TAICS

TAICS TS-0046 v1.0 : 2021

消費性物聯網產品資安測試規範

Cybersecurity test specification for consumer IoT products

2021 / 11 / 25

社團法人台灣資通產業標準協會
Taiwan Association of Informationand Communication Standards

消費性物聯網產品資安測試規範

Cybersecurity test specification for consumer IoT products

出版日期: 2021/11/25
終審日期: 2021/09/24

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人資訊工業策進會 毛敬豪 資安鑄造廠總經理

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 物聯網資安工作組組長：財團法人資訊工業策進會 高傳凱 副主任

技術編輯：財團法人資訊工業策進會 賴怡伶 工程師

財團法人電信技術中心 王慶豐 副主任、許博堯 副理

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

大同股份有限公司、中華資安國際股份有限公司、中華電信股份有限公司、中興保全科技股份有限公司、友達光電股份有限公司、台灣是德科技股份有限公司、台灣惠普資訊科技股份有限公司、台灣德國萊因技術監護顧問股份有限公司、台灣檢驗科技股份有限公司、安華聯網科技股份有限公司、行動檢測服務股份有限公司、尚承科技股份有限公司、神盾股份有限公司、財團法人工業技術研究院、財團法人資訊工業策進會、財團法人電信技術中心、國立陽明交通大學、國家中山科學研究院、勤業眾信聯合會計師事務所、遠傳電信股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

友訊科技股份有限公司、天主教輔仁大學、行政院消費者保護處、財團法人中華民國消費者文教基金會、國立雲林科技大學、國立臺灣科技大學

本規範由國家通訊傳播委員會支持研究制定。

目錄

前言

本規範依據台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業規範。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

有鑑於消費性物聯網產品已逐漸普及應用於日常生活，根據IEK的「物聯網資安威脅與解決方案發展方向」[(1)]研究報告中指出，七大高風險遭駭客攻擊之物聯網裝置排行中(七大高風險物聯網裝置：家用網路路由器、電視盒、智慧家居產品、植入式醫療裝置、關鍵基礎設施、嬰兒監視器及連網汽車)，就有四種屬於消費性物聯網產品(家用網路路由器、機上盒、智慧家居產品、嬰兒監視器)，消費性物聯網產品相對安全防護能力更加不足，資安問題屢見不鮮，卻未有較明顯且具體的改善。因此在國家通訊傳播委員會的支持下，制定本規範。

本規範係依據台灣資通產業標準協會所制定之 TAICS TS-0045 v1.0「消費性物聯網產品資安標準」[1]訂定，其中具體明列資安檢測之測試項目、測試條件、測試方法與測試結果等事項，俾利消費性物聯網產品之製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。

1. 適用範圍

本規範為依據 TAICS TS-0045 v1.0 「消費性物聯網產品資安標準」規定，所訂定之測試規範。

本規範的適用範圍涵蓋消費性物聯網應用設備及其連接之無線網路環境，如下圖 1，惟關聯服務不在本測試規範適用範圍內。

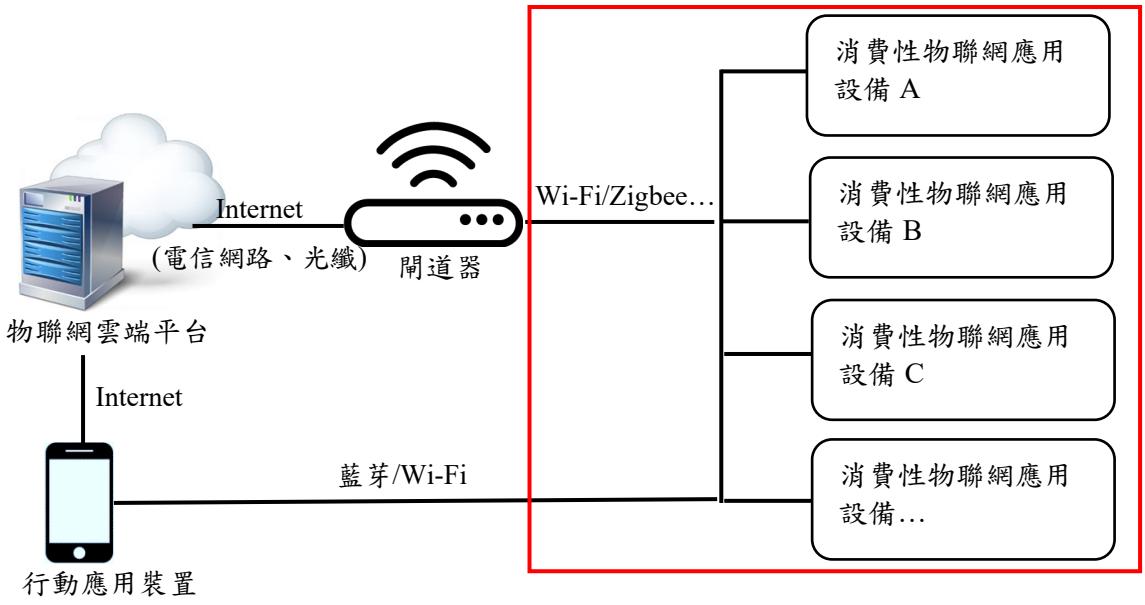

圖 1 適用範圍示意圖

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版(包括補充增修)。無加註年份者，適用該最新版(包括補充增修)。

[1] TAICS TS-0045 v1.0:2021 消費性物聯網產品資安標準

3. 用語及定義

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」所述，及下列用語及定義適用於本規範。

3.1 密碼套件 (Cipher Suite)

係指使用於安全通道(SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分驗證、加密、訊息鑑別碼(MAC)和金鑰交換演算法。

3.2 網路埠掃描 (Port Scan)

使用網路掃描工具對網路埠掃描來偵測電腦有開啟哪些網路埠或網路服務，以此確認可使用的埠口，進一步探尋其漏洞，藉此找到未經授權的存取點。

3.3 本地端管理介面 (Local Management Interface)

消費者直接存取與控制產品的操作介面，不應連接網際網路經由物聯網雲端平台操控產品，例如產品應用程式或透過電腦與產品連接並以 IP 地址開啟的網頁管理頁面等。

4. 測試項目

本節依據 TAICS TS-0045 v1.0「消費性物聯網產品資安標準」制定相對應之安全測試項目與測試方法。

實機測試標準總表，如表 1 所示，第一欄為安全測試構面，包括：(1)身分鑑別、(2)漏洞安全、(3)軟韌體更新、(4)資料機密性與完整性、(5)系統完整性、(6)資源可用性、(7)隱私保護及(8)異常與警示；第二欄為安全要求，係依第一欄安全測試構面設計對應之安全要求；第三欄為安全層級與條件；第四欄為安全測試細項，為各安全測試項目所做之測試標準。其中，關於第三欄安全層級與條件之說明，如下所述：

(a) 第三欄之安全層級說明:

M：此項目為強制性的安全要求。

R：此項為建議的安全要求。

MC：此項目為強制性且有條件的安全要求。

RC：此項目為建議且是有條件的安全要求。

(b) 第三欄之條件說明:

