國防部
Ministry of National Defense , R.O.C

列管軍品廠商資通安全維護稽核作業要點

提報單位：國防部通次室
報告人：林久傑中校
使用時間：10分鐘

綱目

- 依據
- 目的
- 執行單位
- 要點說明
- 廠商安全管控注意事項
- 現地查核提醒事項與所見情形

依據

國防產業發展條例
第五條第二項

授權

主管機關安全
查核辦法

訂定

列管軍品廠商安全
查核辦法

完成

列管廠商資通安全維護
稽核作業要點

目的

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，確保資訊系統（設施）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，爰依國防產業發展條例授權訂定列管軍品廠商安全查核辦法—資通安全維護稽核作業要點。

執行單位

- 國防部通信電子資訊參謀次長室，爰明定本要點之業務執行單位。
- 為使稽核作業及自評項目符合資通安全實況，並參酌資通安全責任等級分級辦法分級責任規範，於114年2月4日修正本要點。

要點說明（九大要項計57條，公布於國防法規資料庫網站）

資訊系統查核

執行國防事務軟、硬體安全維護措施

- 資訊網路
- 個人作業系統
- 周邊連線設備

項次	辦理項目
1	資訊安全管理系統之導入及通過已簽署國際認證論壇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。
2	資通安全專業證照
3	限制使用危害國家資通安全產品
4	資訊作業管理
5	實體與環境安全
6	資訊作業安全管理
7	存取控制
8	危機處理
9	其他（資通系統開發及維護安全類適用）

要點說明（續）

- 申請級別認證廠商及下游供應廠商（涉機密工項）須通過資通安全稽核檢核項目，始為符合資訊系統查核。
- 考量部分廠商屬傳統產業廠商，並未建置資訊系統，爰將查核結果分類為「符合」、「未符合」及「不適用」三類，如稽核項目列為「符合」或「不適用」時，依規定評為「符合」。

要點說明（續）

- 廠商應由所屬具備ISO27001主導稽核員之資安專職人員，依申請之列管軍品等級填具資通安全維護稽核自評表送交執行單位，計有9項57條。
- 執行單位依廠商提供之資通安全維護稽核自評表及佐證文件，先行實施書面審查，發現資料未備齊者，應通知廠商於七日內補正，屆期未補正者，視同未符合資訊系統安全查核基準。

要點說明（續）

- 書面審查後，檢視其真實性，至其相關服務之主營業所或分支、廠房及軟硬體設備(施)所在地進行實地稽核。
- 進行實地稽核僅針對軟硬體設備與資訊資產進行核對，並不會對系統資料進行檢查或安裝檢測軟體，亦不會探知公司營業秘密等情。

要點說明（續）

- 自評表需填註「列管軍品級別」（參照軍備局「國防產業發展條例列管軍品清單索引」），於下列各項目依不同等級，採用不同要求規範，以達其分級效益。

公司名稱	列管軍品項目	列管軍品級別
000	1. 000	一等
	2. XXX	二等
	3. @@@	三等
	（請自行填入並延伸）	
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。	

要點說明（續）

- 項目1.資訊安全管理系統（ISMS）之導入及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。

要點說明（續）

1.1	是否界定公司/專長領域之核心業務，完成資通系統之盤點及分級，且每年至少檢視1次分級之妥適性？	□符合 □未符合
1.2	是否將全部核心資通系統納入資訊安全管理系統（ISMS）適用範圍？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？（證書需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 □不適用
1.3	是否訂定資通安全政策，由管理階層核定，並定期檢視其重要性？	□符合 □未符合
1.4	是否指派副首長或適當人員兼任資通安全長，負責推動及督導機關內資通安全相關事務？	□符合 □未符合
1.5	是否訂定機關人員辦理業務涉及資通安全事項之考核機制及獎懲基準？	□符合 □未符合

要點說明（續）

●項目2. 資通安全專業課程訓練時數取得問題，可以參考行政院資通安全管理法FAQ 3.15項目。

2.1	資通安全專職人員是否每年接受12小時以上之資通安全專業課程訓練或資通安全職能訓練？	□符合 □未符合
2.2	一般使用者及主管是否每年接受3小時以上之資通安全通識教育訓練？	□符合 □未符合
2.3	資安專職人員是否符合資通安全專業證照要求，且分別各自持有證照1張以上，並維持其證照之有效性？	□符合 □未符合

