列管軍品廠商安全查核辦法修正總說明

列管軍品廠商安全查核辦法（以下簡稱本辦法）自一百零九年九月二日訂定發布，一百十年六月十八日施行，迄今未修正。茲考量國防產業發展條例第五條規定之定期查核對象，為合格廠商及得標廠商之下游供應廠商，並未以涉及機密工項者為限，為使本辦法安全查核範圍與授權範圍一致，明確下游供應廠商之範圍，並依作業實需修正資訊系統安全查核基準，俾強化對國防產業廠商安全查核，爰修正本辦法，其修正要點如下：

一、刪除機密工項、建案單位及涉密人員之定義，並修正下游供應廠商之定義。(修正條文第二條)

二、配合下游供應廠商定義修正，修正定期查核、不定期查核之對象、查核方式及查核未符合安全基準之效果。（修正條文第三條、第五條及第七條）

三、修正安全查核項目及基準。(修正條文第四條)

四、增列廠商應於查核前完成自我檢查程序。（修正條文第六條）

五、修正不定期查核之辦理時機。（修正條文第八條）

六、修正辦理安全查核教育訓練權責單位及合格廠商得標後應提供之資料。（修正條文第十條）

七、刪除涉密人員應依相關法令管制入出境及赴陸之規定。（修正條文第十一條）

八、修正本辦法自發布日施行。(修正條文第十二條)

列管軍品廠商安全查核辦法修正條文對照表

修正條文	現行條文	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。	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。	本條未修正。
第二條　本辦法用詞，定義如下： 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。 二、下游供應廠商：指為得標之列管軍品合格廠商，製造或供應該列管軍品主要次系統或關鍵模組之分包或協力之國內法人、機構或團體。 三、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。	第二條　本辦法用詞，定義如下： 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。 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。 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。 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。 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。 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、依國防產業發展條例（以下簡稱本條例）第五條第一項規定，主管機關應每年定期對合格廠商及列管軍品得標廠商之下游供應廠商辦理安全查核，並未以涉及機密工項者為限，配合修正條文第五條及第十條刪除「機密工項」相關規範，因已無定義機密工項之必要，爰刪除第二款機密工項之定義，其後款次配合變更。 二、依本條例第十四條至第十八條規定，列管軍品採購，其得標廠商不限本條例第四條第四項之合格廠商，惟如將本條例第五條第一項規定「列管軍品得標廠商之下游供應廠商」解釋為無論得標廠商是否為合格廠商，其下游供應廠商均應列入安全查核對象，將造成非屬合格廠商之得標廠商無須接受安全查核，其下游供應廠商卻須接受安全查核之現象，故本條例第五條第一項規定之「列管軍品得標廠商之下游供應廠商」，應予限縮解釋，以符立法意旨，爰將「列管軍品得標廠商」修正為「得標之列管軍品合

		格廠商」，及配合修正理由一刪除「涉機密工項」後，為免將無關國防安全之各種物料供應、製造廠商或協力廠商均納入安全查核，爰修正限縮為「製造或供應該列管軍品主要次系統或關鍵模組」之分包或協力廠商。又本款所稱「主要次系統或關鍵模組」，係指列管軍品範圍及認定辦法第二條第二款、第三款及第三條至第五條所定主要次系統及關鍵模組。 三、考量現行條文第五款定義之「建案單位」用語，僅於第十一條第一項使用，又依其條文內容，應係指「申購單位」，與國軍其他法令「建案單位」用語之內涵不符，爰刪除現行條文第五款。 四、配合修正條文第十一條刪除第二項規定，現行條文第六款之涉密人員已無定義之必要，爰予刪除。
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；其對象及時機如下： 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	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<u>項目、</u>對象及時機如下： 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	一、考量安全查核項目及基準為第四條規範內容，爰刪除第一項序文之「項目」；本條例第四條第四項已定有「合格證明」及「合格廠商」，爰刪除第一款及第二款有關合格證明及合格廠商定義文字；又依本條例第五條第一項所定對合格廠商及下游供應廠商辦理不定期辦理安全查核之