(1) 使用通行碼

(2) 使用預設通行碼

(3) 軟體組件不可更新

(4) 受限制設備

(5) 非受限制設備

(6) 收集遙測數據

(7) 基於消費者同意的基礎下處理個人資料

(8) 提供使用者認證的設備

(9) 支援自動更新及/或更新通知的設備

(10) 基於安全起見，設備識別使用硬編碼(hard-coded)唯一性

(11) 更新是透過網路介面傳輸

(12) 有更新機制

(13) 除錯介面是透過實體存取

表 1 實機測試標準總表

安全構面	安全要求	安全層級與條件	安全測試項目
5.1 身分鑑別	5.1.1 通行碼鑑別	MC (1)	5.1.1.1
		MC (2)	5.1.1.2
	5.1.2 鑑別機制	MC (8)	5.1.2.1
		MC (5)	5.1.2.2
		M	5.1.2.3
5.2 安全漏洞	5.2.1 漏洞政策與安全設置	M	5.2.1.1
		R	5.2.1.2
		R	5.2.1.3
		R	5.2.1.4
		R	5.2.1.5
		R	5.2.1.6
	5.2.2 最小暴露攻擊面	M	5.2.2.1
		M	5.2.2.2
		R	5.2.2.3
		MC (13)	5.2.2.4
		R	5.2.2.5
		R	5.2.2.6
		R	5.2.2.7
		R	5.2.2.8
		R	5.2.2.9
5.3 軟韌體更新	5.3.1 更新安全	R	5.3.1.1
		MC (5)	5.3.1.2
		MC (12)	5.3.1.3

安全構面	安全要求	安全層級與條件	安全測試項目
5.3 軟韌體更新	5.3.1 更新安全	RC (12)	5.3.1.4
		RC (12)	5.3.1.5
		RC (9, 12)	5.3.1.6
		MC (12)	5.3.1.7
		MC (12)	5.3.1.8
		RC (12)	5.3.1.9
		M (11, 12)	5.3.1.10
		RC (12)	5.3.1.11
		RC (12)	5.3.1.12
		M	5.3.1.13
		RC (3, 4)	5.3.1.14
		RC (3, 4)	5.3.1.15
		M	5.3.1.16
5.4 資料機密性與完整性	5.4.1 敏感性安全參數儲存	M	5.4.1.1
		MC (10)	5.4.1.2
		M	5.4.1.3
		M	5.4.1.4
	5.4.2 傳輸資料保護	M	5.4.2.1
		R	5.4.2.2
		R	5.4.2.3
		R	5.4.2.4
		M	5.4.2.5
		R	5.4.2.6
		M	5.4.2.7
		M	5.4.2.8

安全構面	安全要求	安全層級與條件	安全測試項目
5.5 系統完整性	5.5.1 實體入侵防護	R	5.5.1.1
	5.5.2 輸入驗證	M	5.5.2.1
5.6 資源可用性	5.6.1 資源管理	R	5.6.1.1
		R	5.6.1.2
		R	5.6.1.3
5.7 隱私保護	5.7.1 隱私保護能力	R	5.7.1.1
		M	5.7.1.2
		M	5.7.1.3
		M	5.7.1.4
		R	5.7.1.5
		R	5.7.1.6
		R	5.7.1.7
		M	5.7.1.8
		MC (7)	5.7.1.9
		M	5.7.1.10
		RC (6)	5.7.1.11
		MC (6)	5.7.1.12
5.8 異常與警示	5.8.1 安全事件警示	R	5.8.1.1
		RC (6)	5.8.1.2

5. 資安測試規範

5.1 身分鑑別測試

檢視消費性物聯網產品之身分鑑別與權限控管安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.1.1 通行碼鑑別測試

5.1.1.1 預設通行碼測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.1.1

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否沒有相同的預設通行碼或預設通行碼會於首次上線後強制要求更改。

(d) 測試條件：

(1) 產品未支援通行碼鑑別機制，則不適用此測項。

(2) 產品應保持出廠預設組態。

(3) 若產品存在預設通行碼，應提供產品預設通行碼之設計文件。

(e) 測試佈局：

如圖 2。

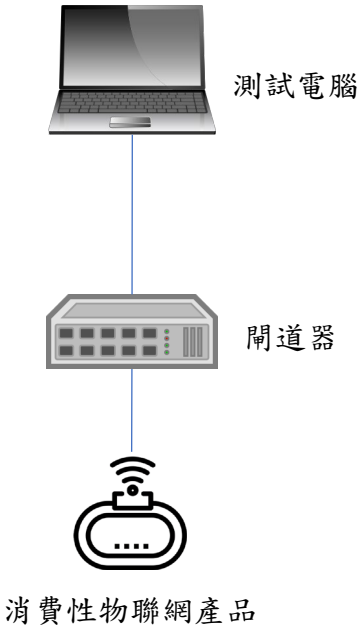

圖 2 測試示意圖

(f) 測試方法：

(1) 審閱產品之預設通行碼設計文件，檢視產品是否存在相同之預設通行碼。

(2) 將測試電腦或行動裝置連接產品。

(3) 根據使用說明文件，從管理介面輸入通行碼。

(4) 確認在未設定新通行碼的情況下，不可存取產品。

(g) 測試結果：

(1) 產品之預設通行碼為全球唯一。

(2) 未經設定新通行碼前無法存取。

(3) 通過：(1)~(2)項任一結果符合。

(4) 不通過：(1)~(2)項皆不符合。

(5) 不適用：產品未支援通行碼鑑別機制。

5.1.1.2 隨機通行碼測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.1.2

(b) 測試資料：

無。

(c) 測試目的：

審閱通行碼生成機制之書面資料。

(d) 測試條件：

(1) 產品應支援通行碼鑑別機制，否則此測項不適用。

(2) 產品之用戶帳號及相關鑑別因子(如通行碼)已經建立。

(3) 產品應提供通行碼生成機制之設計說明。

(4) 產品應支援預設通行碼。

(e) 測試佈局：

如圖 3。

圖 3 測試示意圖

(f) 測試方法：

審閱通行碼生成機制之書面資料。

(g) 測試結果：

(1) 書面資料證實產品產生通行碼機制符合現行區域市場規範之偽隨機數產生器(PRNG)，且偽隨機數產生器(PRNG)符合 NIST 800-90 之規範。例如：歐盟 AIS-20/31。

(2) 產品所使用的產生通行碼機制使用偽隨機數產生器(PRNG)以上規格之隨機通行碼生成機制，例如：PUF(Physical Un-clonable Function)技術。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：產品不支援預設通行碼。