要點說明（續）

●項目3. 需完整提供公司機房及與認證列管軍品相關之資訊軟、硬體設備（含伺服器、電腦及網路設備等），確認產品公司註冊國家為非大陸地區、香港、澳門，以符合其規範。

例：華碩→臺灣、戴爾（DELL）→美國

3.1	是否限制使用中國大陸品牌之軟、硬體服務？	□符合 □未符合

要點說明（續）

●項目4.項次簡併，內容無調整。

4.1	機敏辦公室內電腦應運用軟體是否管制可移除式媒體存取作業？	□符合 □未符合 □不適用
4.2	是否訂定資產異動管理程序，並建立清冊（如識別擁有者及使用者等），且確實盤點及更新？	□符合 □未符合 □不適用
4.3	是否建立資通安全風險管理計畫（包含風險評估作業、處理程序）並針對重要資訊資產鑑別其可能遭遇之風險，並適時調整？	□符合 □未符合 □不適用
4.4	是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？	□符合 □未符合 □不適用

要點說明（續）

4.5	是否訂定委外廠商對於機關委外業務之資安事件通報及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，是否立即通知機關並採行補救措施？	□符合 □未符合 □不適用
4.6	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？且落實執行資通安全責任及保密規定。	□符合 □未符合 □不適用
4.7	是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務報告及紀錄等進行管理及安全檢視（如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等），以利後續追蹤及管理？	□符合 □未符合 □不適用

要點說明（續）

●項目5.參考「資通安全責任等級分級辦法」，依申請不同等級之列管軍品，任命不同人數之資安專職人員，以符合實況。

5.1	配置適當人員經單位資安長核定任命之資安專職人員？且明定其業務職掌，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. 申請一等列管軍品：4人。 2. 申請二等列管軍品：2人。 3. 申請三等列管軍品：1人。	□符合 □未符合 □不適用
5.2	是否設置資通系統之備援設備，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？	□符合 □未符合 □不適用

要點說明（續）

5.3	是否定期執行重要資料之備份及復原作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？	□符合 □未符合 □不適用
5.4	是否訂定資訊及儲存媒體設備回收及汰除之安全控制作業程序？含有儲存媒體的設備項目（如：硬碟、磁帶），是否在報廢、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。	□符合 □未符合 □不適用

要點說明（續）

- 項目6.依申請不同等級之列管軍品，辦理不同程度之資安防護措施，以符合實況。
- 有關每年或每2年辦理1次之查核項目，以安全查核送件日期為節點，往前推算1年或2年期間為查核標準，需於期間內有完整執行查核項目，始符合規範。

要點說明（續）

6.1	是否完成下列資通安全防護措施？並維持其有效性及更新？ 1. 防毒軟體 2. 網路防火牆 3. 電子郵件過濾機制 4. 內部（區域）網路管理系統（防止未授權設備連接公司網路） 5. 入侵偵測及防禦機制 6. 應用程式防火牆（具有對外服務之核心資通系統者） 7. 進階持續性威脅攻擊防禦 分級項目： 1. 申請一等列管軍品：符合1-7項。 2. 申請二等列管軍品：符合1-7項。 3. 申請三等列管軍品：符合1-4項。	□符合 □未符合 □不適用

要點說明（續）

6.2	是否建置資通安全威脅偵測管理（SOC）機制？ 分級項目： 1. 申請一等列管軍品：本項需符合。 2. 申請二等列管軍品：本項需符合。 3. 申請三等列管軍品：本項不適用。	□符合 □未符合 □不適用
6.3	是否針對全部核心資通系統辦理網站安全弱點檢測？（初次辦理安全查核需檢附辦理1次佐證） 分級項目： 1. 申請一等列管軍品：每年辦理2次（上、下半年各一次）。 2. 申請二等列管軍品：每年辦理1次。 3. 申請三等列管軍品：每2年辦理1次。	□符合 □未符合 □不適用
6.4	是否針對全部核心資通系統辦理系統滲透測試？（初次辦理安全查核需檢附辦理1次佐證） 1. 申請一等列管軍品：每年辦理1次。 2. 申請二等列管軍品：每2年辦理1次。 3. 申請三等列管軍品：每2年辦理1次。	□符合 □未符合 □不適用