長領域項別之合格證明；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者，得以定期安全查核之查核結果審查。 二、定期查核：對合格廠商及下游供應廠商，每年辦理一次安全查核。 三、不定期查核：合格廠商及下游供應廠商，於新增、變更資料或有特殊情形時辦理之安全查核。 前項第三款所稱特殊情形，指具有下列情形之一者： 一、將機密資料隱匿、交付或洩漏予第三人之疑慮。 二、資金背景符合陸資廠商。 三、有資安疑慮。 四、違反契約保密條款、應報准而未報准進入大陸地區、香港、澳門，或與大陸地區人民技術交流，衍生國防技術外洩疑慮。 五、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、第六款之罪。 六、有其他足以影響國防安全之情事。 安全查核由國防部政治作戰局（以下簡稱政	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。 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。 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。 前項第三款所稱特殊情形，指具有下列情形之一者： 一、將機密資料隱匿、交付或洩漏予第三人之疑慮。 二、資金背景符合陸資廠商。 三、資訊系統遭病毒或駭客入侵存有資安疑慮。 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。 五、合格廠商負責人、代理人、受僱人或其他	時機，為「有特殊情形，必要時」，並未限縮合格廠商及下游供應廠商範圍，爰修正第三款不定期查核對象不限於「涉及機密列管軍品之得標」合格廠商及下游供應廠商，並酌作文字修正。 二、為簡潔條文，第二項第三款及第四款酌作文字修正；另下游供應廠商之負責人、代理人、受僱人或其他從業人員，如有犯本條例第六條第一項第一款、第二款、第五款、第六款之罪或有其他足以影響國防安全之情事時，亦有納入不定期查核之特殊情形之必要，爰刪除第五款「合格」文字，並將第五款後段之「有其他足以影響國防安全之情事」移列第六款規定，以符實需。 三、考量安全查核之執行係國防部內部事務之分配，本得交由國防部政治作戰局辦理，並由其他相關單位協助執行查核作業，無須再依行政程序法辦理權限委任或委託，爰修正第三項規定，定明安全查核由國防部政治作戰局辦理，增列協辦單位並刪除後段權限委任或委託之規定，以與實務作業相符。 四、配合第三項已刪除權限委任或委託之規定，且相關執行職務人員本應依法保守秘密，無特

戰局）辦理，國防部軍備局及國防部參謀本部通信電子資訊參謀次長室協辦。	從業人員犯本條例第六條第一項第一款、第二款、第五款、第六款之罪或有其他足以影響國防安全之情事。 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。 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。	別規定之必要，爰刪除現行條文第四項規定。
第四條　安全查核之項目及基準如下： 一、人員查核：執行國防事務人員，包含廠商負責人、代理人、受僱人或其他執行該列管軍品事務有關人員，其前科紀錄、國籍及廠商資金來源之身分背景，應符合附表一所列人員安全查核基準。 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，應符合附表二所列設施（備）安全查核基準。 三、資訊系統查核：執行國防事務所使用之資訊網路、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，應符合	第四條　安全查核之內容及基準如下： 一、人員查核：執行國防事務人員特定之身分背景（如附表一）。 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）。 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）。 四、其他有關安全事務。	為符合法律明確性要求，爰修正序文、於第一款增列查核人員範圍及刪除現行條文第四款概括條款，各款並酌作文字修正；另配合資訊安全要求及查核作業實需，修正附表一至附表三之查核項目及內容。

附表三所列資訊系統安全查核基準。		
第五條　安全查核方式如下： 一、申請認證查核：依附表一至附表三申請認證查核項目，辦理安全查核。 二、定期查核： (一)未得標之合格廠商，依附表一至附表三部分或全部項目，辦理安全查核。 (二)得標合格廠商及下游供應廠商，依附表一至附表三部分或全部項目及契約保密條款約定項目，辦理安全查核。 三、不定期查核：依附表一至附表三部分或全部項目及契約保密條款約定項目，辦理安全查核。	第五條　安全查核方式如下： 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。 二、定期查核： (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。 (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。 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、配合修正條文第四條序文用語，將第一款之「細項」修正為「項目」。 二、第二款第一目及第二目刪除涉機密工項相關文字，並酌作文字修正，理由同第二條說明一。 三、配合修正條文第三條第一項第三款不定期查核對象已刪除涉機密工項之限制，爰修正第三款不定期查核內容，以符查核作業實需。
第六條　申請認證查核程序如下： 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，填具執行國防事務人員查核名冊(如附表四)，並檢附列冊人員之國民身分證影本與警察刑事紀錄	第六條　安全查核程序如下： 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	一、安全查核區分為申請認證查核、定期查核及不定期查核程序，本條為申請認證查核程序規定，為與第七條及第八條之定期查核、不定期查核程序有所區別，爰修正第一項序文，增列「申請認證」四字，以資明確；另考量下游供應廠商亦須提供人員

