國防部採購案廠商資安管控作業指導

國防部115年10月20日國通資戰字第1153611882號令頒

一、 為有效管控國防部及所屬機關（構）、部隊、學校（以下簡稱機關）辦理採購案件之資通安全管理，落實資通安全防護措施及查核要求，以降低資安風險，特訂定本指導。

二、 本指導所稱非公開資訊，係指機關持有、管理或因業務產生，未對外公開或僅供特定人取得之資料（訊）、文件、圖資或成果，包括業務資料、技術資料、系統資訊、內部文件及其他經認定不宜公開之資訊。

三、 適用範圍：

各機關對於與其有採購、委外、合作、維護、駐點、系統介接、資料交換或其他業務往來，可能接觸機關非公開資訊、資訊系統、網路環境、資訊設備、實體設施或資料之廠商及其使用人員（以下簡稱廠商及廠商人員），應依本指導辦理資安管控。

四、 資安風險判斷原則：

(一)符合下列情形之一者，具人員風險：

1. 廠商人員須進入機關辦公區域。
2. 廠商人員須進入機關機房或管制區域。
3. 廠商人員須於機關場域執行作業。

(二)符合下列情形之一者，具資料風險：

1. 廠商須接觸、儲存、傳輸、處理及產出機關非公開資訊。
2. 廠商須接觸、儲存、傳輸、處理及產出機關資訊系統、軟體、應用程式之程式碼。
3. 廠商須接觸、儲存、傳輸、處理及產出個人資料或涉密資訊。

(三)符合下列情形之一者，具產品風險：

1. 採購標的具網路連線功能。
2. 採購標的具資料儲存功能。

3. 採購標的具資料處理功能。
4. 採購標的須介接機關資訊系統。
5. 採購標的部署於機關內部網路。
6. 採購標的屬雲端服務或遠端服務。

五、 資安管控要求事項：

依據風險判定結果，規劃「廠商人員安全管控」、「廠商作業環境」及「物品安全認證」等三個面向之資安管控要求事項（如附件一）作法如下：

（一）針對人員風險，考量廠商人員進入機關內部執行業務，可能衍生因通信資訊資器材造成資訊外洩、未經授權存取或其他資通安全風險，應實施下列管控措施：

1. 針對廠商人員攜帶或持有之通信資訊器材實施管制，依國軍營內民用通信資訊器材管理要點辦理（要求事項如附件二）。
2. 門禁管理及人員涉密查核，依國軍現行內部管理及人員涉密查核規定辦理；並依採購案涉密等級，依從事及參與國防安全事務人員安全調查辦法及國防科技工業合作對象安全調查執行作法辦理人員安全查核，且履約之廠商人員不得為大陸地區人士或香港、澳門居民。

（二）針對資料風險，依資料重要性區分為三級，並分別適用下列廠商資安管理要求：

1． 等級劃分：

（1）第一級：機密級以上之採購案件或廠商須接觸、處理或產出涉機密級以上之資料（訊）。

（2）第二級：採購案件涉及一般公務機密資訊或廠商須接觸、處理或產出涉一般公務機密之資料（訊）。

（3）第三級：無涉密採購案件，惟廠商須接觸、處理或產出國軍非公開資料（訊）。

2． 資安要求：

（1）資安基本要求：依前目等級劃分針對廠商資訊安全管理、資通安全專業證照、限制使用危害國家資通安全產品、資訊作業管理、實體與環境安全、存取控制及危機處理等項律定資安基本要求，並納入契約規範(要求事項如附件三)。

（2）作業環境資安認證：針對涉及個人資料、資訊系統開發或維運、涉密資訊處理之案件，廠商作業環境應具備完善資通安全管理措施並通過第三方驗證（要求事項如附件四）。

（3）涉及資通系統服務規劃、設計、開發、維護或代管之採購案件，應同時符合國軍委外辦理資通系統服務資安管控指導要點規範要求。

（三）針對產品風險，考量廠商提供之產品或服務可能影響國軍資通安全，為降低弱點及供應鏈風險，應要求廠商取得相關資安認證、安全檢測或合格證明，以確保產品及服務符合資安要求，說明如下：

1．驗收採購標的物為資訊（系統）硬體，須具備政府機關核發資安認證標章、第三方資安檢測報告或廠商自我安全評估報告（要求事項如附件五）。

2．驗收採購標的物為資訊 （系統）軟體，須完成原始碼檢測、第三方元件檢測及弱點掃描等安全檢測作業，且無中、高風險之項目，並提供軟體物料清單（SBOM）及檢測合規報告（要求事項如附件六）。

六、 各機關應於採購各階段落實下列管控作業程序：

(一)計畫申購階段：

1．申購部門：於提出採購需求時，應填列廠商資安風險判定表（如附件七)，將風險項目對應資安要求事項（同附件二至附件六）納入採購契約規範，並依個案實際需求

訂定相關罰則,提供機關通資部門審查(流程如附件八)；無法認定風險或有認定爭議時，由所屬司令部、國防部直屬機關（構)、軍事學校或參謀本部直屬機構、部隊通資部門判定，仍無法判定時則轉呈國防部，由國防部參謀本部通信電子資訊參謀次長室審認。