5.1.2 鑑別機制測試

5.1.2.1 變更或重設產品身分認證因子測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.2.1

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否具備身分認證機制且身分認證因子可變更或重設。

(d) 測試條件：

(1) 應提供可與產品相連之雲端平台。

(2) 應提供包含身分認證因子機制之產品使用手冊等書面資料。

(e) 測試佈局：

如圖 4。

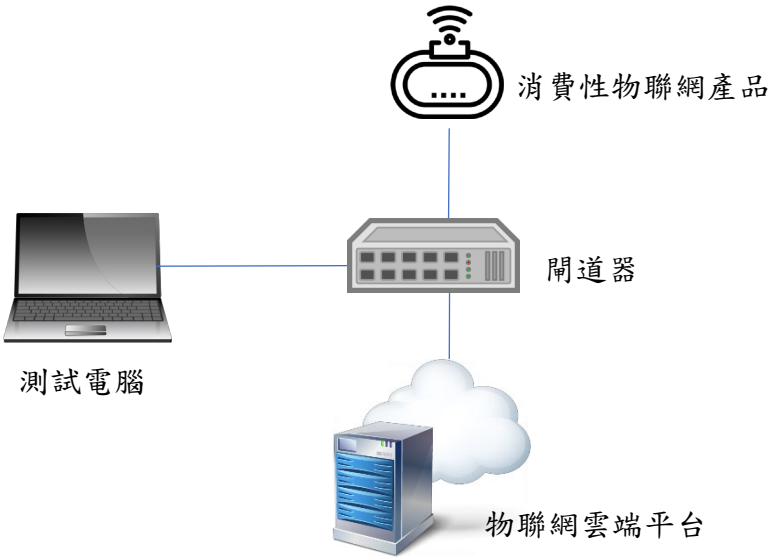

圖 4 測試示意圖

(f) 測試方法：

(1) 審閱具備身分認證程序說明之書面資料。

(2) 將產品與物聯網雲端平台對連。

(3) 更改身分認證因子，例如:將使用者帳號密碼更改成指紋辨識等。

(4) 重新與物聯網雲端平台建立連線，檢視是否可登入平台。

(5) 重設身分認證因子，例如:重設使用者密碼、重設指紋等。

(6) 重複步驟(4)。

(g) 測試結果：

(1) 產品支援身分認證機制。

(2) 產品提供之身份認證因子機制使用說明足以幫助使用者設置。

(3) 產品可正確以變更、重設的身分認證因子連線至物聯網雲端平台。

(4) 通過：(1)~(2)二項結果符合。

(5) 不通過：(1)~(2)二項結果不符合。

(6) 不適用：產品不支援身分認證機制。

5.1.2.2 通行碼的輸入頻率及次數限制測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.2.2

(b) 測試資料：

產品之安全通道的憑證。

(c) 測試目的：

驗證通行碼鑑別機制是否有防止暴力破解能力。

(d) 測試條件：

(1) 產品應為非受限制設備。

(2) 產品須支援通行碼鑑別機制。

(3) 產品之使用者帳號及相關鑑別因子(如通行碼)已經建立。

(4) 產品須提供帳號鎖定機制之設計說明。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 將測試電腦與產品連結在同一個區域網路中。

(2) 根據產品使用說明，開啟相應之管理介面連接工具以執行身分鑑別。

(3) 不斷輸入錯誤且相異的通行碼。

(4) 檢視產品於帳號鎖定計數器重設為 0 前，連續登入失敗次數 5 次以內，是否會鎖定帳號。

(5) 帳號鎖定後，於鎖定期間內持續輸入相異且錯誤的通行碼，比對廠商宣告帳號鎖定時限內，檢視帳戶是否解除鎖定。

(6) 同一帳號任一次登入失敗後，於廠商宣告計數器重設時限內，重新輸入錯誤且相異的通行碼，檢視輸入失敗次數是否有重新計算。

(g) 測試結果：

(1) 輸入次數 5 次以上，會鎖定帳號。

(2) 於廠商宣告之帳號鎖定時限內，帳戶未解除鎖定。

(3) 於廠商宣告計數器重設時限內，失敗次數未重新計算。

(4) 通過：(1)~(3)三項結果符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：產品為受限制設備。

5.1.2.3 身分鑑別因子傳輸安全測試

實體介面之外的邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(一) 本地端管理介面：

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.2.3

(b) 測試資料：

產品之系統管理員帳密。

(c) 測試目的：

驗證本地端介面之身分鑑別因子於傳輸中是否加密。

(d) 測試條件：

(1) 產品應支援本地端管理介面。

(2) 廠商應提供傳輸加密演算法書面資料作為審查依據。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 於未登入的狀況下，存取身分鑑別頁面外之頁面，確認是否要求身分鑑別。

(3) 對產品使用安全掃描工具，比對掃描安全通道的加密演算法是否符合廠商提供審查文件。

(4) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(5) 根據產品使用說明，開啟本地端管理介面身分認證頁面。

(6) 檢視所側錄之封包是否採用安全通道。

(7) 以產品之系統管理員帳密登入，執行身分鑑別操作。

(8) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。

(9) 檢視身分驗證結果。

(g) 測試結果：

(1) 產品於本地端管理介面能正常執行身分鑑別機制。

(2) 產品身分鑑別因子傳輸加密須符合 NIST SP 800-140C 所核可同等或以上等級之加密演算法。

(3) 身分鑑別機制具備抵抗重送攻擊的能力。

(4) 通過: (1)~(3)三項結果皆符合。

(5) 不通過: (1)~(3)三項結果不符合其一。

(6) 不適用: 產品不支援本地端管理介面。

(二) 網路協定與 API 介面：

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.1.2.3

(b) 測試資料：

產品之系統管理員帳密。

(c) 測試目的：

驗證網路協定與 API 介面之身分鑑別因子於傳輸中是否加密。

(d) 測試條件：

(1) 產品應支援網路協定介面。

(2) 產品應支援 API 介面。

(3) 廠商應提供傳輸加密演算法書面資料作為審查依據。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 在未登入產品的狀態下，存取身分驗證頁面之外的使用者頁面，確認是否要求身分驗證。

(3) 對產品使用安全掃描工具，比對掃描安全通道的加密演算法是否符合廠商聲明文件。

(4) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(5) 根據產品使用說明，開啟使用者身分驗證頁面。

(6) 檢視所側錄之封包是否採用安全通道。

(7) 以產品之系統管理員帳密登入，執行身分驗證操作。

(8) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。

(9) 檢視身分驗證結果。

(g) 測試結果：

(1) 產品於網路協定介面能正常執行身分鑑別機制。

(2) 產品於 API 介面正面能正常執行身分鑑別機制。

(3) 身分鑑別機制具備抵抗重送攻擊的能力。

(4) 傳輸加密方式採用 NIST SP 800-140C 所核可之同等或以上等級的加密演算法。

(5) 通過: (1)~(4)四項結果皆符合。

(6) 不通過: (1)~(4)四項結果不符合其一。

(7) 不適用: 產品不支援網路協定介面。

(8) 不適用: 產品不支援 API 介面。

(三) 測試結果：

(a) 測試依據：通過: (一)~(二)二項結果皆符合。

(b) 不通過：(一)~(二)二項結果不符合其一。

(c) 不適用：(一)~(二)二項介面產品皆不支援。

5.2 漏洞安全測試

檢視消費性物聯網產品之漏洞安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.2.1 漏洞政策與安全設置測試

5.2.1.1 漏洞揭露政策宣告測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否具有漏洞揭露政策宣告。

