第四條 附表一

列管軍品廠商人員安全查核基準表		
項次	查核項目	查核基準
1	前科紀錄	未曾犯國家機密保護法第三十二條第一項、第二項、第四項、第三十三條第一項、第二項、第四項或第三十四條第一項至第四項之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。
2		未曾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、第三項，或內亂、外患、重利、背信、侵占及詐欺等罪、違反洗錢防制法之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。
3		未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。
4		未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。
5		未曾犯國家安全法第七條第一項至第四項之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。
6		未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。

7	國籍	具有中華民國國籍，且非大陸地區、香港、澳門人士。
8	廠商資金背景	非陸資廠商。
備註：		

第四條 附表二

列管軍品廠商設施（備）安全查核基準表		
項次	查核項目	查核基準
1	庫房	1.為鋼筋混凝土建築，設置空間牆面為RC結構。 2.空間內之窗戶及通風口必須設有防盜鐵窗。 3.具檢驗合格之消防及空調設備。
2	照明	1.出入口及建物周遭(含主要道路)均應妥適設置照明設備。 2.入侵警報啟動後照明設備應即自動開啟。
3	出入門及鎖鑰	1.庫房出入門之材質須為金屬防火、防盜門，並具二道鎖鑰裝置輔以高度安全掛鎖及遮蔽式搭扣。 2.鑰匙須分開安置並指定由二人保管及管制進入（即二位授權保管人須同在現場始得開啟進入)。 3.不得使用萬用或複製鑰匙。
4	圍牆	圍牆須安裝入侵警監系統(intrusion detection system, IDS)。
5	監控與警戒系統	1.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。 2.須建置中央監控站並具備第三方監控、警報功能且須連線至國防部指定地點。 3.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國防部辦理審查，就國防部審查意見應無條件完成改善。

		4.警監系統未運作時，須有二十四小時警衛監控。
6	進出設施之管制	1.須設置門禁系統。 2.相關人員欲於機敏品項儲放設施執行任何活動，須由二位指定授權人同時抵達現場後始得進行。 3.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。
7	保全	1.雇用之保全須為政府核准設立之保全公司。 2.入侵警報啟動後第一波支援人員須於十五分鐘內抵達現場，第二波於三十分鐘內抵達。 3.保全契約須包含應變機制，應提交國防部審查，就國防部審查意見應無條件完成改善。
8	支援協定	履約場所須協調轄區派出所設置巡邏點，並完成支援協定，申辦過程得請國防部提供必要協助。
9	監控紀錄	各項門禁、警報、監控設備之電磁、紙本紀錄應保存五年，國防部得隨時調閱。
10	系統重置	入侵警報啟動後應立即通知國防部，並俟國防部人員查驗無虞後始得重置系統。
備註： 1.參照國防部令頒「採購契約及委製協議書特別保密條款（範本）」。 2.本基準表之查核項目及基準屬原則性，如廠商設施(備)因空間、環境及不可抗力因素，應陳述窒礙原因，另提出精進作為或配套措施，經查核單位審視可行性及安全性後，完成查核結論判定。		

第四條 附表三

列管軍品廠商 資訊系統安全查核基準表	
查核項目	查核基準
資訊安全管理系統(Information Security Management System，ISMS)之導入及通過已簽署國際認證論壇(International Accreditation Forum,IAF)多邊相互承認協議之認證機構(含 TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構驗證	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 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),並通過已簽署國際認證論壇(IAF)多邊相互承認協議之認證機構(含 TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構驗證（證書須有驗證及認證機構之簽署，或提供認證機構之官方網站連結佐證)。
資通安全專業證照	1、資通安全專職人員及一般使用者每年須接受特定時數資通安全專業課程訓練、職能訓練或通識課程。 2、資通安全專職人員持有一張以上有效之資通安全專業證照。
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，不得採購及使用數位發展部核定之廠商生產、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，經數位發展部核可後，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數位發展部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。
資訊作業管理	1、資訊資產管理程序：應識別相關聯之資產，並製作及維持此等資產之資產清冊及管制作為。 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。 3、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