2．通資部門：審查採購案件風險及契約，確認採購文件已依風險判定結論納入資安要求事項。

(二)招標階段：

1．申購部門（採購部門協助)：

（1）將資安要求事項納入招標文件公告，俾供廠商自評估是否參標，並由採購部門協同申購部門於開標作業前審查廠商資格。

（2）針對涉及個人資料、資訊系統開發或維運、涉密資訊處理之採購案件，須將作業環境資安認證（作業區域須通過第三方驗證，如：CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準）納入廠商資格審查。

2．申購部門（保防部門協助)：落實廠商資金與背景查核，如投標廠商屬經濟部公告之陸資企業應判定為不合格標。

(三)訂（簽）約階段：

1．申購部門（保防部門協助)：決標後，由申購部門將得標廠商人員安全調查資料提供保防部門辦理安全調查，並依採購案件涉密等級，依從事及參與國防安全事務人員安全調查辦法及國防科技工業合作對象安全調查執行作法辦理人員安全查核，且履約人員不得為大陸地區人士或香港、澳門居民。

2．申購部門（通資部門協助)：具資料風險之採購案件，應

要求得標廠商依採購契約完成資通安全維護稽核自評表（如附件九）並檢附書面佐證資料，於簽約日之次日起七日內提供。

(四)履約階段：

1．申購部門（通資部門協助）：由申購部門偕同通資部門於履約期間針對具資料風險之採購案件得標廠商（含分包商，分包商之資安管理由主承包商負督導之責，並由機關依實際需求辦理書面或實地查核)進行資安查核作業，查核基準同附件九資通安全稽核檢核項目；履約期間逾一年者，每年至少辦理一次查核；履約期間未滿一年者，履約期間至少辦理一次查核；採購品項如屬列管軍品，廠商具同品項列管軍品廠商資格級別認證合格證明者，年度得合併列管軍品廠商安全查核時機辦理資安稽核作業。

2．申購部門（採購部門協助）：查核結果不合格時，依採購契約規範，要求廠商限期改善或罰款。

3．申購、保防及通資部門：於廠商人員進場維護時，落實營區及管制場域民用通訊器材管控及相關保密作為。

(五)驗收階段：

1．申購部門（通資部門協助）：

（1）驗收標的具產品風險之資訊軟、硬體，應依附件五、附件六基準辦理驗收。

（2）依國軍採購禁用大陸地區、香港、澳門產品認定及履約驗收作業指導及國軍資訊資產管理作業規定，實施陸製品（牌）查驗。

2．申購部門（通資部門協助）：結案需完成帳號回收、資料清除、憑證撤銷、關閉遠端連線通道等後續作業。

(六)為兼顧國防安全及採購效能，必要時得採行下列替代作

法：

1．採購案件作業範圍、標的僅限局部之小額採購案件，經申購部門評估，認定為非必要管控風險，申購部門得依採購案件性質、範圍等項提出需求，經通資部門審查後，可免除物品安全認證之第三方驗證，改由廠商自我評核（檢測）出具合格證明（項目如附件十）及簽署切結書（範本如附件十一）佐證，通資部門並得要求納入部分要求事項。

2．因其他特殊情形確無法依本指導規定辦理者，機關應敘明理由、完成風險評估並規劃補強措施（範本如附件十二），逐級呈報國防部各直屬一級單位資安長核准（如國防部陸軍司令部含所屬單位，即由該司令部資安長核准），並留存相關紀錄備查。

七、 各單位須於每年一月底前呈報前一年度資安管控案件統計表（如附件十三），提供國防部業管部門辦理稽核驗證。

附件一

各類風險資安管控要求事項

面向	風險類別 / 資安管控要求事項	人員風險	資料風險	產品風險
廠商人員安全管控	1.廠商人員攜帶通信資訊器材管制(如附件二)	◎		
廠商作業環境	2.資安基本要求(如附件三)		◎	
	3.作業環境資安認證(如附件四)		◎	
物品安全認證	4.硬體設備資安認證(如附件五)			◎
	5.軟體資安檢測(如附件六)			◎

■ 「人員安全查核」依採購案涉密等級，遵循「從事及參與國防安全事務人員安全調查辦法」及「國防科技工業合作對象安全調查執行作法」辦理人員安全調查作業。

■ 「陸製品（牌）查驗」依「國軍採購禁用大陸地區、香港、澳門產品認定及履約驗收作業指導」辦理。

附件二

資安管控要求事項-廠商人員安全管控	
項目	要求事項
廠商人員攜帶通信資訊器材管制	廠商人員如攜有、持有國軍營內民用通信資訊器材管理要點所列管制通信資訊器材，應依規定安裝管制軟體，無法配合者，機關應律定管制作法，並落實管控；契約並應納入廠商人員違反規定之違約效力規範。
備註：具人員風險購案均應將本表納入管制。	