(d) 測試條件：

(1) 廠商應提供漏洞揭露與改善措施政策文件。

(2) 產品應提供廠商之漏洞揭露與改善措施政策之連結。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供漏洞揭露與改善措施政策文件。

(2) 驗證產品漏洞揭露與改善措施政策頁面或連結。

(3) 核對該頁面內容及廠商提供之漏洞揭露與改善措施政策文件。

(g) 測試結果：

(1) 廠商應提供產品之漏洞揭露與改善政策。

(2) 漏洞揭露與改善措施政策之內容應符合：

(i) 回報漏洞問題之連絡資訊。例如:廠商提供漏洞回報的專線或 eMail 信箱於使用說明書中。

(ii) 接收漏洞問題的初始確認程序。例如:漏洞揭露政策中訂定收到漏洞後多久時間內須完成問題確認。

(iii) 問題處理至問題解決之各階段的狀態更新。例如:廠商可透過與漏洞賞金平台合作，運用平台的漏洞回報與處理流程機制。

(3) 通過：(1)~(2)二項結果符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.2.1.2 漏洞處理計畫測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.2

(b) 測試資料：

無。

(c) 測試目的：

查驗廠商是否具備處理產品已揭露漏洞之漏洞修正計畫。

(d) 測試條件：

廠商應提供處理產品之漏洞修正計畫相關書面文件，例如:包括但不限於產品計畫書、產品程序書。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供漏洞修正計畫之書面文件。

(g) 測試結果：

(1) 書面文件之漏洞修正計畫應包括但不限於產品漏洞風險等級定義、各風險等級所對應之漏洞處理時間。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.1.3 漏洞監控、識別與修正測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.3

(b) 測試資料：

無。

(c) 測試目的：

驗證產品漏洞揭露政策宣告是否包含維護期間的安全漏洞監控、識別和修正聲明。

(d) 測試條件：

(1) 廠商應提供漏洞揭露與改善措施政策文件。

(2) 產品應提供廠商之漏洞揭露與改善措施政策之連結。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供漏洞揭露與改善措施政策文件。

(2) 驗證產品漏洞揭露與改善措施政策頁面或連結。

(3) 核對該頁面內容及廠商提供之漏洞揭露與改善措施政策文件。

(g) 測試結果：

(1) 漏洞揭露政策聲明之內容應包括維護期間內對其產品之安全漏洞持續監控、識別與修正。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.1.4 安全性設置測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.4

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否提供使用者以簡易方式完成產品最佳安全設置。

(d) 測試條件：

(1) 廠商應提供產品安裝及使用說明文件。

(2) 產品應提供安全性設置功能。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供的產品安裝及使用說明文件。

(2) 驗證產品的安全性設置功能，依產品安全性設置程序完成安全設定。

(g) 測試結果：

(1) 產品應有簡易安全性設置程序(例如:設定精靈)協助使用者設定，各設定步驟中應有最佳安全建議及具安全性的預設設定參數的選項，且該選項應以顯目提示方式呈現。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.1.5 安全設置指南測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.5

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否具有產品設置安全指南。

(d) 測試條件：

廠商應提供產品設置安全指南之使用手冊或網頁連結作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱產品設置安全指南之使用手冊或網頁連結。

(2) 使用手冊應含安全指南說明，包括但不限於：

(i) 產品安全功能的涵蓋範圍。

(ii) 設置安全的使用環境(例如:網路安全設定)。

(iii) 安全功能的設置(例如:安裝、身分驗證、授權、加密、更新等)。

(iv) 刪除儲存於產品的資料或檔案。

(v) 警示與通知。

(g) 測試結果：

(1) 產品應有產品安全設置指南。

(2) 產品安全設置指南應針對每項與安全性相關的設定選項，描述其如何實現最佳安全安全設置的說明與建議。

(3) 通過：(1)~(2)二項結果符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.2.1.6 安全設置檢驗測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.1.6

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否提供有關如何檢查安全設置是否已完成安全設置的方法。

(d) 測試條件：

廠商應提供產品設置安全指南之使用手冊或網頁連結作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱產品設置安全指南之使用手冊或網頁連結。

(2) 檢視使用手冊應。

(g) 測試結果：

(1) 產品應有產品安全設置指南。

(2) 產品安全設置指南應有對於如何檢查產品安全設置是否已完成安全設置的方法說明。

(3) 通過：(1)~(2)二項結果符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.2.2 最小暴露攻擊面測試

5.2.2.1 網路服務最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.1

(b) 測試資料：

產品之 IP 位址。

(c) 測試目的：

驗證產品是否存在預期以外之網路埠。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供所啟用之網路服務與對應埠之宣告。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 啟動具網路埠掃描功能之工具。

(3) 對產品執行 TCP 埠 0~65535 之掃描。

(4) 檢視掃描結果所呈現之網路服務與對應埠。

(5) 對產品執行 UDP 埠 0~65535 之掃描。

(6) 檢視掃描結果所呈現之網路服務與對應埠。

(h) 測試結果：

(1) 產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

(2) 產品未開啟自我宣告以外之網路服務。

(3) 產品無法從未宣告的網路服務開啟登入介面。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：產品無網路服務之功能。

5.2.2.2 初始狀態網路服務最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.2

(b) 測試資料：

產品之 IP 位址。

(c) 測試目的：

驗證產品在初始狀態下網路服務公開與安全性相關的資訊是否為服務必要之所需。

(d) 測試條件：

(1) 產品應保持出廠狀態。

(2) 產品應提供所啟用之網路服務與對應埠之宣告。

(3) 產品應提供網路傳輸所需公開安全性資訊之說明文件。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供的產品自我宣告。

(2) 設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(3) 根據產品說明文件，於產品初始狀態開啟網路服務。

(4) 檢視側錄到的封包。

(g) 測試結果：

(1) 產品所開啟之網路服務與對應埠，與產品自我宣告之「網路服務」、「通訊埠」、「連結伺服器之 IP/DN/公司主機名稱」及「資料內容」相符。

(2) 產品未公開自我宣告以外之安全性資訊。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品無網路服務之功能。

5.2.2.3 實體介面最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.3

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否存在預期以外之實體介面。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應於文件中列出啟用的實體介面，並說明其功用、使用情境與其必要性。

(3) 廠商至少提供二件受測產品。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 審閱啟用之實體介面的說明文件。

(2) 使用檢測工具探查產品可能使用之實體介面。

(3) 檢視探查結果。

(g) 測試結果：

(1) 產品所開啟之實體介面與產品說明文件相符。

(2) 產品不存在說明文件以外的實體介面。

(3) 說明文件以外之實體介面預設關閉。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果皆不符合。

(6) 不適用：無。

5.2.2.4 除錯模式測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.4

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否透過實體介面存取作業系統之除錯模式。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應於文件中說明進入作業系統除錯模式之方法。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 根據文件所述連接相應之實體介面。

