# 列管軍品廠商安全查核辦法總說明

依國防產業發展條例（以下簡稱本條例）第四條第四項規定，申請列管軍品廠商資格級別認證完成級別評鑑之廠商，及本條例第五條第一項規定，合格廠商及列管軍品廠商之下游供應廠商均應辦理安全查核，並於第五條第二項授權主管機關訂定安全查核之對象、內容、實施方式、地點、程序、查核基準及其他相關事項之辦法。茲為促進國防工業廠商參與國防產業鏈，並強化內部安全措施，確保相關人員、設施（備）及資訊系統符合國防安全管控要求，以落實國防軍事科技安全維護之目的，爰訂定「列管軍品廠商安全查核辦法」（以下簡稱本辦法），其要點如下：

一、本辦法之訂定依據。（第一條）

二、本辦法之用詞定義。（第二條）

三、安全查核項目、對象及時機。（第三條）

四、安全查核之內容及基準。（第四條）

五、安全查核之方式。（第五條）

六、申請認證查核之程序。（第六條）

七、定期安全查核之程序及結果處理。（第七條）

八、不定期查核之方式及結果處理。（第八條）

九、不服安全查核結果之複查及處理。（第九條）

十、合格廠商落實自主安全管理及一般應注意事項。（第十條）

十一、列管軍品屬機密級以上案件，購案契約應納入特別保密條款，並依法辦理相關人員管制作業。（第十一條）

十二、本辦法之施行日期。（第十二條）

# 列管軍品廠商安全查核辦法

| 條　　文 | 說　　明 |
| --- | --- |
| 第一條　本辦法依國防產業發展條例(以下簡稱本條例)第五條第二項規定訂定之。 | 一、本辦法之訂定依據。<br>二、本辦法依本條例第五條第二項「前條第四項及前項安全查核之對象、內容、實施方式、地點、程序、查核基準及其他相關事項之辦法，由主管機關定之。」規定訂定。 |
| 第二條　本辦法用詞，定義如下：<br>一、安全查核：指對國防產業廠商人員、設施（備）、資訊系統及安全有關事務之安全管制措施，實施查驗評核。<br>二、機密工項：指核定機密等級以上建案、計畫之關鍵技術或涉及機敏資訊之工作項目。<br>三、下游供應廠商：指列管軍品得標廠商且涉機密工項之物料供應、製造或分包、協力之國內法人、機構或團體。<br>四、陸資廠商：指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。<br>五、建案單位：指武器系統與裝備軍事投資計畫之研發、生產或製造及設施工程案之主辦機關（構）、單位。<br>六、涉密人員：指受國軍單位委託或依契約從事國防事務，涉及國家機密之個人或機關（構）、民間團體之成員。 | 一、本辦法之用詞定義。<br>二、第一款為明確本辦法所稱安全查核之內涵，定明安全查核依本條例第四條第四項規定，包括對人員、設施（備）、資訊系統及安全有關之事務，實施查驗評核。<br>三、第二款為實施安全查核事項之範圍，定明機密工項之定義，指核定機密等級以上建案或計畫申購單位之關鍵技術或涉及機敏資訊之工作項目。<br>四、第三款為規範安全查核延伸對象，明定下游供應廠商之範圍，指列管軍品得標廠商物料供應、製造或分包、協力之國內法人、機構或團體，於參與列管軍品研發、產製、提供國軍維修服務時，不致因其人員、設施（備）、資訊系統及安全管理缺失，影響國防安全。<br>五、第四款為明確限制受大陸地區資金控制廠商，明定陸資廠商之涵義及範圍，指大陸地區人民來臺投資許可辦法第三條第一項所定大陸地區人民、法人、團體、其他機構或其於第三地區投資之公司，依該辦法規定在臺灣地區從事投資行為者，以及第五條所定投資人持有所投資事業之股份或出資額，合計超過該事業之股份總數或資本總額三分之一以上等陸資投資事業。<br>六、第五款為使本辦法與國軍建案規範結合，定明建案單位之定義，指軍事投資計畫之武器系統與裝備採購、生產、研發（製）及設施工程案之主辦機關（構）、單位。<br>七、第六款為明確參與國防事務人員之範 |