附件三

資安管控要求事項-廠商資安基本要求					
項目	類別	要求事項	適用等級		
			一	二	三
資安基本要求	資訊安全管理	(1) 應界定公司/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。	●	●	●
		(2)應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) ➢ 未涉及個人資料、資訊系統開發或維運、涉密資訊處理之案件得不適用。	●	●	●
		(3)訂定資通安全政策，由管理階層核定，並定期檢視其重要性。(各級適用)	●	●	●
		(4)指派適當高層人員兼任資通安全長，負責推動及督導公司內部資通安全相關事務。	●	●	●
		(5)訂定公司人員辦理業務涉及資通安全事項之考核機制及獎懲基準。	●	●	●
	資通安全	(6)資通安全專職人員應每年接受 12 小時以上之資通安全專業	●	●	●

	專業證照	課程訓練或資通安全職能訓練。			
		(7)一般使用者及主管應每年接受3小時以上之資通安全通識教育訓練。	●	●	●
		(8)資安專職人員應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。	●	●	●
	限制使用危害國家資通安全產品	(9)購(專)案範圍須限制使用中國大陸品牌之軟、硬體服務。	●	●	●
	資訊作業管理	(10)辦公室內電腦應運用軟體管制可移動式儲存媒體存取作業。	●	●	
		(11)應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。	●	●	●
		(12)應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。	●	●	●
		(13)應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。			
		（14）應訂定委外廠商對於公司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，須立即通知公司並採行補救措施。	●	●	●
		（15）委外關係終止或解除時，應確認委外廠商返還、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。	●	●	●
		（16）應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（如對委外廠商端實地稽核、要求委外廠商提供異常報告、要求委外廠商提供相關安全檢測紀錄等），以利後續追蹤及管理。	●	●	●
	實體與環境安全	（17）應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） 第一級：4 人 第二級：2 人 第三級：1 人	●	●	●

		（18）應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。	●	●	●
		（19）應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，存放處所環境須符合實體安全防護。	●	●	●
		（20）應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。(各級適用)	●	●	●
	資訊作業安全管理	（21）須完成下列資通安全防護措施，並維持其有效性及更新。 A.防毒軟體 B.網路防火牆 C.電子郵件過濾機制 D.內部（區域）網路管理系統（防止未授權設備連接公司網路） E.入侵偵測及防禦機制 F.應用程式防火牆(具有對外服務之核心資通系統者） G.進階持續性威脅攻擊防禦 第一級：符合 A-G 項。 第二級：符合 A-G 項。 第三級：符合 A-D 項。	●	●	●

		(22) 應建置資通安全威脅偵測管理（SOC）機制。 第一級：本項需符合。 第二級：本項需符合。 第三級：本項不適用。	●	●	
		(23) 應針對全部核心資通系統辦理網站安全弱點檢測。 第一級：每年辦理2次(上、下半年各一次)。 第二級：每年辦理1次。 第三級：每2年辦理1次。	●	●	●
		(24) 應針對全部核心資通系統辦理系統滲透測試。 第一級：每年辦理1次。 第二級：每2年辦理1次。 第三級：每2年辦理1次。	●	●	●
		(25) 應辦理資通安全健診，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。 第一級：每年辦理1次。 第二級：每2年辦理1次。 第三級：每2年辦理1次。	●	●	●
		(26) 應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)，並針對日誌、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。(各級適用)			
		(27) 應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、針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則、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)。	●	●	●
		(28) 應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。	●	●	●
		(29) 應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。	●	●	●
		(30) 網路架構設計須符合業務需要及資安要求，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。	●	●	●
		(31) 針對公司內部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。			
		(32)每年進行1次社交工程演練，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。	●	●	●
		(33) 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。	●	●	●
		(34) 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)，針對重要資料的交換過程，保存適當之監控紀錄。	●	●	●
		(35) 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。	●	●	●
		(36) 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)。	●	●	●
		(37) 針對使用者電腦訂定軟體安裝管控規則，確認授權軟體及免費軟體之使用情形，且定期檢查。	●	●	●
		(38) 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。			
	存取控制	（39）訂定人員之資通安全作業程序、權責及應負之資安責任，明確告知保密事項，且簽署保密協議。	●	●	●
		（40）辦公室規範律定資訊帳號密碼須符合複雜度要求並不得少於： 第一級：15 碼以上 第二級：12 碼以上 第三級：8 碼以上	●	●	●
		（41）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。	●	●	●
		（42）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。	●	●	●
	危機處理	（43）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。	●	●	●
		（44）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。			
		（45）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。	●	●	●
	其他（資通系統開發及維護安全類適用）如無資通系統開發業務，本項均勾選不適用）	（46）自行或委外開發之資通系統應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。	●	●	●
		（47）資通系統開發前，應設計安全性要求，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。	●	●	●
		（48）資通系統設計階段，應依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估。	●	●	●
		（49）資通系統開發階段，須避免常見漏洞（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。(各級適用)	●	●	●
		（50）資通系統測試階段，須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。			
		（51）資通系統上線前，須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。	●	●	●
		（52）資通系統開發如委外辦理，應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。	●	●	●
		（53）應將開發、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。	●	●	●
		（54）儲存及管理資通系統發展相關文件，應有版本及權限控管。	●	●	●
		（55）資通系統測試如使用正式作業環境之測試資料，應針對測試資料建立保護措施，且留存相關作業紀錄。	●	●	●
		（56）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。	●	●	●
備註：具資料風險購案應依級別將本表要求事項納入管制。					