要點說明（續）

6.5	是否辦理資通安全健診，包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆設定檢視等？並執行修補或改善作業？（初次辦理安全查核需檢附辦理1次佐證） 1. 申請一等列管軍品：每年辦理1次。 2. 申請二等列管軍品：每2年辦理1次。 3. 申請三等列管軍品：每2年辦理1次。	□符合 □未符合 □不適用
6.6	是否針對資通系統及相關設備，建立適當之監控措施（如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等）是否針對日誌、紀錄、軌跡資料或證據建立適當之保護機制，以避免遭到竄改，且落實執行並定期稽核？	□符合 □未符合 □不適用

要點說明（續）

6.7	是否訂定電子郵件之使用規則，並律定機密性、敏感性規範傳送限制？是否針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則？是否針對電子郵件進行分析，主動發現異常行為且進行改善（如針對大量異常電子郵件來源之IP位址，於防火牆進行阻擋等）？	□符合 □未符合 □不適用
6.8	是否建立電子資料安全管理機制，包含分級規則（如機密性、敏感性及一般性等）、存取權限、資料安全、人員管理及處理規範等，且落實執行	□符合 □未符合 □不適用
6.9	是否建立網路服務安全控制措施，符合業務需要及資安要求？且定期檢測網路運作環境之防護措施與安全？	□符合 □未符合 □不適用

要點說明（續）

6.10	網路架構設計是否符合業務需要及資安要求？是否依網路服務需要區隔獨立的邏輯網域（如DMZ、內部或外部網路等），且建立適當之防護措施，以管制過濾網域間之資料存取？	□符合 □未符合 □不適用
6.11	是否針對機關內無線網路服務之存取及應用訂定安全管控程序，且落實執行？	□符合 □未符合 □不適用
6.12	是否每年進行1次社交工程演練？是否針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？	□符合 □未符合 □不適用
6.13	是否針對電腦機房及重要區域之安全控制、人員進出管控、環境維護（如溫溼度控制）等項目建立適當之管理措施，且落實執行？	□符合 □未符合 □不適用

要點說明（續）

6.14	是否針對資訊之交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性（如採行識別碼通行碼管制、電子資料加密或電子簽章認證等）？是否針對重要資料的交換過程，保存適當之監控紀錄	□符合 □未符合 □不適用
6.15	是否訂定資訊設備作業程序（含變更管理程序及管理責任），且落實執行？	□符合 □未符合 □不適用
6.16	是否針對電子資料相關設備進行安全管理（如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等）？	□符合 □未符合 □不適用
6.17	是否針對使用者電腦訂定軟體安裝管控規則？是否確認授權軟體及免費軟體之使用情形，且定期檢查？	□符合 □未符合 □不適用
6.18	是否針對個人行動裝置及可攜式媒體訂定管理程序，且落實執行，並定期審查、監控及稽核？	□符合 □未符合 □不適用

要點說明（續）

●項目7.項次簡併，內容無調整。

7.1	是否訂定人員之資通安全作業程序、權責及應負之資安責任？是否明確告知保密事項，且簽署保密協議？	□符合 □未符合
7.2	機敏辦公室規範是否律定資訊帳號密碼須符合複雜度要求並不得少於15碼以上。	□符合 □未符合 □不適用
7.3	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。	□符合 □未符合 □不適用
7.4	是否訂定外部遠端連線至內部存取資料之規範？如允許，應由權責主管逐筆辨證同意後，始得辦理存取。	□符合 □未符合 □不適用

要點說明（續）

●項目8.項次文字修訂，內容無調整。

8.1	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。	□符合 □未符合 □不適用
8.2	是否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？	□符合 □未符合 □不適用
8.3	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，俾利辦理事件查處作業？	□符合 □未符合
8.4	是否加入TWCERT/CC會員，以完備通報機制？	□符合 □未符合

要點說明（續）

●項目9.如無資通系統開發業務，本項均勾選不適用，並請提供現用軟體清單，以佐證非自行開發。

9.1	針對自行或委外開發之資通系統是否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 □不適用
9.2	資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？	□符合 □未符合 □不適用

要點說明（續）

9.3	資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？	□符合 □未符合 □不適用
9.4	資通系統開發階段，是否避免常見漏洞（如OWASP Top 10等）？且針對防護需求等級高者，執行源碼掃描安全檢測？	□符合 □未符合 □不適用
9.5	資通系統測試階段，是否執行弱點掃描安全檢測且針對防護需求等級高者，執行滲透測試安全檢測？	□符合 □未符合 □不適用
9.6	資通系統上線前，是否執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試等，且檢討執行情形？	□符合 □未符合 □不適用
9.7	資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約？	□符合 □未符合 □不適用

