	A	B	C	D	E	F
1	一般要求	安全要求內容		安全等級 (*代表僅屬於網路攝影機資安要求)		
2				1級	2級	3級
3	實體安全	5.1.1. 實體埠之安全管控	5.1.1.1 產品僅提供使用者有限權限之設計，即預設不應透過實體介面存取產品作業系統之除錯模式。	V		
4			5.1.1.2 卸除式儲存媒體使用的插槽須移除；抑或卸除式儲存媒體支援儲存媒體保護機制，即產品之儲存媒體不應在本機以外的機器被存取。		V*	
5		5.1.2. 實體異常行為警示	5.1.2.1 產品須具有實體埠插拔操作記錄功能。			
6			5.1.2.2 產品須具備相關警示機制於實體操作發生斷訊時。			
7		5.1.3. 實體防護	5.1.3.1 產品外部不應有徒手即可還原預設通行碼的設計。	V		
8			5.1.3.2 產品須採用一體成形或防拆螺絲等機殼防拆除保護設計。		V*	
9		5.1.4. 安全啟動	5.1.4.1 產品應支援安全啟動(Secure Boot)功能，不應以未經授權的韌體、驅動程式及作業系統執行開機，以確保系統的完整性及可信度。			V
10	系統安全	5.2.1. 作業系統與網路服務安全	5.2.1.1 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統CVSS v3嚴重性等級評比為重大。	V		
11			5.2.1.2 產品之作業系統與網路服務，不應存在國家弱點資料庫所公開的常見弱點與漏洞資料，且漏洞評鑑系統CVSS v3嚴重性等級評比為高。			V
12		5.2.2. 網路服務連接埠安全	5.2.2.1 產品開啟之網路服務須為廠商提供必要服務之所需，防止產品因啟用網路介面而被侵入的可能性，且廠商須於產品文件中標註得啟用之網路服務，避免未宣告之網路服務被開啟。	V		
13		5.2.3. 更新安全	5.2.3.1(a) 產品若支援離線手動更新，則更新檔案須加密保護以確保機密性，且須採用FIPS 140-2 Annex A [14] 所核可之加密演算法；抑或是產品韌體之程式碼與安裝檔內其它檔案中，不應存在明文或甚至可被解密回復之敏感性資料。	V		
14			5.2.3.1(b) 產品若支援線上更新，其更新路徑須通過安全通道，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)，其中於身分鑑別過程須驗證憑證合法性，以及有效性(如：發證單位、有效期限、格式錯誤及憑證簽章等)。	V		
15			5.2.3.2 產品必須具備驗證韌體之正確性及完整性的功能。	V		
16			5.2.3.3 產品必須具備備援更新功能，即發生更新失敗時，系統能回復正常運作。	V		
17		5.2.4. 敏感性資料儲存安全	5.2.4.1 產品所儲存的敏感性資料，須被授權的個體始可存取。	V		
18			5.2.4.2 產品所儲存之身分鑑別因子、加解密用之金鑰(不含非對稱加密用之公鑰)及個人資料不應明文儲存，而保護資料的加密方式須採用FIPS 140-2 Annex A所核可之加密演算法。	V		

	A	B	C	D	E	F
1	一般要求	安全要求內容		安全等級 (*代表僅屬於網路攝影機資安要求)		
2				1級	2級	3級
19			5.2.4.3 產品須提出金鑰管理程序，以確保金鑰管理的品質。		V	
20			5.2.4.4 敏感性資料須存放於產品的安全區域(Security Domain)，從正常作業環境中隔離。			V
21		5.2.5. 網頁管理介面安全	5.2.5.1 產品之網頁管理介面不應存在OWASP web top 10 [15]之Injection及Cross-Site Scripting (XSS)攻擊。	V		
22		5.2.6. 操控程式之應用程式安全	5.2.6.1 應用程式介面，須具備身分鑑別機制，且其鑑別機制安全依5.4.1.1及5.4.1.2之要求。	V		
23			5.2.6.2 應用程式介面，其通行碼鑑別安全依5.4.2該要求項之所有要求。	V		
24			5.2.6.3 應用程式介面，其權限管控依5.4.3該要求項之所有要求。	V		
25		5.2.7. 日誌檔與警示	5.2.7.1 須具備安全事件記錄與顯示功能，確實記錄使用者的存取行為，得以查核未授權或異常的登入操作。其內容須包括完整時間戳記、使用者身分及及執行結果，供後續查閱之用。	V		
26			5.2.7.2 產品之安全事件紀錄須具備權限控管機制，該日誌檔不應允許未經授權的存取。	V		
27			5.2.7.3 產品之安全事件日誌檔須具備日誌滾動(log rotate)機制。	V		
28			5.2.7.4 產品須提供系統警示功能以避免安全事件紀錄無法儲存之狀況發生。		V	
29		5.3.1. 敏感性資料傳輸安全	5.3.1.1 敏感性資料之網路傳輸預設須通過安全通道，且安全通道版本須符合「附錄A」的要求，同時金鑰交換協議應支援前向安全功能(Forward Secrecy)，其中於身分鑑別過程須驗證憑證合法性，以及有效性(如：發證單位、有效期限、格式錯誤及憑證簽章等)。	V		
30			5.3.1.2 安全通道所使用之加密演算法須支援AES-256同等或以上加密強度的演算法。			V
31		5.3.2. 通訊協定與設置安全	5.3.2.1 產品須提供使用者得自行開/關「網路裝置資訊探詢」功能，包括：通用隨插即用通訊協定 (UPnP)、簡單網路管理協定 (SNMP) 及零配置通訊協定 (Bonjour)。	V		
32			5.3.2.2 預設不應透過網路連線存取產品作業系統之除錯模式。	V		
33	通訊安全		5.3.2.2 產品所提供之自行開/關「網路裝置資訊探詢」功能，預設須為關閉，包括：通用隨插即用通訊協定(UPnP)、簡單網路管理協定(SNMP)及零配置通訊協定(Bonjour)。			V*