附件四

資安管控要求事項-廠商作業環境	
項目	要求事項
廠商作業環境資安認證	廠商辦理購案之相關程序及環境，應具備完善之資通安全管理措施及通過第三方驗證（如：CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準），且需提供證明文件供甲方審認。
備註：針對涉及個人資料、資訊系統開發或維運、涉密資訊處理之購案，應將本表納入管制，餘則不適用。	

附件五

<table>
<tr><th colspan="3">資安管控要求事項-物品安全認證</th></tr>
<tr><th>項目</th><th colspan="2">要求事項</th></tr>
<tr><td>硬體設備資安認證</td><td colspan="2">驗收採購標的物具資訊（數位）特徵之硬體，應提供下列認證：
（1） 商用無人機類應通過數位發展部遙控無人機資安檢測規範，並取得合格證明。
（2） 物聯網（IOT）設備如影像監控系統、網路攝影機須符合應符合經濟部資安環境標準 CNS16120 相關要求事項，並取得標章。
（3） 非上述採購標的物或無取得標章之設備，應交第三方檢測單位檢測，並提供資安檢測報告，檢測項目至少包含弱點掃描、基本滲透測試、惡意程式/後門檢測、帳號與密碼安全檢測、通訊加密安全檢測及系統安全設備檢測。
<table>
<tr><th>檢測項目</th><th>檢測內容</th></tr>
<tr><td>弱點掃描</td><td>● 作業系統漏洞掃描
● Web 系統漏洞掃描
● 已知 CVE 漏洞
● 常見 Web 漏洞</td></tr>
<tr><td>基本滲透測試</td><td>● 身分繞過驗證
● 權限提升
● API 安全
● Session 管理</td></tr>
<tr><td>惡意程式/後門檢測</td><td>● 木馬程式
● 隱藏帳號
● 可疑程序
● 可疑對外連線
● 後門程式</td></tr>
<tr><td>帳號與密碼安全檢測</td><td>● 預設帳號
● 弱密碼
● 密碼政策
● 密碼鎖定機制</td></tr>
<tr><td>通訊加密安全檢測</td><td>● TLS 版本
● 憑證有效性
● 是否使用弱加密</td></tr>
</table>
</td></tr>
</table>

	● 是否使用明文傳輸
系統安全設備檢測	● 不必要服務是否關閉 ● Port 開放情形 ● 系統權限設定 ● Patch 更新狀況

（4） 因產品特性、市場供應限制、預算成本或其他特殊因素，致無法提供前述證明文件者，經專案簽奉核准後，得由廠商提供自我安全檢測、評估報告(韌體安全性更新報告及漏洞更新管理機制等)、切結書及相關佐證等資料替代，廠商所提供之自我檢測結果如有虛偽不實，或交付產品經發現具重大資安風險者，單位得依契約辦理解約、求償或停止採購往來。

檢測項目	報告內容
已知漏洞檢查	● 弱點掃描工具名稱 ● 掃描日期 ● 漏洞等級（H/M/L） ● 高風險漏洞修補情形
惡意程式掃描	● 使用防毒或檢測工具名稱 ● 檢測結果 ● 是否發現木馬或後門
預設帳號及密碼檢查	● 是否存在預設帳號 ● 預設密碼是否變更 ● 是否符合基本密碼強度
通訊安全檢查	● 是否使用加密通訊（HTTPS/TLS） ● 是否存在明文傳輸 ● 是否使用弱加密技術
系統安全檢查	● 不必要服務是否關閉 ● 不必要 Port 是否關閉 ● 系統更新與 Patch 狀況

（5） 其他：國內無相關認證機制，且非資安防護設備、未處理敏感資料及不影響系統運作安全之設備或周邊，其資安風險較低，經採購單位通資業管部門審認無風險疑慮後，免取得認證；如鍵盤、滑鼠、螢幕、投影機、記憶卡等。

（6） 未安裝作業系統之電腦、伺服器等設備，於交付驗收

	時，提供下列佐證（擇一或數項）者，得免辦理系統層級資安檢測： ①韌體（BIOS 等）最新版本佐證。 ②產品來源及授權證明文件。 ③設備未預載聲明文件。 ④設備規格及韌體資訊文件。 ⑤供應鏈安全或交付完整性說明。 ⑥其他足以證明設備未遭竄改之相關文件。 （7） 共同供應契約採購之物品或設備，依該契約既有審查機制及資安相關規範辦理，不另要求廠商提供資安檢測報告或證明文件。
備註：驗收標的物具產品風險之購案且屬硬體，應將本表納入管制。	