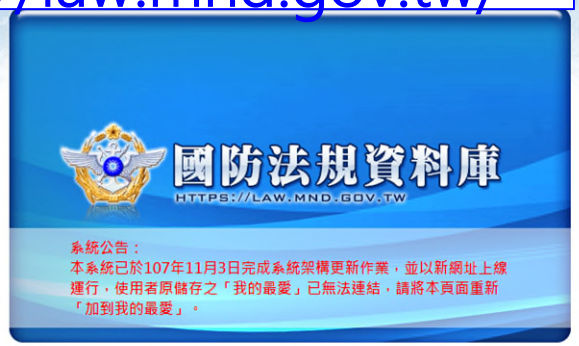
要點說明（續）

9.8	是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？	□符合 □未符合 □不適用
9.9	是否儲存及管理資通系統發展相關文件？儲存方式及管理方式為何？	□符合 □未符合 □不適用
9.10	資通系統測試如使用正式作業環境之測試資料，是否針對測試資料建立保護措施，且留存相關作業紀錄？	□符合 □未符合 □不適用
9.11	是否針對資通系統所使用之外部元件或軟體，注意其安全漏洞通告，且定期評估更新？	□符合 □未符合 □不適用

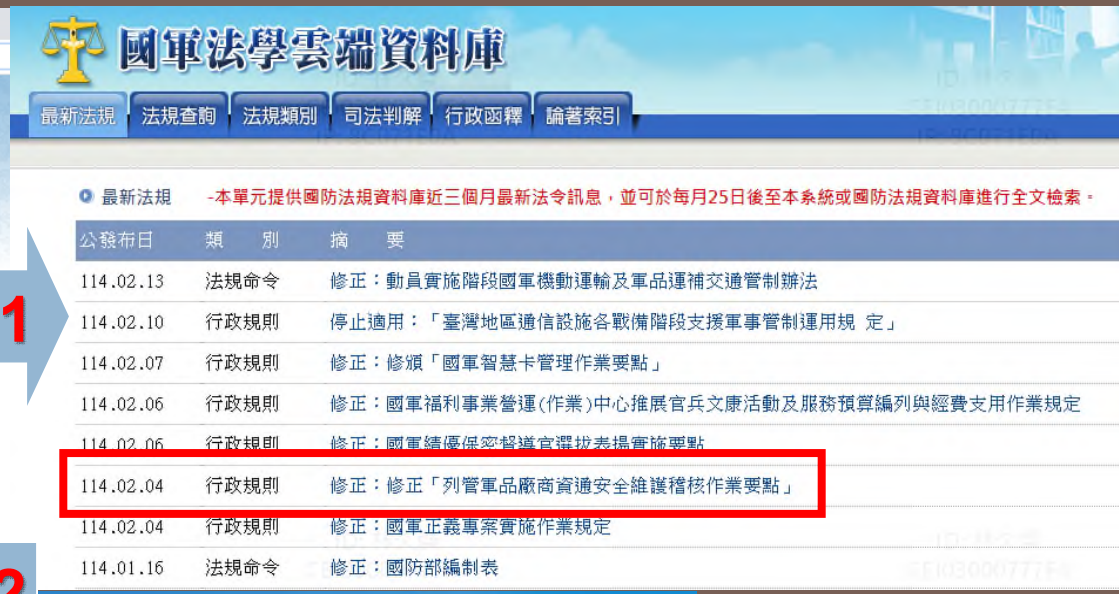
廠商安全管控注意事項

- 有關列管軍品廠商資通安全維護稽核作業要點與查核項目表公布於國防法規資料庫網站，歡迎查詢。

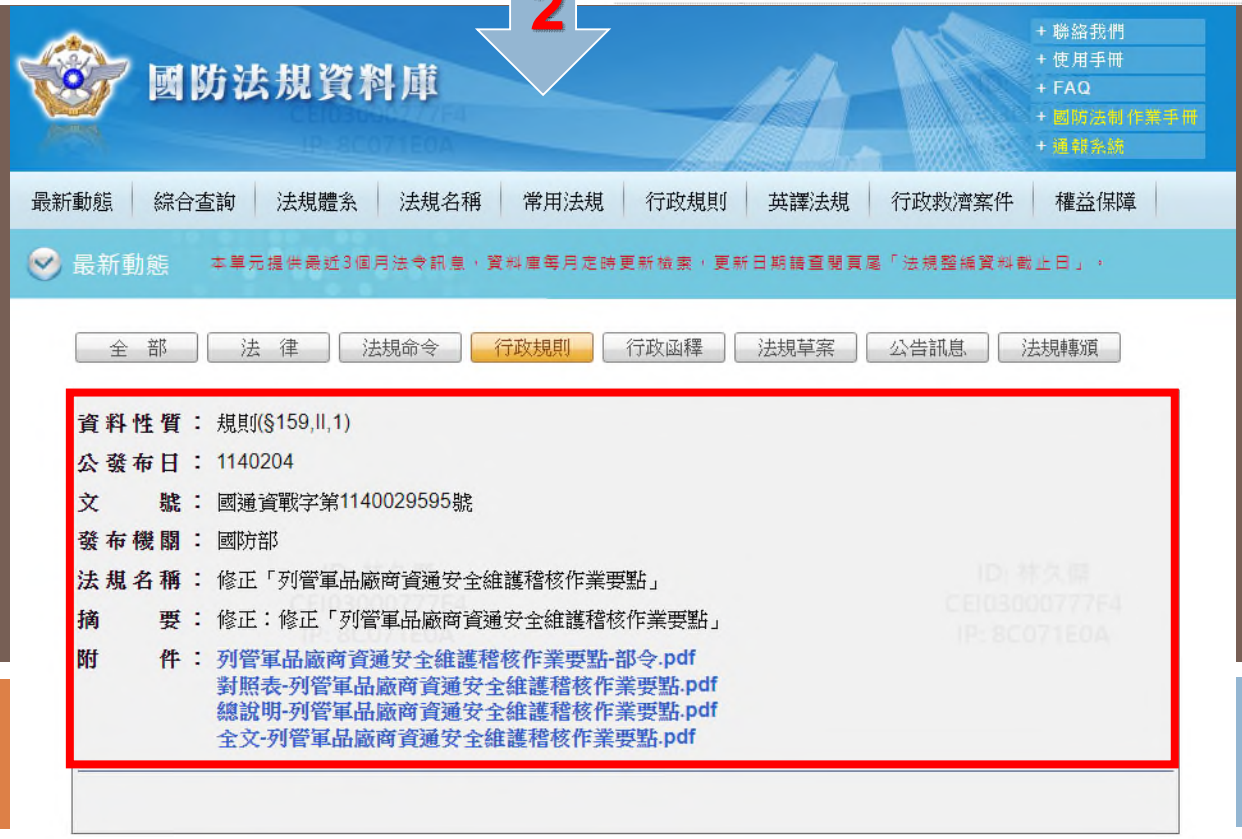
https://law.mnd.gov.tw/



1



2



現地查核提醒事項與所見情形

- 現地訪查前應完成事項如下：