	。 4、落實資通安全風險管理及資訊作業委外管理程序相關計畫作為。
實體與環境安全	1、配置適當人員經單位資安長核定任命之資安專職人員，明定其業務職掌，並完備執行業務之紀錄（如內部稽核報告、到勤紀錄等） 分級項目： （1）一等列管軍品：四人。 （2）二等列管軍品：二人。 （3）三等列管軍品：一人。 2、設備安全應依安置地點、環境之特性設置適當防護措施，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。 3、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，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。 4、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，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、依列管軍品級別完成各項資通安全防護措施，建置資通安全偵測威脅偵測管理（SOC）機制，針對核心資通系統執行系統及網站弱點檢測、滲透測試、資通安全健診等作業。 2、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，防制電腦病毒及惡意程式攻擊。 3、禁止使用未取得相關授權的軟體程式。 4、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。 5、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。
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，應立即通報國防部，並依程序蒐集、保存及呈現數位證據。
資通系統開發及維護	針對自行或委外開發之資通系統，須依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施。
備註： 1.資通安全專業證照，指由數位發展部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及香港澳門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.查核單位得視廠商產業性質及實際情況裁量，由廠商提出可行之配套措施，經查核單位審視可行性及安全性後，予以判定查核結論。	

第六條 附表四

「００公司」執行國防事務人員查核名冊								
項次	姓名	出生日期	身分證統一編號	職務	性別	出生地	前次完成查核時間	類別
1	王○○	81.○.○		○○專案經理			114.○.○	完成列管軍品資格級別評鑑廠商
2	陳○○	82.○.○		○○專案助理			114.○.○	合格廠商
3	林○○	84.○.○		○○專案專員			114.○.○	下游供應廠商
合計：○員								
備註：執行國防事務人員如有異動時，完成列管軍品資格級別評鑑之廠商、合格廠商應檢附異動人員之國民身分證影本、警察刑事紀錄證明書及安全查核切結書，將異動人員名冊送政戰局審查，俟政戰局通知查核結果後，始得更換執行人員。								

第六條 附表五

列管軍品廠商非陸資及安全查核切結書

○○○（廠商）為參與國防產業，遵守本辦法之非陸資安全查核基準，保證本公司非屬「大陸地區人民來臺投資許可辦法」第三條第一項所定之投資人、第五條所定之陸資投資事業及其依我國法律設立之公司，並瞭解參與國防產業應通過審認具有國防安全履約能力，並應由(國防部政治作戰局)實施安全查核，承諾配合相關安全查核程序，提供查核所需書面或數位資訊文件、接受實地查訪、人員訪談等一切必要等事項。以上如有不實或未予配合，致安全查核無法進行，將限制參與國防產業之權利。

此致

○○○

廠商名稱：

代表人：

簽署人員/職稱：

簽署日期：

第六條 附表六

<table>
<tr><th colspan="4">人員安全查核結果表</th></tr>
<tr><td colspan="4">一、廠商名稱：</td></tr>
<tr><td colspan="4">二、查核對象：○○○等○員</td></tr>
<tr><td>查核項目</td><td>查核基準</td><td>分項查核結果</td><td>備考</td></tr>
<tr><td rowspan="7">前科紀錄</td><td>未曾犯國家機密保護法第三十二條第一項、第二項、第四項、第三十三條第一項、第二項、第四項或第三十四條第一項至第四項之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>未曾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、第三項，或內亂、外患、重利、背信、侵占及詐欺等罪、違反洗錢防制法之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>未曾犯國家安全法第七條第一項至第四項之罪，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>未曾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，經有罪判決確定。但受緩刑宣告、易科罰金、易服社會勞動者，不在此限。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>國籍</td><td>具有中華民國國籍，且非大陸地區、香港、澳門人士。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td>廠商資金背景</td><td>非陸資廠商。</td><td>□符合
□未符合</td><td></td></tr>
<tr><td colspan="2">安全查核結果</td><td colspan="2">□符合　　□未符合</td></tr>
<tr><td colspan="2">未符合內容</td><td colspan="2"></td></tr>
</table>