(2) 測試電腦連接產品之 USB 埠，並開啟相應之管理介面連接工具。

(3) 透過 USB 埠存取作業系統之除錯模式。

(4) 測試電腦連接產品之 UART 埠，並開啟相應之管理介面連接工具。

(5) 透過 UART 埠存取作業系統之除錯模式。

(6) 測試電腦連接產品之 JTAG 埠，並開啟相應之管理介面連接工具。

(7) 透過 JTAG 埠存取作業系統之除錯模式。

(g) 測試結果：

(1) 產品不存在進入作業系統除錯模式之介面。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.2.5 軟體服務最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.5

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否存在預期以外之軟體服務。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應於文件中列出啟用的軟體服務並說明其功用、使用方式與其必要性。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 審閱啟用之軟體服務的說明文件。

(2) 開啟產品各軟體服務。

(3) 比對產品軟體服務與說明文件內容。

(g) 測試結果：

(1) 產品所啟用之軟體服務與產品說明文件相符。

(2) 產品不存在說明文件以外的軟體服務。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：無。

5.2.2.6 程式碼最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.6

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否存在預期以外之程式碼。

(d) 測試條件：

(1) 廠商應提供產品原始碼檔案，版本應與產品送驗相同。

(2) 廠商應提出已完成產品的程式碼優化及完成死碼消除(Dead code elimination)之證明與使用工具。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供之程式最小化的證明文件。

(2) 使用檢測工具檢驗產品程式碼。

(g) 測試結果：

(1) 產品符合程式最小化，已確實移除程式碼中非產品功能或服務所需的程式，例如:不必要的字符、註解或註銷的程式片段等。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2.2.7 權限控制機制

(一) 本地端管理介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.7

(b) 測試資料：

(1) 產品之系統管理者帳號密碼。

(2) 產品之其他權限使用者帳號密碼。

(c) 測試目的：

驗證產品資源的存取是否具有權限控制機制。

(d) 測試條件：

(1) 產品應具備權限控制機制。

(2) 產品應提供角色權限設定說明文件。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 審閱產品使用者角色權限說明文件。

(2) 將測試電腦連接產品。

(3) 開啟本地端管理介面。

(4) 以其他權限之使用者帳密登入。

(5) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(6) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(7) 進行登出，並以系統管理者帳密登入。

(8) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(9) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(g) 測試結果：

(1) 各角色操作權限應僅限該角色所設定之角色任務之所需。

(2) 於本地端管理介面的身分授權與產品自我宣告相符.

(3) 產品宜具備多個不同權限角色之功能，若此功能會對營運產生不利影響，產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項任一結果不符合。

(6) 不適用：產品不支援本地端管理介面。

(二) 網路協定與 API 介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.7

(b) 測試資料：

(1) 產品之系統管理者帳號密碼。

(2) 產品之其他權限使用者帳號密碼。

(c) 測試目的：

驗證產品資源的存取是否具有權限控管機制。

(d) 測試條件：

(1) 產品應具備權限控制機制。

(2) 產品應提供角色權限設定說明文件。

(3) 產品應支援網路協定介面。

(4) 產品應支援 API 介面。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 審閱產品使用者角色權限說明文件。

(2) 將測試電腦連接產品。

(3) 根據產品使用說明，開啟網路協定介面。

(4) 以一般使用者帳密登入。

(5) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(6) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(7) 以一般系統管理者帳密登入。

(8) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(9) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(10) 根據產品使用說明，開啟所支援的 API 介面。

(11) 以一般使用者帳密登入。

(12) 存取產品功能頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(13) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(14) 以一般系統管理者帳密登入。

(15) 存取產品功能頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(16) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(g) 測試結果：

(1) 各角色操作權限應僅限該角色所設定之角色任務之所需。

(2) 於網路協定介面的身分授權與產品自我宣告相符。

(3) 於 API 介面的身分授權與產品自我宣告相符。

(4) 產品應具備多個不同權限角色之功能，若此功能會對營運產生不利影響，產品之宣告應提出相關之說明，則產品可具備單一權限角色即可。

(5) 通過：(1)~(3)三項結果皆符合。

(6) 不通過：(1)~(3)三項任一結果不符合。

(7) 不適用：產品不支援網路協定介面及/或不支援 API 介面。

(三) 雲端管理介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.7

(b) 測試資料：

(1) 網雲端平台 ip 位址。

(2) 產品之系統管理員帳號密碼。

(3) 產品之其他權限使用者帳號密碼。

(c) 測試目的：

驗證產品是否具有權限控管機制。

(d) 測試條件：

(1) 備權限控制機制。

(2) 產品應提供角色權限設定說明文件。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(3) 使用者角色權限說明文件。

(4) 將測試電腦連接產品物聯網雲端平台。

(5) 開啟雲端管理介面。

(6) 以一般使用者帳密登入。

(7) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(8) 嘗試存取系統管理者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(9) 進行登出，並以系統管理者帳密登入。

(10) 存取產品資源，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符。

(11) 嘗試存取一般使用者頁面，檢視該帳號之身分類型與其對應之權限是否與產品自我宣告相符

(g) 測試結果：

(1) 作權限應僅限該角色所設定之角色任務之所需。

(2) 於雲端管理介面的身分授權與產品自我宣告相符。

(3) 於雲端管理介面的身分授權與產品自我宣告不相符，或產品無支援創建多個不同權限使用者之功能。

(4) 通過：(1)~(2)二項結果皆符合。

(5) 不通過：(1)~(2)項結果不符合其一。

(6) 不適用：產品不支援雲端管理介面。

(四) 測試結果：

(a) 通過：(一)~(三)三項結果皆符合。

(b) 不通過：(一)~(三)三項結果不符合其一。

(c) 不適用：(一)~(三)項之介面產品皆不支援。

5.2.2.8 記憶體存取控制測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.8

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否為硬體等級的存取控制機制。

(d) 測試條件：

廠商應提供所使用記憶體存取控制機制之說明文件，例如: Memory Management Unit (MMU)、Memory Protection Unit (MPU)等技術。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供產品使用之記憶體控制機制之書面資料。

(g) 測試結果：

(1) 書面資料證實產品使用硬體等級之記憶體存取控制機制進行空間保護，例如:MMU、MPU 技術。

(2) 通過：(1)項結果皆符合。

(3) 不通過：(1)項結果皆不符合。

(4) 不適用：無。

5.2.2.9 安全開發驗證測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.2.2.9

(b) 測試資料：

無。

(c) 測試目的：

查驗產品開發流程是否符合安全開發要求。

(d) 測試條件：

廠商應提供相關說明文件(見附錄 C 所述)作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱具備此功能證明之書面資料。

(g) 測試結果：

(1) 書面資料證實產品符合安全開發之規定。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.3 軟韌體更新測試

檢視消費性物聯網產品之軟韌體更新安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。安全測試項目 5.3.3~5.3.12 須根據 5.3.1 或 5.3.2 所規範之更新機制執行測試。

5.3.1 更新安全測試

5.3.1.1 更新功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品的所有軟體組件支援安全更新功能。

(d) 測試條件：

(1) 廠商應提供更新機制說明文件。

(2) 產品應支援更新功能，包括但不限於線上更新或手動更新方式。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供之安全更新機制說明文件，內容包括但不限於：