  - 導入及通過資訊安全管理系統驗證並取得資通安全專業證照。
  - 依「資通安全維護稽核自評表」逐項提供符合自評表描述之佐證資料（電子檔），如有不適用項目仍須有相關證明。
  - 各項資通安全管控措施，應持續更新及維持有效性。

現地查核提醒事項與所見情形（續）

項次	所見情形	項次	所見情形
1	未取得(通過)資訊安全管理系統驗證	10	儲存媒體使用與管理未完善
2	驗證機構非我國標準法行政院委託機構認證之驗證機構	11	危機處理機制未完善如：未加入TWCERT/CC通報機制
3	須管理階層核定(簽署)資料未核定	12	資通安全軟硬體防護措施未完善
4	人員業務涉及資通安全事項無考核機制	13	核心資通系統網站安全弱點檢測次數不足
5	專業證照及資安專職人員數量不足	14	資通安全健診未實施
6	資訊安全教育訓練時數不足	15	社交工程演練次數不足
7	未提供(標明)資訊資產清冊及是否為陸製廠牌	16	核心資通系統滲透測試未執行
8	委外廠商管理機制未完善	17	存取遠端資料機制未完善
9	資通系統之備援、復原機制未完善	18	機敏處所資訊帳號密碼少於十五碼

國防部

Ministry of National Defense , R.O.C

簡報完畢