附表六

人員安全查核結果表		
一、廠商名稱：		
二、查核對象：〇〇〇等〇員		
查核項目	分項查核結果	備考
犯國家機密保護法第三十二條第一項至第三項、第三十三條第一項至第三項或第三十四條之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
犯刑法第一百零九條第一項至第三項、第一百十一條第一項、第二項、第一百三十二條第一項或第三項之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
犯貪污治罪條例第四條第一項第五款、第五條第一項第三款或第十一條第一項至第四項之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
犯營業秘密法第十三條之一第一項、第二項、第十三條之二第一項或第二項之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
犯國家安全法第五條之一第一項或第二項之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
犯陸海空軍刑法第二十條第一項至第三項、第二十一條或第二十二條第一項至第三項之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
執行國防事務人員為大陸地區、香港、澳門人士。	□無 □有	
資金背景符合陸資廠商條件。	□無 □有	
涉刑法內亂、外患、重利、背信、侵占及詐欺等罪、違反洗錢防制法之罪。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。	□無 □有	
其他有關安全事務，經研判足以影響國防安全或有危安疑慮。		
安全查核結果	□符合　　□未符合	
未符合內容		
查核人員簽證		

調查完成時間	年　　月　　日

設施(備)安全查核結果表

一、廠商名稱：

二、查核廠房：

查核項目	查核內容	分項查核結果	備考
庫房	為鋼筋混凝土建築，設置空間牆面為 RC 結構，空間內之窗戶及通風口必需設有防盜鐵窗，且具檢驗合格之消防及空調設備。	□符合 □未符合	
照明	照明設備應妥適設置於出入口及建物周遭(含主要道路)入侵警報啟動後即自動開啟。	□符合 □未符合	
出入門及鎖鑰	庫房出入門之材質須為金屬防火、防盜門，並具兩道鎖鑰裝置輔以高度安全掛鎖及遮蔽式搭扣，鑰匙須分開安置並指定由兩人保管及管制進入（即兩位授權保管人須同在現場始得開啟進入)，嚴禁使用萬用或複製鑰匙。	□符合 □未符合	
圍牆	圍牆須安裝入侵警監系統(intrusion detection system, IDS)。	□符合 □未符合	
監控與警戒系統	須佈署二十四小時警衛或警衛結合防止入侵警監系統（intrusion detection system, IDS)；監控範圍包含庫房及廠商管控之全部場域，且需建置中央監控站並具備第三方監控、警報功能且需連線至主管機關指定地點。警監系統之線路應具備適當防護，系統配置圖說及維護契約應提交主管機關辦理審查，就主管機關審查意見應無條件完成改善。但當警監系統未運作時，二十四小時警衛監控為必要之安全措施。	□符合 □未符合	
進出設施之管制	需設置門禁系統，相關人員欲於機敏品項儲放設施執行任何活動，須由兩位指定授權人同時抵達現場後始得進行，鎖鑰裝置及相關程序之規劃，應確保個人在無隨扈或監視之任何情況，均無法獨自進入庫房。	□符合 □未符合	

保　　全	雇用之保全需為政府核准設立之保全公司；入侵警報啟動後第一波支援人員需於十五分鐘內抵達現場，第二波於三十分鐘內抵達，保全契約需包含應變機制，應提交主管機關審查，就主管機關審查意見應無條件完成改善。	□符合 □未符合	
支援協定	本契約標的之履約場所需協調轄區派出所設置巡邏點，並完成支援協定，申辦過程主管機關應提供必要協助。	□符合 □未符合	
監控記錄	各項門禁、警報、監控設備之電磁、紙本紀錄應保存五年，主管機關得隨時調閱、提供，廠商不得拒絕。	□符合 □未符合	
系統重置	入侵警報啟動後應立即通知主管機關，並俟主管機關人員查驗無虞後始得重置系統。	□符合 □未符合	
其他有關安全事務，經研判足以影響國防安全或有危安疑慮。			

安全查核結果	**□符合　　□未符合**
未符合內容	
查核人員簽證	
調查完成時間	年　　月　　日

資訊系統安全查核結果表			
一、廠商名稱：			
二、查核廠房：			
查核項目	查核內容	分項查核結果	備考
資訊安全管理系統(Information Security Management System，ISMS)之導入及通過我國標準法行政院委託機構認證之機構驗證	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 /ISO 27001、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，並通過我國標準法行政院委託機構認證之機構驗證(如尚無委託者則依經國際標準(ISO 或 IEC）認證之系統驗證機構，且經本條例主管機關認可)；應持續維持其驗證有效性。	□符合 □未符合	
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。	□符合 □未符合	
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，不得採購及使用主管機關核定之廠商生產、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，經主管機關核可後，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主管機關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。	□符合 □未符合	
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。	□符合 □未符合	

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。	□符合 □未符合	
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	□符合 □未符合	

	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、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。	□符合 □未符合	
其他有關安全事務,經研判足以影響國防安全或有危安疑慮。			

安　全　查　核　結　果	**□符合　　□未符合**
未　符　合　內　容	
查核人員簽證	
調查完成時間	年　　月　　日