查核人員簽證		受查廠商 代表簽證	
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	查核基準	分項查核結果	備考
庫房	1.為鋼筋混凝土建築，設置空間牆面為RC結構。 2.空間內之窗戶及通風口必須設有防盜鐵窗。 3.具檢驗合格之消防及空調設備。	□符合 □未符合	
照明	1.出入口及建物周遭(含主要道路)均應妥適設置照明設備。 2.入侵警報啟動後照明設備應即自動開啟。	□符合 □未符合	
出入門及鎖鑰	1.庫房出入門之材質須為金屬防火、防盜門，並具二道鎖鑰裝置輔以高度安全掛鎖及遮蔽式搭扣。 2.鑰匙須分開安置並指定由二人保管及管制進入（即二位授權保管人須同在現場始得開啟進入)。 3.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	1.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。 2.須建置中央監控站並具備第三方監控、警報功能且須連線至國防部指定地點。 3.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國防部辦理審查，就國防部審查意見應無條件完成改善。 4.警監系統未運作時，須有二十四小時警衛監控。	□符合 □未符合	
進出設施之管制	1.須設置門禁系統。 2.相關人員欲於機敏品項儲放設施執行任何活動，須由二位指定授權人同時抵達現場後始得進行。 3.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	1.雇用之保全須為政府核准設立之保全公司。 2.入侵警報啟動後第一波支援人員須於十五分鐘內抵達現場，第二波於三十分鐘內抵達。 3.保全契約須包含應變機制，應提交國防部審查，就國防部審查意見應無條件完成改善。	□符合 □未符合	
支援協定	履約場所須協調轄區派出所設置巡邏點，並完成支援協定，申辦過程得請國防部提供必要協助。	□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，國防部得隨時調閱。	□符合 □未符合	
系統重置	入侵警報啟動後應立即通知國防部，並俟國防部人員查驗無虞後始得重置系統。	□符合 □未符合	
安全查核結果	**□符合　　□未符合**		
未符合內容			
查核人員簽證		受查廠商 代表簽證	
調查完成時間	年　　月　　日		

資訊系統安全查核結果表

查核廠房	列管軍品項目	列管軍品級別：
	1.甲	一等
	2.乙	二等
	3.丙	三等
備註	廠商申請多項列管軍品項目，其自評表以最高列管軍品級別進行填寫。	

查核項目	查核基準	分項查核結果	備考
資訊安全管理系統(Information Security Management System，ISMS)之導入及通過已簽署國際認證論壇(International Accreditation Forum,IAF)多邊相互承認協議之認證機構(含 TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構驗證	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 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），並通過已簽署國際認證論壇(IAF)多邊相互承認協議之認證機構(含 TAF)所認證之資訊安全管理系統驗證機構、稽核員驗證或註冊之國際專業機構驗證（證書須有驗證及認證機構之簽署，或提供認證機構之官方網站連結佐證)。	□符合 □未符合	
資通安全專業證照	1、資通安全專職人員及一般使用者每年須接受特定時數資通安全專業課程訓練、職能訓練或通識課程。 2、資通安全專職人員持有一張以上有效之資通安全專業證照。	□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，不得採購及使用數位發展部核定之廠商生產、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，經數位發展部核可後，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數位發展部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	
資訊作業管理	1、資訊資產管理程序：應識別相關聯之資產，並製作及維持此等資產之	□符合 □未符合	

	資產清冊及管制作為。 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。 3、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。 4、落實資通安全風險管理及資訊作業委外管理程序相關計畫作為。		
實體與環境安全	1、配置適當人員經單位資安長核定任命之資安專職人員，明定其業務職掌，並完備執行業務之紀錄（如內部稽核報告、到勤紀錄等） 分級項目： （1）一等列管軍品：四人。 （2）二等列管軍品：二人。 （3）三等列管軍品：一人。 2、設備安全應依安置地點、環境之特性設置適當防護措施，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。 3、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，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。 4、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，防範文件或資訊被未經授權的人員取用、遺失或被破壞。	□符合 □未符合	
資訊作業安全管理	1、依列管軍品級別完成各項資通安全防護措施，建置資通安全偵測威脅偵測管理（SOC）機制，針對核心資通系統執行系統及網站弱點檢測、滲透測試、資通安全健診等作業。 2、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	□符合 □未符合	

	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，防制電腦病毒及惡意程式攻擊。 3、禁止使用未取得相關授權的軟體程式。 4、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。 5、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。		
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	□符合 □未符合	

	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，應立即通報國防部，並依程序蒐集、保存及呈現數位證據。	□符合 □未符合	
資通系統開發及維護	針對自行或委外開發之資通系統，須依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施。	□符合 □未符合	
安全查核結果	**□符合　□未符合**		
未符合內容			
查核人員簽證		受查廠商 代表簽證	
調查完成時間	年　月　日		

第六條 附表七

安全查核結果通知書

受理日期：

廠商名稱		負　責　人	
受理案號		聯絡人電話	
查核種類	□初查□複查□定期查核□不定期查核		
查核結果	□ 符合		
	□ 未符合	原由	
查核效期	至　　年　　月　　日　有效		