附件六

資安管控要求事項-物品安全認證	
項目	要求事項
軟體資安檢測	（1）驗收採購標的物為資訊（系統）軟體，須完成原始碼檢測、第三方元件檢測及弱點掃描等安全檢測作業，並提供軟體物料清單（SBOM）及檢測報告，檢測發現之資安弱點應完成修補及驗證。 （2）如屬國際通用或原廠標準化商品（如微軟 Word 等），無法提供個別資安檢測報告者，得以下列資料代替（擇一或數項）： ①原廠公開之產品安全白皮書或安全架構說明文件（原廠資安證明文件）。 ②原廠之弱點揭露（CVE）與修補機制說明。 ③原廠安全更新及維護政策文件。 （3）共同供應契約採購之商用軟體，依該契約既有審查機制及資安相關規範辦理，不另要求廠商提供資安檢測報告或證明文件。
備註：驗收標的物具產品風險之購案且屬軟體，應將本表納入管制。	

附件七

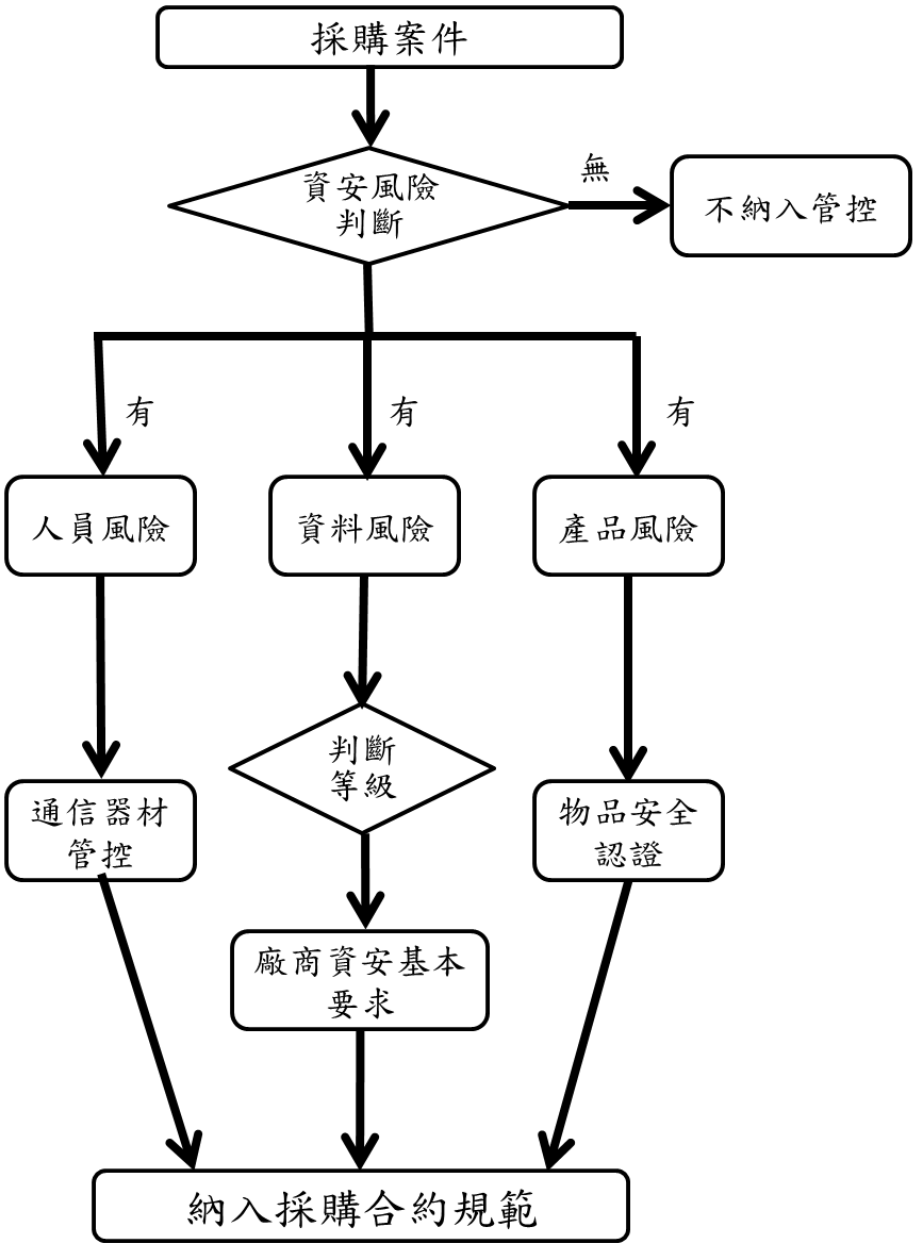
廠商資安風險判定表

名稱/案號：
單位：
購案類型：
承辦人：
評估日期：

項次	項目	判定結果	備考
1.1	廠商人員須進入機關辦公區域。 □是□否	□具人員風險	符合一項以上
1.2	廠商人員須進入機關機房或管制區域 □是□否		
1.3	廠商人員須於機關場域執行作業。□是□否		
2.1	廠商須接觸、儲存、傳輸、處理及產出機關非公開資訊。 □是□否	□具資料風險	符合一項以上
2.2	廠商須接觸、儲存、傳輸、處理及產出機關資訊系統、軟體、應用程式之程式碼。 □是□否		
2.3	廠商須接觸、儲存、傳輸、處理及產出個人資料或涉密資訊。□是□否		
3.1	採購標的具網路連線功能。 □是□否	□具產品風險	符合一項以上
3.2	採購標的具資料儲存功能。 □是□否		
3.2	採購標的具資料處理功能。 □是□否		
3.4	採購標的介接機關資訊系統。□是□否		
3.5	採購標的部署於機關內部網路。□是□否		
3.6	採購標的屬雲端服務或遠端服務。 □是□否		