(i) 更新方式。

(ii) 支援更新之軟體組件。

(iii) 不支援更新之軟體組件，並說明不支援更新的原因。

(2) 啟動更新。

(3) 查驗產品更新結果。

(g) 測試結果：

(1) 安全更新功能與說明文件相符。

(2) 不支援更新之軟體組件不影響產品安全性。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.3.1.2 安全更新測試

(一) 防止降版安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否可降為較舊之系統版本。

(d) 測試條件：

(1) 若產品支援線上更新，須由廠商負責觸發線上更新。

(2) 產品應為非受限制設備。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

使用舊軟韌體版本執行更新安裝。

(g) 測試結果：

(3) 軟韌體更新失敗。

(4) 通過：(1)項結果符合。

(5) 不通過：(1)項結果不符合。

(6) 不適用：產品為受限制設備。

(二) 軟韌體更新路徑

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證產品的韌體線上更新是否採用安全通道。

(d) 測試條件：

(1) 產品須支援線上更新。

(2) 廠商應提出採用安全更新機制作法之說明文件。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供之安全更新機制說明文件是否足以證明更新採取安全通道傳輸。

(g) 測試結果：

(1) 廠商提供之安全更新機制說明文件證實產品之線上更新路徑通過安全通道，且安全通道所使用之密碼演算法須符合 NIST SP 800-140C 同等或以上等級。

(2) 通過：(1)項結果皆符合。

(3) 不通過：(1)項任一結果不符合。

(4) 不適用：無。

(三) 測試結果：

(a) 通過：(一)~(二)二項結果符合其一。

(b) 不通過：(一)~(二)二項結果皆不符合。

(c) 不適用：產品為受限制設備。

5.3.1.3 更新方式測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.3

(b) 測試資料：

無。

(c) 測試目的：

驗證產品之安全更新機制是否滿足簡單易用之更新方式。

(d) 測試條件：

(1) 產品應具備更新機制。

(2) 廠商應提供軟韌體更新方法之產品使用說明書。

(3) 若產品支援自動更新，受測廠商應協助觸發產品之線上更新。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 閱審廠商提供之軟韌體更新說明文件。

(2) 根據軟韌體更新說明文件之方式，啟動軟韌體更新。

(3) 檢視產品更新過程。

(4) 確認產品更新結果。

(g) 測試結果：

(1) 產品軟韌體更新方式符合簡單步驟原則，且產品使用說明書清楚描述使用操作步驟。簡單更新方式，例如: 包括但不限於自動更新軟韌體、透過關聯服務啟動更新、透過產品之 web 介面啟動更新等方式。

(2) 產品完成軟韌體更新。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援更新機制。

5.3.1.4 自動更新測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.4

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否具備自動軟體更新機制。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 廠商應提供產品自動更新設計說明文件與產品使用說明書。

(3) 受測廠商應協助觸發產品之線上更新。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供之自動更新相關說明文件。

(2) 觸發產品自動更新，比對說明文件之自動更新方式。

(g) 測試結果：

(1) 產品之自動更新機制符合使用者不需要自行操作更新功能。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援更新機制。

5.3.1.5 檢查可用更新測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.5

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否具有於產品初始後自動定期檢查可用更新之功能。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 產品應保持出廠預設狀態。

(3) 廠商應提供產品更新機制設計說明文件與產品使用說明書。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供之更新機制相關說明文件，包括但不限於功能：產品初始化後自動檢查可用更新、觸發產品本身檢查可用更新功能、產品定期自動檢查可用更新。

(2) 產品初始化，驗證產品是否自動觸發可用軟韌體更新檢查。

(3) 驗證觸發產品可用軟韌體更新檢查。

(4) 驗證產品是否有定期檢查可用軟韌體更新之功能。

(g) 測試結果：

(1) 更新機制說明文件證實產品具備可用更新檢查功能，包括但不限於：產品初始化後自動檢查可用更新、觸發產品本身檢查可用更新功能、產品定期自動檢查可用更新。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援更新機制。

5.3.1.6 自動更新通知測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.6

(b) 測試資料：

無。

(c) 測試目的：

驗證產品具有自動更新與自動更新通知功能，且使用者可設定開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲更知的功能選項。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 產品應支援自動更新及/或更新通知。

(3) 產品應保持出廠預設狀態。

(4) 受測廠商應協助觸發產品之線上更新。

(5) 廠商應提供產品更新機制設計說明文件與產品使用說明書。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供之更新機制相關說明文件，自動更新與更新通知功能內容包括但不限於：開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲更知的設定選項。

(2) 根據說明文件觸發產品更新，驗證產品自動更新與更新通知之開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲更知的設定選項。

(g) 測試結果：

(1) 更新機制說明文件證實產品具備自動更新與更新通知設定功能，包括但不限於：開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲更知的設定選項。

(2) 產品之自動更新與更新通知功能應可正確設定開啟更新、關閉更新、延遲更新、開啟通知、關閉通知及延遲更知之選項。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援更新機制。

(6) 不適用：產品不支援自動更新、更新通知功能。

5.3.1.7 韌體更新路徑的保護

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.7

(b) 測試資料：

測試用假憑證。

(c) 測試目的：

驗證產品的韌體線上更新是否採用安全通道，以確保韌體之機密性、正確性及完整性，同時是否具有鑑別安全通道所使用憑證之合法性及有效性。

(d) 測試條件：

(1) 產品應支援更新機制。
(2) 產品應提供所有相連更新伺服器之宣告。
(3) 受測廠商應協助觸發產品之線上更新。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 將測試電腦、產品與更新伺服器連結在同一個區域網路中。
(2) 啟動韌體更新。
(3) 使用工具側錄更新伺服器與產品之間的封包。
(4) 檢視所側錄之封包。
(5) 再次啟動更新。
(6) 於更新伺服器發送憑證予產品之間，攔截更新伺服器憑證。
(7) 置換憑證公鑰或憑證資訊，包括發證單位、有效期限、格式錯誤及憑證簽章。
(8) 發送已竄改之憑證予產品。
(9) 於安全通道建立的交握過程中監聽封包。
(10) 檢視所側錄之封包。

(g) 測試結果：

(1) 產品之線上更新路徑通過安全通道，且安全通道須支援「附錄 A」中所建議之密碼套件，安全更新機制應採用 NIST SP 800-140C 所核可之同等或以上等級密碼演算法。

(2) 更新伺服器之憑證公鑰或憑證資訊其一被竄改，安全通道建立失敗。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一或不支援線上更新功能。

(5) 不適用：產品不支援更新機制。

5.3.1.8 安全更新部署

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.8

(b) 測試資料：

無。

(c) 測試目的：

驗證產品的即時安全更新政策與部署。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 廠商應提供更新機制說明文件。

(3) 廠商應提供漏洞處理與即時更新政策宣告，及流程管理與部署證明。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供之安全更新機制說明文件與即時更新的漏洞處理政策。

(g) 測試結果：

(1) 產品有制定漏洞處理與安全更新之程序，且該程序須已達到 5.2.1.2 之即時漏洞處理期限和有效及時部署產品安全更新。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援更新機制。