| | |
|---|---|
| | 圍，定明涉密人員之定義，指受國軍單位委託從事國防事務之民間團體或個人，為辦理、持有或使用、知悉國家機密事項之人員。 |
| 第三條　國防部應對參與列管軍品廠商及下游供應廠商實施安全查核；其項目、對象及時機如下：<br>一、申請認證查核：申請列管軍品廠商資格級別認證之國內法人、機構或團體（以下簡稱廠商），應於完成級別評鑑後三個月內辦理安全查核，符合查核基準者，核發該國防產業專長領域項別之列管軍品廠商資格級別認證合格證明（以下簡稱合格證明）。同時申請多項專長領域項別之合格證明者，得合併實施安全查核。已取得合格證明之廠商，再申請其他專長領域項別合格證明時，得以定期安全查核之查核結果審查。<br>二、定期查核：對符合查核基準廠商（以下簡稱合格廠商）及其下游供應廠商，每年辦理一次安全查核。<br>三、不定期查核：涉及機密列管軍品之得標合格廠商及其下游供應廠商，於新增資訊、變更資料或因特殊情形而有必要時辦理安全查核。<br>前項第三款所稱特殊情形，指具有下列情形之一者：<br>一、將機密資料隱匿、交付或洩漏予第三人之疑慮。<br>二、資金背景符合陸資廠商。<br>三、資訊系統遭病毒或駭客入侵存有資安疑慮。<br>四、涉密人員違反契約保密條款或未報准進入大陸地區、香港或澳門，或與大陸地區人民技術交流，衍生國防技術外洩疑慮。<br>五、合格廠商負責人、代理人、受僱人或其他從業人員犯本條例第六條第一項第一款、第二款、第五款、第 | 一、為落實國防安全管控，以達國防獨立自主之基本方針，申請列管軍品廠商資格級別認證合格證明並完成級別評鑑之國內法人、機構或團體，應每年定期對取得合格證明之廠商及列管軍品得標廠商之下游供應廠商持續辦理安全查核。因特殊情形且有必要時得不定期辦理安全查核，爰於第一項明定安全查核之項目、對象及時機。<br>二、第二項明定第一項第三款所稱特殊情形之態樣。<br>三、國防部為執行安全查核，得委由所屬機關國防部政治作戰局辦理，至其他安全項目之查核，因涉關國防部各單位及行政院相關機關業管權責，如國防部軍備局負責辦理設施(備)有關事項查核、國防部參謀本部通信電子資訊參謀次長室負責辦理資訊系統有關事項查核及其他相關部會協力查核等事項，爰於第三項明定就安全查核項目得委任所屬相關機關（構）或委託其他機關（構）辦理。<br>四、第四項明定受委任（託）機關（構）之保密義務。 |