附件八

國防採購廠商資安風險判定流程圖



說明：

1. 依風險判定結果將「資安管控要求項目」納入採購契約附件，要求廠商據以執行。
2. 參照「國防部內購資訊服務採購契約通用條款」第十五條「違約及服務績效違約金」及其附表加註資安查核罰則，違約金計點參考範例如次：

評估項目	評斷方式	要求基準	違約金計點
資安查核	未依資安基本要求事項辦理	每次統計	每次每項__點

附件九

資通安全維護稽核自評表

公司名稱：

級別：□一級/□二級/□三級

稽核項目	資通安全稽核檢核項目	自評結果	佐證文件
1.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。			
1.1	應界定公司/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。（各級適用）	□符合 □未符合	
1.2	應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） ➢ 未涉及個人資料、資訊系統開發或維運、涉密資訊處理之案件得不適用。	□符合 □未符合 □不適用	
1.3	訂定資通安全政策，由管理階層核定，並定期檢視其重要性。（各級適用）	□符合 □未符合	
1.4	指派適當高層人員兼任資通安全長，負責推動及督導公司內部資通安全相關事務。（各級適用）	□符合 □未符合	
1.5	訂定公司人員辦理業務涉及資通安全事項之考核機制及獎懲基準。（各級適用）	□符合 □未符合	
2. 資通安全專業證照			
2.1	資通安全專職人員應每年接受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。（各級適用）	□符合 □未符合	

2.2	一般使用者及主管應每年接受 3 小時以上之資通安全通識教育訓練。(各級適用)	□符合 □未符合	
2.3	資安專職人員應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。(各級適用)	□符合 □未符合	
3.限制使用危害國家資通安全產品			
3.1	購（專）案範圍須限制使用中國大陸品牌之軟、硬體服務。(各級適用)	□符合 □未符合	
4.資訊作業管理			
4.1	辦公室內電腦應運用軟體管制可移動式儲存媒體存取作業。(各級適用)	□符合 □未符合 □不適用	
4.2	應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。(各級適用)	□符合 □未符合 □不適用	
4.3	應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。(各級適用)	□符合 □未符合 □不適用	
4.4	應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。(各級適用)	□符合 □未符合 □不適用	
4.5	應訂定委外廠商對於公司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，是否立即通知公司並採行補救措施。(各級適用)	□符合 □未符合 □不適用	
4.6	委外關係終止或解除時，應確認委外廠商返還、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。(各級適用)	□符合 □未符合 □不適用	
4.7	應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（如對委外廠商端實地稽核、要求委外廠商	□符合 □未符合 □不適用	

	提供異常報告、要求委外廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理。(各級適用)		
5.實體與環境安全			
5.1	應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. 第一級：4 人。 2. 第二級：2 人。 3. 第三級：1 人。	□符合 □未符合 □不適用	
5.2	應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。(各級適用)	□符合 □未符合 □不適用	
5.3	應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，存放處所環境須符合實體安全防護。(各級適用)	□符合 □未符合 □不適用	
5.4	應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。(各級適用)	□符合 □未符合 □不適用	
6.資訊作業安全管理			
6.1	須完成下列資通安全防護措施，並維持其有效性及更新。 A. 防毒軟體 B. 網路防火牆 C. 電子郵件過濾機制 D. 內部（區域）網路管理系統（防止未授權設備連接公司網路） E. 入侵偵測及防禦機制 F. 應用程式防火牆（具有對外服務之核心資通系統者）	□符合 □未符合 □不適用	

	G. 進階持續性威脅攻擊防禦 分級項目： 1. 第一級：符合 A-G 項。 2. 第二級：符合 A-G 項。 3. 第三級：符合 A-D 項。		
6.2	應建置資通安全威脅偵測管理（SOC）機制。 1. 第一級：本項需符合。 2. 第二級：本項需符合。 3. 第三級：本項不適用。	□符合 □未符合 □不適用	
6.3	應針對全部核心資通系統辦理網站安全弱點檢測。 分級項目： 1. 第一級：每年辦理2次（上、下半年各一次）。 2. 第二級：每年辦理1次。 3. 第三級：每 2 年辦理 1 次。	□符合 □未符合 □不適用	
6.4	應針對全部核心資通系統辦理系統滲透測試。 1. 第一級：每年辦理 1 次。 2. 第二級：每 2 年辦理 1 次。 3. 第三級：每 2 年辦理 1 次。	□符合 □未符合 □不適用	
6.5	應辦理資通安全健診，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。 1. 第一級：每年辦理 1 次。 2. 第二級：每 2 年辦理 1 次。 3. 第三級：每 2 年辦理 1 次。	□符合 □未符合 □不適用	
6.6	應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），並針對日誌、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。(各級適用)	□符合 □未符合 □不適用	
6.7	應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、針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則、	□符合 □未符合 □不適用	