5.3.1.9 更新檔案安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.9

(b) 測試資料：

無。

(c) 測試目的：

驗證產品安裝更新檔是否採用簽章驗證機制，以確保更新檔案之真實性與完整性。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 廠商應提供韌體簽章加密程序說明文件，及所使用之簽章演算法資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 使用具二進制檔案字串搜尋功能之工具，查找是否具有關鍵安全參數。

(2) 使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(3) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(4) 審閱可證明所使用加密演算法之書面資料。

(5) 確認關鍵安全參數的保密機制是否採用 NIST SP 800-140C 所核可之加密演算法。

(6) 確認金鑰是否可被擷取。

(7) 確認是否存在產品所宣告之相連伺服器外之 IP 資料。

(8) 確認是否存在產品所宣告之相連伺服器外之 URL 資料。

(g) 測試結果：

(1) 產品確認韌體更新檔之簽章加密機制採用 NIST SP 800-140C 所核可之同等或以上強度的簽章演算法。

(2) 產品之更新來源應與廠商自我宣告中所宣告之「資料連結伺服器之 IP/DN/公司主機名稱」相符。

(3) 通過：(1)項結果符合。

(4) 不通過：(1)項結果不符合。

(5) 不適用：產品不支援更新機制。

5.3.1.10 更新伺服器信任關係驗證

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.10

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否對更新伺服器鑑別身分之真實性，以確保更新傳輸過程中之真實性與完整性。

(d) 測試條件：

(1) 產品應支援線上更新。

(2) 產品應支援更新機制。

(3) 廠商應提供產品與更新伺服器之間如何建立信任關係之作法說明作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱廠商提供的與更新伺服器建立信任關係作法之書面資料。

(2) 根據廠商提供之書面資料驗證產品與更新伺服器間的網路傳輸。

(g) 測試結果：

(1) 廠商提供之佐證資符合產品與伺服器間建立有效的安全信任關係，有效的信關係包括但不限於：

(i) 更新透過安全通道，安全通道之加密演算法須採用 NIST SP 800-140C 所核可之同等或以上強度的加密演算法。

(ii) 更新透過簽章認證方式，簽章須採用 NIST SP 800-140C 所核可之同等或以上強度的簽章演算法。

(iii) 產品在建立網路連線時須透過關鍵安全參數或密碼，密碼須採用 NIST SP 800-140C 所核可之同等或以上強度的密碼演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援線上更新機制。

5.3.1.11 更新通知與資訊測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.11

(b) 測試資料：

無。

(c) 測試目的：

驗證產品之更新通知是否有清楚說明更新資訊。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 廠商應提供產品更新功能說明文件。

(3) 廠商應協助觸發產品更新。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 廠商觸發軟韌體更新。

(2) 檢視產品更新功能。

(g) 測試結果：

(1) 產品之更新通知方式包括但不於：於產品本地端管理介面使用彈跳視窗、推播訊息，及寄送電子郵件。

(2) 更新通知內容應包括但不限於：更新版本、該次更新所能緩解的風險、修正的 bug。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援更新機制。

5.3.1.12 更新警語測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.12

(b) 測試資料：

無。

(c) 測試目的：

查驗產品於進入更新程序前是否有提示警語。

(d) 測試條件：

(1) 產品應支援更新機制。

(2) 廠商應提供產品更新功能說明文件或產品使用手冊。

(3) 廠商應協助觸發產品更新。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商提供之更新說明文件中的更新警語功能。

(2) 廠商觸發軟韌體更新。

(3) 檢視產品在進入更新程序前是否有警示。

(g) 測試結果：

(1) 更新警語功能證實與廠商提供之說明文件相符，更新警語之內容，包括但不限於：什麼情況下中斷功能或哪些情況下不會完全關閉、預計更新持續多少時間、更新期間可能中斷連線的時間等。

(2) 產品在更新程序開始前，產品本地端管理介面應顯示更新警語提示。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援更新機制。

5.3.1.13 支援更新期限測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.13

(b) 測試資料：

無。

(c) 測試目的：

查驗產品具有產品支援期限之聲明宣告。

(d) 測試條件：

(1) 廠商應提供產品支援期限之聲明文件作為審查依據，包括但不限於產品網路、使用手冊、包裝等公告方式。

(e) 測試佈局：

無。

(f) 測試方法：

查驗廠商所提供之產品支援聲明文件或網頁連結。

(g) 測試結果：

(1) 產品支援期限與廠商提供之聲明文件相符，且聲明描述應淺顯易懂。

(2) 產品支援期限聲明公告於，包括但不限於產品官網、產品使用手冊、產品包裝等處，公告產品支援期限。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.3.1.14 受限制設備更新說明

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.14

(b) 測試資料：

無。

(c) 測試目的：

查驗軟體組件無法更新之受限制設備產品是否提供無法更新的理由或更新替代方法。

(d) 測試條件：

(1) 產品為軟體組件無法更新之受限制設備。

(2) 廠商應提供產品之更新替代方案之宣告，以作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

查驗廠商所提供之無法軟體更新之宣告。

(g) 測試結果：

(1) 產品無法軟體更新或支援硬體替換之宣告方式，包括但不限於公告於產品官網、產品使用手冊、產品包裝等處。

(2) 產品應以淺顯易懂的敘述說明無法軟體更新之理由；若產品支援硬體替換方式代替軟體更新，應宣告支援期限與替換方法。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品為非受限制設備。

5.3.1.15 受限制設備更新替代方法

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.15

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否可被隔離且可替換硬體。

(d) 測試條件：

(1) 產品為軟體組件無法更新之受限制設備。

(2) 廠商應提供產品硬體替換方案之設計說明資料，以作為審查依據。例如:產品使用手冊等。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱廠商所提供產品更新替代方案之說明文件。

(2) 依據廠商提供之說明文件，驗證產品是否可被隔離。

(3) 依據廠商提供之說明文件，驗證產品可替換硬體。

(g) 測試結果：

(1) 產品之更新替代方案應符合可被隔離的設計，例如：若產品之無法更新的組件被中止網路連線，系統仍保持正常運作。

(2) 使用者可可根據說明文件之描述替換產品硬體。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品非受限制設備。

5.3.1.16 產品標示測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.3.1.16

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否載明產品型號及產品名稱於使用者易於辨識之處。

(d) 測試條件：

廠商應提供產品產品概述說明表(如附錄 B)作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

查驗產品型號及名稱標示。

(g) 測試結果：

(1) 產品型號及名稱應標示在包括但不限於產品標籤或實體介面，且應讓使用者清楚辨識。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4 資料機密性與完整性測試

檢視消費性物聯網產品之資料機密性與完整性安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.4.1 安全敏感性資料儲存測試

5.4.1.1 安全敏感性資料加密儲存測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.1.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品持久性儲存器之敏感性安全參數是否加密儲存或存放安全區域。

(d) 測試條件：

(1) 廠商應提供持久性儲存器中的敏感性安全參數之保存方式之書面資料作為審查依據。

(2) 廠商應聲明使用的安全儲存技術之書面資料作為審查依據，包括但不限於加密儲存、儲存於安全區域。

(e) 測試佈局：

無。

(f) 測試方法：

審閱具備能證明敏感性安全參數能安全儲存於持久性儲存器之證明文件。

(g) 測試結果：

(1) 書面資料證實產品之敏感性安全參數已加密儲存。

(2) 書面資料證實產品之敏感性安全參數存放於安全區域。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：無。