| | |
|---|---|
| 六款之罪或有其他足以影響國防安全之情事。<br>第一項安全查核之執行，國防部得委由國防部政治作戰局（以下簡稱政戰局）辦理，並得就安全查核項目委任所屬相關機關（構）或委託其他機關（構）辦理。<br>前項受委任或委託之機關（構）對於辦理受任或受託事務所獲悉特定非公務機關之秘密，不得洩漏。 | |
| 第四條　安全查核之內容及基準如下：<br>一、人員查核：執行國防事務人員特定之身分背景（如附表一）。<br>二、設施（備）查核：執行國防事務主營業所或其分支、廠房、辦公室等處所設施（備）之安全管制措施（如附表二）。<br>三、資訊系統查核：執行國防事務資訊網路、個人作業系統與周邊連線設備軟體及硬體之安全維護措施（如附表三）。<br>四、其他有關安全事務。 | 為詳實辦理安全查核，以落實國防安全管控，爰明定人員、設施(備)、資訊系統及其他安全有關事務之安全查核項目、內容。 |
| 第五條　安全查核方式如下：<br>一、申請認證查核：依附表一至附表三申請認證查核細項，辦理安全查核。<br>二、定期查核：<br>(一)未得標列管軍品之合格廠商及列管軍品未涉機密工項之得標合格廠商，依附表一至附表三擇有關項目，辦理安全查核。<br>(二)列管軍品涉機密工項之得標合格廠商及其下游供應廠商，依附表一至附表三擇有關項目與契約特別保密條款之項目及要求，辦理安全查核。<br>三、不定期查核：依契約特別保密條款之項目及要求，辦理安全查核。 | 一、申請列管軍品廠商資格級別認證之廠商，其安全查核須符合所有安全查核項目之基準，爰於第一款明定申請認證之查核細項。<br>二、定期查核區分為二類，未得標列管軍品之合格廠商及列管軍品非涉機密工項之得標合格廠商，係依安全查核基準表內之項目，擇有關項目查核。至列管軍品涉機密工項之得標合格廠商及其下游供應廠商，除依安全查核基準表內之項目擇有關項目查核外，應依人員查核基準表及國防部特別保密條款(範本)辦理安全查核，爰於第二款明定定期查核之方式。<br>三、合格廠商及列管軍品得標廠商下游供應廠商，如發生影響國防安全情事，為求即時因應，以確保國防技術不外洩，爰於第三款明定國防部得對其實施不定期安全查核。 |

| | |
|---|---|
| 第六條　安全查核程序如下：<br>一、完成列管軍品廠商資格級別評鑑之廠商，應於接獲國防部通知之日起十日內，填具列管軍品廠商執行國防事務人員查核名冊（如附表四），並檢附廠商人員之國民身分證影本與警察刑事紀錄證明書、非陸資及安全查核切結書（如附表五），送交政戰局實施書面審查。檢附文件、資料未備齊者，應於接獲通知後七日內補正；屆期未補正，視同未符合安全查核基準。<br>二、政戰局完成書面審查後，必要時得至廠商執行國防事務相關主要或其分支營業所、廠房、辦公室或軟硬體設備（施）之所在地，實施現地訪查或其他必要查察；廠商拒絕者，視同未符合安全查核基準。<br>三、受委任或委託機關（構）完成委任及委託查核事項後，應將查核情形（如附表六）送交政戰局彙整查核結果。<br>政戰局依前項所定程序完成查核後，應填載安全查核結果通知書（如附表七），陳報國防部續辦核發合格證明之審查，並建立檔案列管。 | 一、申請合格證明廠商，於完成本條例第四條第二項列管軍品資格級別評鑑後，依該條第四項實施安全查核之程序及結果處理。<br>二、完成列管軍品廠商資格級別評鑑之廠商，應檢附相關資料送查核，爰於第一項第一款明定廠商應於通知後填具及檢附之資料，由政戰局實施書面審查，該審查階段廠商文件、資料未齊備之補正通知及屆期未補正之效果。<br>三、完成書面審查之列管軍品廠商資格級別評鑑之廠商，政戰局得採現地訪查，爰於第一項第二款明定政戰局必要時並得實施現地訪查或其他必要查察，以及廠商拒絕現地查訪之效果。<br>四、為彙整查核資料，於第一項第三款明定受委任或委託機關(構)完成查核，應送交政戰局彙整查核結果。<br>五、政戰局完成第一項查核資料彙整，應報國防部審查，爰於第二項明定查核結果之處理流程。 |
| 第七條　政戰局辦理定期查核，應於六十日前通知合格廠商及其下游供應廠商查核之時間、事項、地點、設施（備）及相關文件、資料，必要時得以隨機抽檢方式辦理。<br>定期查核未符合安全查核基準者，政戰局應以書面通知限期改正；屆期未改正者，依下列方式處理：<br>一、安全疑慮仍未改善之合格廠商，視同未符合安全查核基準。<br>二、安全疑慮仍未改善之下游供應廠商，合格廠商應輔導其改正；其未改正者，應終止與下游供應廠商之該得標項目列管軍品物料供應、製造或分包、協力契約；未終止契約者，視同合格廠商未符合安全查核基準。 | 一、為利廠商預先準備受查事宜，第一項明定政戰局辦理定期查核應事先通知合格廠商及下游供應廠商之日數及定期查核之時間、事項、地點及廠商應備資料及設施（備）及相關文件、資料。<br>三、政戰局應通知未符合安全查核基準之合格廠商及其下游供應廠商應於期限內改正，爰於第二項明定政戰局應以書面通知定期查核未符合安全查核基準之合格廠商及下游供應廠商，及屆期未改正之處理方式。 |
| 第八條　政戰局得以隨機抽檢方式實施不 | 一、為能確實明瞭廠商執行國防事務安全 |