	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）。(各級適用)		
6.8	應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。(各級適用)	□符合 □未符合 □不適用	
6.9	應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。(各級適用)	□符合 □未符合 □不適用	
6.10	網路架構設計須符合業務需要及資安要求，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。(各級適用)	□符合 □未符合 □不適用	
6.11	針對公司內部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。(各級適用)	□符合 □未符合 □不適用	
6.12	每年進行 1 次社交工程演練，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。(各級適用)	□符合 □未符合 □不適用	
6.13	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。(各級適用)	□符合 □未符合 □不適用	
6.14	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），針對重要資料的交換過程，保存適當之監控紀錄。(各級適用)	□符合 □未符合 □不適用	
6.15	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。(各級適用)	□符合 □未符合 □不適用	
6.16	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）。(各級適用)	□符合 □未符合 □不適用	

6.17	針對使用者電腦訂定軟體安裝管控規則，確認授權軟體及免費軟體之使用情形，且定期檢查。(各級適用)	□符合 □未符合 □不適用	
6.18	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。(各級適用)	□符合 □未符合 □不適用	
7.存取控制			
7.1	訂定人員之資通安全作業程序、權責及應負之資安責任，明確告知保密事項，且簽署保密協議。(各級適用)	□符合 □未符合	
7.2	辦公室規範律定資訊帳號密碼須符合複雜度要求並不得少於： 第一級：15 碼以上 第二級：12 碼以上 第三級：8 碼以上	□符合 □未符合	
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。(各級適用)	□符合 □未符合 □不適用	
7.4	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。(各級適用)	□符合 □未符合 □不適用	
8.危機處理			
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。(各級適用)	□符合 □未符合 □不適用	
8.2	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。(各級適用)	□符合 □未符合 □不適用	
8.3	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	□符合 □未符合	

	理事件查處作業。(各級適用)	□不適用	
9.其他(資通系統開發及維護安全類適用)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	自行或委外開發之資通系統應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。(各級適用)	□符合 □未符合 □不適用	
9.2	資通系統開發前，應設計安全性要求，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。(各級適用)	□符合 □未符合 □不適用	
9.3	資通系統設計階段，應依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估。(各級適用)	□符合 □未符合 □不適用	
9.4	資通系統開發階段，須避免常見漏洞(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。(各級適用)	□符合 □未符合 □不適用	
9.5	資通系統測試階段，須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。(各級適用)	□符合 □未符合 □不適用	
9.6	資通系統上線前，須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。(各級適用)	□符合 □未符合 □不適用	
9.7	資通系統開發如委外辦理，應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。(各級適用)	□符合 □未符合 □不適用	
9.8	應將開發、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。(各級適用)	□符合 □未符合 □不適用	
9.9	儲存及管理資通系統發展相關文件，應有版本及權限控管。(各級適用)	□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，應針對測試資料建立保護措施，且留存相關作業紀錄。(各級適用)	□符合 □未符合 □不適用	
9.11	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。(各級適用)	□符合 □未符合 □不適用	

附件十

廠商自行評核（檢測）項目		
項次	檢測項目	報告內容
硬體	已知漏洞檢查	● 弱點掃描工具名稱 ● 掃描日期 ● 漏洞等級（H/M/L） ● 高風險漏洞修補情形
	惡意程式掃描	● 使用防毒或檢測工具名稱 ● 檢測結果 ● 是否發現木馬或後門
	預設帳號及密碼檢查	● 是否存在預設帳號 ● 預設密碼是否變更 ● 是否符合基本密碼強度
	通訊安全檢查	● 是否使用加密通訊（HTTPS/TLS） ● 是否存在明文傳輸 ● 是否使用弱加密技術
	系統安全檢查	● 不必要服務是否關閉 ● 不必要 Port 是否關閉 ● 系統更新與 Patch 狀況
軟體	驗收採購標的物為資訊（系統）軟體，須完成原始碼檢測、第三方元件檢測及弱點掃描等安全檢測作業，並提供檢測報告，檢測發現之資安弱點應完成修補及驗證。	