證明書、非陸資廠商及安全查核切結書（如附表五）及依附表一至附表三完成自我檢視結果，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，視為未符合安全查核基準。 二、政戰局完成書面審查後，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）所在地，實施現地訪查或其他必要查察；廠商規避、妨礙或拒絕者，視為未符合安全查核基準。 政戰局依前項所定程序完成查核後，應依查核結果表（如附表六）彙整判定查核結果，填載安全查核結果通知書（如附表七），報國防部續辦核發合格證明之審查，並建立檔案列管。	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。 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。 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。 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。	名冊，及實務執行時，由廠商先行自我檢視以提高查核效率之作法，爰修正第一款查核名冊之名稱為「執行國防事務人員查核名冊」，並增列廠商應辦理自我檢視，及將檢視結果併同於十日內檢送政戰局。 二、為簡潔條文及因應實需，第一項第二款酌作文字修正。 三、配合修正條文第三條第三項已刪除權限委任或委託之規定，爰刪除現行條文第一項第三款規定，並將政戰局依查核結果表彙整判定查核結果之程序，移至第二項規定。
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。 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	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。 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	一、配合修正條文第二條第二款下游供應廠商定義，刪除第一項之「其」字。 二、為符法制體例，及配合修正條文第二條第二款下游供應廠商定義，第二項第一款及第二款酌作文字修正。

處理： 一、未改正之合格廠商，視為未符合安全查核基準。 二、未改正之下游供應廠商，合格廠商應輔導其改正；其未改正者，合格廠商應終止與該下游供應廠商有關該得標項目列管軍品主要次系統或關鍵模組之供應、製造或分包、協力契約；未終止契約者，視為合格廠商未符合安全查核基準。	處理： 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。 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。	
第八條　政戰局實施不定期查核，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。 廠商拒絕前項查核、現地訪查或其他必要查察者，視為未符合安全查核基準。 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，依前條第二項各款規定處理。	第八條　政戰局得以隨機抽檢方式實施不定期查核；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。 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。 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。	一、配合第三條第一項第三款辦理不定期查核之時機及本條例第五條第一項但書規定，為避免產生無特定事由仍得隨機為不定期查核之誤解，爰刪除第一項隨機抽檢之辦理方式。 二、為與第一項用語一致，爰於第二項增列「其他」二字，並酌作文字修正。 三、第三項增列「各款」二字。
第九條　不服安全查核結果者，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，並以一次為限。 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。	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。 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，	一、考量行政程序法第五十條第一項已有申請回復原狀規定，且較現行條文第一項除書規定，較有利於廠商，爰刪除第一項之除書，並酌作文字修正，以符法制體例。 二、第二項未修正。

	最長不得逾二個月。	
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下游供應廠商參與國防部辦理之安全查核教育訓練。 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。 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執行國防事務人員查核名冊、非陸資廠商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。	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。 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。 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、考量現行實務廠商安全查核教育訓練均由國防部統籌辦理，爰修正第一項合格廠商所屬人員及下游供應廠商參與教育訓練辦理機關為國防部。 二、第二項未修正。 三、配合修正條文第六條第一項第一款修正查核名冊名稱，修正第三項合格廠商得標時應提供之資料，並酌作文字修正。
第十一條　列管軍品涉密級以上資訊之案件，申購單位應於採購作業階段，將國防部保密條款納入招標文件及契約書。	第十一條　列管軍品屬機密級以上之案件，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。 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。	一、為強化保密安全要求，將現行條文第一項「機密級」修正為「密級以上」採購案件，即應將國防部相關保密條款納入招標文件及契約書，並將「建案單位」修正為「申購單位」，以臻明確；另定期及不定期安全查核時機及查核方式，已明確規範於第三條及第五條，爰刪除查核範圍規定。 二、考量涉及機密級以上採購案之相關涉密人員，其入出境管制仍應依國家機密保護法、臺灣地區與大陸地區人民關係條例相關規定辦理，本辦法無重複訂定之必要，爰刪除現行條