| | |
|---|---|
| 定期查核；必要時得至廠商執行國防事務相關主要或其分支營業所、廠房、辦公室或軟硬體設備（施）之所在地，實施現地訪查及其他必要查察。<br>廠商拒絕前項查核、現地訪查或必要查察者，視同未符合安全查核基準。<br>不定期查核未符合安全查核基準者，政戰局應以書面通知限期改正；屆期未改正者，依前條第二項規定處理。 | 管控之情形，爰於第一項明定政戰局得採隨機抽檢方式實施不定期查核：必要時得實施現地訪查地點或其他必要查察。<br>二、為使廠商瞭解政戰局實施不定期查核時之配合義務，於第二項明定廠商拒絕第一項不定期查核、現地訪查或其他必要查察之處理。<br>三、為使廠商瞭解未符合安全基準之處理方式，於第三項明定不定期查核未符合安全查核基準之處理方式。 |
| 第九條　不服安全查核結果者，除有不可抗力之事由外，得於查核結果書面通知送達之日起十日內，以書面向政戰局申請複查。但以一次為限。<br>政戰局應自收受申請複查書面通知之次日起二個月內完成複查，必要時得予延長，並通知申請人。延長以一次為限，最長不得逾二個月。 | 一、為使廠商明瞭不服安全查核結果救濟方式，爰於第一項明定不服安全查核結果者，得申請複查之時間、方式及次數。<br>二、為期複審能及時完成，以維護當事人權益，爰於第二項明定政戰局受理申請複查之處理時間、得延長處理時間之通知、次數及期限。 |
| 第十條　合格廠商應落實自主安全管理事項，並指派所屬人員及要求其下游供應廠商參與政戰局及其委任、委託機關（構）辦理之安全查核教育訓練。<br>合格廠商於合格證明有效期內，變更安全查核書面資料，應主動檢附變更資料通知國防部。<br>合格廠商得標列管軍品購案時，應向政戰局通報下游供應廠商涉機密工項人員之安全調查表，與非陸資及安全查核切結書供查核；列管軍品購案履約期間，合格廠商每年應定期彙整下游供應廠商營運異動資訊、安全查核及履約督導結果送交國防部。 | 一、為落實安全查核、合格廠商自主管理、促進查核程序效率，於第一項明定合格廠商應派所屬人員及要求其下游供應廠商參與配合政戰局及其委任、委託機關辦理相關安全查核之教育訓練。<br>二、為掌握安全查核事項資料變動，作為定期或不定期安全查核事項之重點，爰於第二項明定廠商於合格證明之有效期限內，發生安全查核時所提資料有變更者，應檢附變更資料主動通知國防部。<br>三、為落實國防安全管控、合格廠商自主管理，爰於第三項明定合格廠商得標列管軍品購案時，應向政戰局通報涉機密工項之下游供應商人員之資料，以利國防部對其實施安全查核，且於列管軍品購案履約期間，應每年定期掌握及管制下游供應商之營運異動，如屬涉機密工項之下游供應商，亦應依契約之特別保密條款，彙整下游供應商營運異動資訊或安全查核及履約督導結果，並將結果陳報國防部查核權責機關，以利定期安全查核。 |
| 第十一條　列管軍品屬機密級以上之案件 | 一、為有效管控合格廠商及下游供應廠商 |