	A	B	C	D	E	F
1	一般要求	安全要求內容		安全等級 (*代表僅屬於網路攝影機資安要求)		
2				1級	2級	3級
34			5.3.2.3 產品之關鍵通訊協定(見附錄B)，不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。		V	
35		5.3.3. Wi-Fi通訊安全	5.3.3.1 產品須提供使用者得自行開/關「Wi-Fi保護設置 (WPS)」之WPS PIN功能，而其預設值須為關閉狀態。	V		
36			5.3.3.2 Wi-Fi的安全機制預設須採用「Wi-Fi保護存取 (WPA)」，且Wi-Fi保護存取之版本須符合「附錄C」的要求。	V		
37			5.3.3.3 產品支援Wi-Fi協定，則不應存在錯誤處理漏洞，包括檢視訊息長度、訊息識別碼及關鍵協定屬性等欄位，導致產品因發生崩潰而服務中止的情形。		V	
38			5.3.3.4 Wi-Fi認證安全機制須支援802.1X基於埠的網路存取控制(Port-Based Networks Access Control)。			V
39	身分鑑別與授權	5.4.1. 鑑別機制安全	5.4.1.1 存取產品資源前，須透過具備防止重送攻擊之身分鑑別機制。	V		
40			5.4.1.2 鑑別錯誤訊息不應顯露出合法使用者名稱。	V		
41			5.4.1.3 產品應具備上傳憑證之功能，以增加憑證鑑別機制之可信度。		V	
42			5.4.1.4 產品每一次還原出廠設定時，憑證之金鑰(包括SSH及TLS)都須改變，確保每台產品金鑰之唯一性，及降低金鑰外洩可能引發之資安風險。		V	
43			5.4.1.5 產品之鑑別機制須採用多因子鑑別。			V
44			5.4.1.6 相連之影像監控產品須支援雙向認證，確保相連裝置之可信度。			V
45		5.4.2. 通行碼鑑別機制	5.4.2.1 廠商所生產之裝置，其預設通行碼都須相異；抑或首次成功取得產品存取之授權，須強制更改預設通行碼。	V		
46			5.4.2.2 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼長度至少大於8個字元。	V		
47			5.4.2.3 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼中之字元必須符合下列四種字元中的三種，1.英文大寫字元 (A 到 Z)；2.英文小寫字元 (a 到 z)；3.10 進位數字 (0 到 9)；4.非英文字母字元 (例如：！、$、#、%)。	V		
48			5.4.2.4 產品在登入通行碼的設計上須有輸入頻率及次數的限制，即：(a) 最高五次嘗試登入失敗即鎖定帳戶、(b) 在一定時間內須鎖定帳戶、(c) 至少經過一定時間，始可將失敗的登入嘗試計數器重設為零次。	V		
49			5.4.2.5 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼含使用者帳戶名稱全名中，不能包含3個以上之連續字元。			V

	A	B	C	D	E	F
1	一般要求	安全要求內容		安全等級 **(*代表僅屬於網路攝影機資安要求)**		
2				1級	2級	3級
50			5.4.2.6 通行碼強度原則參照政府組態基準之通行碼原則類別，通行碼須執行歷程記錄。			V
51		5.4.3. 權限控管	5.4.3.1 產品須將使用者角色切割成數個使用者環境，例如：一般使用者與系統管理者等，並於產品文件中定義個別的權限，確保產品之角色權限與產品文件所宣告的相符。	V		
52			5.4.3.2 產品之授權行為，須存在閒置時限供使用者設定，假如遠端連線逾時、遺失或結束，須要求新的鑑別。	V		
53	隱私保護	5.5.1. 隱私資料的存取保護	5.5.1.1 產品所儲存的隱私資料，須被授權的個體始可存取。	V		
54			5.5.1.2 使用者對其儲存的隱私資料擁有刪除之權限和功能。	V		
55			5.5.1.2 產品應支援隱私遮罩，避免正常作業引發之隱私外洩風險。		V*	
56			5.5.1.3 每次發生新的存取事件時，產品必須主動發出警示。	V		
57		5.5.2. 隱私資料的傳輸保護	5.5.2.1 隱私資料傳輸機密性依「5.3.1.1敏感性資料傳輸安全」該節之要求。	V		
58			5.5.2.2 隱私資料傳輸機密性依「5.3.1.2敏感性資料傳輸安全」該節之要求。			V