦應使用單機版防毒軟體及相關電腦系統資安設定及措施，以防制電腦病毒及惡意程式攻擊，降低危害風險。 2、禁止使用未取得相關授權的軟體程式，以防制電腦病毒及惡意程式之攻擊。 3、資訊紀錄應安全存管，屬機密資訊者，應實施加密，且不得儲存於對外開放之資訊系統，各項資訊稽核紀錄妥慎保存並設定存取權限及程序，保

	存期限應為一年以上。各資訊系統管理者之系統存取活動亦應紀錄管制。 4、硬體設備安全：伺服主機設備，除針對作業系統之資安設定外，亦應建立依使用者安全等級設定授權之機制，以管制硬體安全使用，且應禁止遠端設定、連線及控制作業；機敏辦公室電腦移出入時，須清除相關電磁資料及紀錄，以防止相關機敏資料外洩。 5、網路安全管理：機敏辦公室電腦應與其他無關聯之網路完全隔離，與其他網路間的資訊交換，須經獨立「檢疫」程序，以確保所交換資訊的安全性。
存取控制	1、應建立使用者存取管理程序，明確律定資訊系統的存取授權，針對存取授權原則、安全等級與分類、保護資料與服務存取責任義務、註冊、帳號與權限管理等，以書面或電子郵件方式告知使用者系統存取授權範圍，確保授權人員對資訊系統存取及防止非經授權之不當存取。並依據資安等級劃分及分類，針對不同等級資訊，課以相對責任。 2、密碼設定原則：機敏辦公室資訊帳號密碼須符合複雜度要求並不得少於定十五碼以上。 3、網路設備須具備網路管理與網路安全管理功能，並可設定交換埠使用之限制。 4、應建立使用者對維護合法有效存取控制措施之認知及所負責任，要求妥慎保管密碼使用、保護設備安全、加強文件輸出管制及降低隨身文件資

	訊損害風險，以防制非法使用者存取資訊，及防治其破壞、竊取資訊設備。 5、廠商於境外存取遠端資料時，應由該廠商指定權責主管逐筆辦證同意後始得辦理存取。
危機處理	1、危機處理機制應包含天然、人為、資訊安全及其他災害等應變作為，律定危機處理之人員責任、緊急應變措施安排及建立緊急應變作業程序、流程，並以書面或其他電子方式記載，以保護資訊資產與其相關資訊系統遭破壞時，可藉以維持或恢復運作，並確保資訊的可用性在要求時間內達到所要求等級。 2、應建立管理責任與程序，以確保對資訊安全事件與弱點，能迅速、有效及有序處置，並依程序、通報、監視及評估資訊安全事件之整體管理過程中，建立持續改進的流程。 3、機敏辦公室發生資訊安全事件時，應立即通報甲方，並依程序蒐集、保存及呈現數位證據。
備註： 1.資通安全專業證照，指由本辦法所列舉與行政院公布之資通安全專業證照清單。 2.危害國家資通安全產品，指對國家資通安全具有直接或間接造成危害風險，影響政府運作或社會安定之資通系統或資通服務；如「國軍辦理涉及大陸地區財物或勞務採購注意事項」要求事項。 3.專案有關資通系統若不涉及資訊科技(IT)安全或作業科技(OT)安全，得免予導入 CNS/ISO 27001 或 IEC 62443-2-1 等資訊安全管理系統標準。 4.查驗標準視廠商實際情況裁量，惟廠商應提出至當可行之配套措施，經主管機關審視可行性及安全性後，予以裁定結論。	