| | |
|---|---|
| ，建案單位應於採購作業階段，將國防部特別保密條款納入招標文件及契約書，以為定期及不定期安全查核範圍。<br>前項案件之合格廠商及下游供應廠商涉密人員，應依國家機密保護法、臺灣地區與大陸地區人民關係條例規定，納入出境及進入大陸地區之管制對象，並依契約書保密約定辦理管制作業。 | 未來承攬國防部機敏專案，履行國家機密保護法要求，國防部國防採購室於一百零六年三月十六日訂定委製協議書特別保密條款範本，主要規範已包含廠商涉密人員安全查核、設施（備）管制、機敏辦公室管制、機敏資訊管制、檔案管理、通訊安全管制、會議保密要求、專案資訊公開管制及參訪管制等九類，爰於第一項明定建案單位應於採購作業階段將該條款納入採購契約，以為定期及不定期安全查核範圍，有效防杜國防科技研究成果、關鍵技術或機敏資訊等遭竊取或不當移轉，確保整體國防事務安全無虞。<br>二、依國家機密保護法第二十六條及臺灣地區與大陸地區人民關係條例第九條所定之人員，無論在職或離職，未經核准不得出境，未經許可不得進入大陸地區，爰於第二項明定列管軍品屬機密級以上案件合格廠商及下游供應廠商涉密人員，受出境及進入大陸地區相關管制規定，並依契約執行管制作業。 |
| 第十二條　本辦法自本條例第五條施行之日施行。 | 本辦法之施行日期。 |

附表一

| 列管軍品廠商人員安全查核基準表 | |
|---|---|
| 項次 | 調查項目 |
| 1 | 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 4 | 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。 |
| 5 | 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。 |
| 6 | 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。 |
| 7 | 執行國防事務人員未具有中華民國國籍，或為大陸地區、香港、澳門人士。 |
| 8 | 犯刑法內亂、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。 |
| 9 | 廠商資金背景查察符合陸資廠商條件。 |
| 備註： | |

附表二

| 列管軍品廠商設施（備）安全查核基準表 | | |
|---|---|---|
| 項次 | 檢查設施 | 查驗標準 |
| 1 | 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。 |
| 2 | 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。 |
| 3 | 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。 |
| 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 | 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。惟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。 |
| 6 | 進出設施 | 需設置門禁系統，相關人員欲於機敏品項儲放設施 |

| | | |
|---|---|---|
| | 之管制 | 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。 |
| 7 | 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。 |
| 8 | 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。 |
| 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，主管機關得隨時調閱、提供，廠商不得拒絕。 |
| 10 | 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。 |
| 備註：<br>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）」。<br>2. 「設施（備）安全查核基本要求」，查核內容屬原則性，如國防廠商設施(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，經設施(備)安全主管機關審視可行性及安全性後同意。 | | |

附表三

| 列管軍品廠商<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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：<br>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。<br>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。

附表四

| 「００公司」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 | 備考 |
| 1 | 王◯◯ | 81.◯.◯ | | ◯◯專案經理 | | | 108.◯.◯ | |
| | | | | | | | | |
| | | | | | | | | |
| 合計：◯員 | | | | | | | | |

**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」及「大陸地區之營利事業在臺設立分公司或辦事處許可辦法」之陸資企業，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：

附表六

| 人員安全查核結果表 | | |
|---|---|---|
| 一、廠商名稱： | | |
| 二、查核對象：○○○等○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<br>□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<br>□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<br>□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<br>□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<br>□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<br>□有 | |
| 執行國防事務人員為大陸地區、香港、澳門人士。 | □無<br>□有 | |
| 資金背景符合陸資廠商條件。 | □無<br>□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<br>□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<br>□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<br>□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<br>□未符合 | |
| 圍牆 | 圍牆須安裝入侵警監系統(intrusion detection system, IDS)。 | □符合<br>□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<br>□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<br>□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<br>□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<br>□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<br>□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<br>□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<br>□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<br>□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。<br>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。<br>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<br>□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。<br>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<br>□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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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<br>□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<br>□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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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<br>□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 | | |

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 | | |