附件十一

切結書（範本）

立切結書人（廠商名稱）：

統一編號：

茲因承攬（機關名稱）：＿＿＿＿＿＿＿＿＿＿＿＿＿＿之「＿＿＿＿＿＿＿＿＿＿＿＿＿＿案」（以下簡稱本案），

涉及提供　　設備，為確保資通安全，特立本切結書，並承諾遵守下列事項：

一、所提送之資安檢測報告、檢測結果及佐證資料均為本公司據實提供，內容真實無虛偽、偽造、變更或隱匿情事。

二、本公司已依機關規定之檢測項目及檢測方式完成檢測，並確認所提供產品(或系統)符合本案資安要求。

三、如經查證有不實、偽造、變造、隱匿重要資訊或其他違反契約情事，本公司願負一切法律責任，並接受機關依契約、政府採購法及相關規定辦理。

四、本公司同意機關於必要時得要求提供檢測過程紀錄、原始檢測資料或其他相關佐證文件，以供查驗。

五資安事件通報與處理

（一）如發現設備存在重大資安漏洞或遭受攻擊情形，應於知悉後 24 小時內通報機關。

（二）應配合機關進行資安事件調查及改善措施。

六、維護與支援

（一）應提供至少＿＿年之安全更新與維護服務。

（二）於產品生命週期內應持續提供漏洞修補。

七、違約責任：如違反本切結書之約定，機關得終止或解除契約，立切結書人願負相關法律及賠償責任。

此致

（機關名稱）

立切結書人：＿＿＿＿＿＿＿＿＿＿＿＿（公司大小章）

中　華　民　國　　年　　月　　日

附件十二

風險評估報告（範本）

一、案由

本單位辦理「○○資訊設備採購案」，依現行資訊安全規範，原要求廠商所提供設備須通過第三方實驗室資安檢測後始得採購，以確保設備符合資通安全要求。惟經市場調查及廠商評估，目前第三方實驗室檢測費用高昂，部分設備檢測成本已超出本採購案預算編列範圍，若仍維持原要求，恐導致廠商無法投標、購案流標，或無法於預定期程內完成採購，進而影響單位業務推動。爰依風險管理原則，評估於特定條件下，改採「開源檢測工具自主檢測及廠商切結書」之替代措施，並報請資安長核准辦理。

二、現行規範要求

（一）資訊設備應符合本單位資通安全要求。

（二）原規定須提供第三方實驗室資安檢測證明文件，始得辦理驗收或採購。

（三）第三方檢測範圍包含：

1. 弱點掃描。
2. 惡意程式檢測。
3. 預設帳號與密碼檢查。
4. 韌體/軟體版本檢視。
5. 網路服務與通訊埠檢查。

三、問題說明

（一）經洽詢多家廠商，第三方實驗室檢測費用約占設備總價之○%至○%。

（二）部分低單價設備，其檢測費用甚至高於設備本體價格。

（三）若強制要求第三方檢測，可能產生下列影響：

1. 廠商無投標意願。
2. 採購預算不足。
3. 採購案流標。
4. 專案期程延宕。
5. 單位業務運作受影響。

四、風險評估分析

（一）風險項目分析

1. 未經第三方驗證：設備可能存在未知弱點。
2. 廠商自主檢測可信度不足：檢測完整性可能不一致。
3. 惡意韌體或後門風險：可能影響資訊安全。
4. 採購無法進行：業務中斷或延宕。
5. 預算超支：無法完成年度採購。

（二）替代措施風險降低作法

1. 使用開源弱點掃描工具進行檢測。
2. 提供掃描報告及檢測紀錄。
3. 提供設備軟韌體版本資訊。
4. 關閉不必要服務與預設帳號。
5. 提供資安切結書。
6. 同意本單位後續抽測或複測。
7. 如發現重大漏洞，廠商須限期改善。

五、建議替代方案

（一）適用條件

1. 低風險資訊設備。
2. 不涉及機敏資料處理。
3. 不具關鍵基礎設施控制功能。
4. 預算不足以支應第三方檢測。
5. 經專案風險評估後可接受者。

（二）替代作法，由廠商提出下列文件，經本單位審查通過後，得作為第三方檢測之替代措施：

1. 開源檢測工具掃描報告。
2. 自主檢測紀錄。
3. 資安切結書。
4. 後續漏洞修補承諾。

六、風險接受評估

（一）本案設備屬低至中度風險設備。

（二）雖未採第三方實驗室檢測，惟透過開源工具檢測、文件佐證及切結機制，可部分降低資安風險。

（三）相較於採購無法執行之營運風險，本案資安風險尚屬可控範圍。

（四）建議於強化後續抽測及漏洞管理機制下，同意採行替代措施。

七、擬辦

（一）建請同意本案於預算限制情形下，得以「開源檢測工具自主檢測及廠商資安切結書」方式替代第三方實驗室檢測。
（二）後續由承辦單位留存相關檢測報告及切結文件備查。
（三）如後續發現重大資安疑慮，得要求廠商補送第三方檢測報告或限期改善。

八、附件

（一）廠商資安切結書範本。
（二）開源檢測工具建議清單。
（三）自主檢測報告範例。
（四）風險評估表。
（五）採購預算分析資料。

附件十三

（單位名稱）XX年度 採購案廠商資安管控案件統計表								
項次	採購案名稱	採購類型	風險面向	是否納入資安要求	是否進行資安稽核	稽核結果	缺失改進情形	備考
1	○○系統建置案	資訊服務	□人員 □資料 □產品	是	是	符合	無	