		文第二項規定。
第十二條　本辦法自發布日施行。	第十二條　本辦法自本條例第五條施行之日施行。	修正本辦法施行日期。

第四條 附表一(修正後)

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：		

修正說明：為明確查核項目及基準，增訂查核項目欄位，並配合國家機密保護法及國家安全法條次變更，及酌作文字修正。

第四條 附表一(修正前)

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：	

第四條 附表二（修正後）

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。		

修正說明：為明確查核項目及基準，修正欄位名稱，並將查核基準分點敘述及修正備註2文字，以臻明確。

第四條 附表二（修正前）

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。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。
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執

	之管制	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： 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. 「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。		

第四條 附表三(修正後)

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。	

修正說明：

一、為明確查核項目及基準，修正欄位名稱。

二、為符合列管軍品廠商資訊系統安全查核作業實需，修正資訊系統安全查核項目及內容，並增列資通系統開發及維護項目。

第四條 附表三(修正前)

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辨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。	

第六條 附表四(修正後)

「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。								

修正說明：

一、修正表格名稱。

二、為利識別查核對象類別，爰增訂備註欄，定明申請認證查核、定期安全查核對象，須依格式區分完成列管軍品資格級別評鑑之廠商、合格廠商及下游供應廠商之類別完成註記。

三、為明確律定執行人員異動時之處理，爰增加類別欄位，定明廠商、合格廠商（含得標合格廠商）、下游供應廠商執行人員如有異動時之辦理事項。

第六條 附表四(修正前)

「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								

第六條 附表五（修正後）

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：

修正說明：修正陸資廠商之定義與第二條第三款定義一致。

第六條 附表五（修正前）

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：

第六條 附表六（修正後）

<table>
<tr><td colspan="4">人員安全查核結果表</td></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>
<tr><td>查核人員簽證</td><td></td><td>受查廠商
代表簽證</td><td></td></tr>
</table>

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用相關資安防護設定及措施，單機	□符合 □未符合	

	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	□符合 □未符合	

	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		

修正說明：

一、配合所引國家機密保護法及國家安全法條項次修正，並酌作文字修正。

二、為符合列管軍品廠商資訊系統安全查核作業實需，爰修正資訊系統安全查核結果表之查核項目及基準，並增列資通系統開發及維護項目。

三、配合現行條文第四條第四款刪除，爰刪除其他有關安全事務，經研判足以影響國防安全或有危安疑慮，為人員、設施（備）及資訊系統安全查核內容。

第六條 附表六(修正前)

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 □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

第六條 附表七（修正後）

安全查核結果通知書

受理日期：

<table>
<tr><td>廠商名稱</td><td></td><td>負　責　人</td><td></td></tr>
<tr><td>受理案號</td><td></td><td>聯絡人電話</td><td></td></tr>
<tr><td>查核種類</td><td colspan="3">□初查□複查□定期查核□不定期查核</td></tr>
<tr><td rowspan="2">查核結果</td><td colspan="3">□ 符合</td></tr>
<tr><td>□ 未符合</td><td>原由</td><td></td></tr>
<tr><td>查核效期</td><td colspan="3">至　　年　　月　　日　有效</td></tr>
</table>

修正說明：本附表未修正。

第六條 附表七（修正前）

安全查核結果通知書

受理日期：

<table>
<tr><td>廠 商 名 稱</td><td colspan="2"></td><td>負　責　人</td><td></td></tr>
<tr><td>受 理 案 號</td><td colspan="2"></td><td>聯絡人電話</td><td></td></tr>
<tr><td>查 核 種 類</td><td colspan="4">□初查□複查□定期查核□不定期查核</td></tr>
<tr><td rowspan="2">查 核 結 果</td><td colspan="4">□ 符合</td></tr>
<tr><td colspan="2">□ 未符合</td><td>原由</td><td></td></tr>
<tr><td>查 核 效 期</td><td colspan="4">至　　年　　月　　日　有效</td></tr>
</table>