5.4.1.2 硬編碼測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證產品之唯一識別碼是否以硬編碼方式儲存。

(d) 測試條件：

(1) 產品應支援產品識別碼硬編碼唯一性。

(2) 產品應提供保護產品唯一識別碼硬編碼儲存遭篡改之安全設計書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱符合保護產品以硬編碼儲存唯一識別碼之安全設計之書面資料。

(2) 防止產品唯一識別碼硬編碼儲存遭篡改之安全設計。

(g) 測試結果：

(1) 書面資料證實產品以安全晶片方式將產品唯一識別碼硬編碼加密儲存。

(2) 書面資料證實產品將唯一識別碼以雜湊演算法及簽章方式確保防止被篡改。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：產品不支援產品識別碼硬編碼唯一性。

5.4.1.3 韌體安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.1.3

(b) 測試資料：

產品之韌體檔案。

(c) 測試目的：

查驗產品之韌體程式碼不存在之關鍵安全參數。

(d) 測試條件：

(1) 廠商應提供產品之韌體檔案。

(2) 產品應提供所使用之加密演算法書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱可證明所使用加密演算法之書面資料。

(2) 由產品官網下載韌體或廠商提供產品之韌體，使用具韌體拆解功能之工具，對產品之韌體進行拆解。

(3) 檢視該韌體更新檔是否可被解析出檔案系統目錄。

(4) 確認是否有關鍵安全參數可被擷取。

(g) 測試結果：

(1) 韌體無法解析出關鍵安全參數。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4.1.4 關鍵安全參數唯一性測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.1.4

(b) 測試資料：

無。

(c) 測試目的：

驗證產品於更新及與關聯服務間傳輸所使用的關鍵安全參數是否具唯一性。

(d) 測試條件：

(1) 廠商應聲明所使用之關鍵安全參數為何之書面資料作為審查依據。

(2) 廠商應提供具唯一性的關鍵安全參數生成機制之書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱具備能證明關鍵安全參數具唯一性的生成機制證明文件。

(g) 測試結果：

(1) 書面資料證實產品用於更新及與關聯服務間傳輸所使用的關鍵安全參數具唯一性。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4.2 傳輸資料保護測試

5.4.2.1 資料傳輸保護測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品資料之傳輸是否採用符合國際標準要求或公認之資安產業慣例最佳傳輸加密技術。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 廠商應提供所使用傳輸加密技術書面資料作為審查依據。

(3) 產品應提供物聯網雲端平台。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 將產品與物聯網雲端平台連線，同時側錄封包。

(3) 檢視所側錄之封包是否採用安全通道。

(4) 比對掃描結果是否與廠商提供之加密技術相符。

(g) 測試結果：

(1) 產品與物聯網雲端平台之資料傳輸，採用符合國際標準要求或公認之資安產業慣例最佳傳加密技術。例如：安全通道使用 TLS v1.2 以上版本、採用

NIST SP 800-140C 所核可的同等或以上等級之密碼演算法、IPSec、MPLS 等。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4.2.2 安全開發驗證測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.2

(b) 測試資料：

無。

(c) 測試目的：

查驗產品之網路與安全功能在上線/出廠前是否通過審查(review)或評估(evaluate)。

(d) 測試條件：

廠商應提供產品的網路和安全功能已通過審查或評估的佐證資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供之證明書面資料。

(g) 測試結果：

(1) 書面資料證實產品確實於上線/出廠前已通過審查或評估。

(i) 審查之內容包括但不限於，廠商已識別之資安缺陷及漏洞修補結果。

(ii) 評估內容包括但不限於，供應商所識別的必要安全措施及緩解措施。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4.2.3 密碼演算法期限

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.3

(b) 測試資料：

無。

(c) 測試目的：

查驗產品建議的使用年限是否不起過所使用之密碼演算法及密碼基元(cryptographic primitives)的建議使用期限。

(d) 測試條件：

廠商應提供產品的密碼演算法及密碼基元更新說明文件或產品與密碼演算法/密碼基元建議使用年限之書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供之產品使用密碼演算法及密碼基元書面資料。

(1) 非受限制設備產品：書面資料內容包括但不限於

(i) 使用的密碼演算法及密碼基元。

(ii) 密碼演算法及密碼基元的更新計畫與方法。

(2) 受限制設備產品：書面資料容包括但不限於

(i) 使用的密碼演算法及密碼基元。

(ii) 產品建議使用期限與密碼演算法及密碼基元的建議使用期限。

(g) 測試結果：

(1) 非受限制設備產品：書面資料證實產品所使用的密碼演算法及密碼基元可被更新。

(2) 受限制設備產品：書面資料證實產品的建議使用期限不超過密碼演算法建議使用期限。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：無。

5.4.2.4 身分鑑別機制測試

實體介面之外的邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(一) 本地端管理介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.4

(b) 測試資料：

產品之系統管理員帳密。

(c) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(d) 測試條件：

產品應支援本地端管理介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 於未登入的狀況下，存取身分鑑別頁面外之頁面，確認是否要求身分鑑別。

(3) 根據產品使用說明，開啟本地端管理介面。

(4) 以產品之系統管理員帳密登入，執行身分鑑別操作。

(5) 檢視鑑別結果。

(g) 測試結果：

(1) 產品於本地端管理介面能正常執行身分鑑別機制。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 通過: (1)~(2)二項結果皆符合。

(4) 不通過: (1)~(2)二項結果不符合其一。

(5) 不適用: 產品不支援本地端管理介面。

(二) 網路協定與 API 介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.4

(b) 測試資料：

產品之系統管理員帳密。

(c) 測試目的：

驗證產品是否具備可靠之身分鑑別機制。

(d) 測試條件：

(1) 產品應支援網路協定介面。

(2) 產品應支援 API 介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品使用說明，開啟所支援網路協定介面。

(3) 以產品之系統管理員帳密登入，執行身分鑑別操作。

(4) 檢視鑑別結果。

(5) 根據產品使用說明，開啟所支援 API 介面。

(6) 以產品之 API 驗證連接方式，執行身分鑑別操作。

(7) 檢視鑑別結果。

(g) 測試結果：

(1) 產品於網路協定介面能正常執行身分鑑別機制。

(2) 產品於 API 介面正面能正常執行身分鑑別機制。

(3) 通過: (1)~(2)二項結果皆符合。

(4) 不通過: (1)~(2)二項結果不符合其一。

(5) 不適用: 產品不支援網路協定介面。

(6) 不適用: 產品不支援 API 介面。

(三) 實體介面

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.4

(b) 測試資料：

產品之系統管理員帳密。

(c) 測試目的：

查驗不可透過產品實體介面，直接存取產品之除錯模式。

(d) 測試條件：

(1) 產品應保持出廠預設組態。

(2) 產品應支援實體介面。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 檢查產品是否存在可進入除錯模式之介面。

(2) 若存在可控制除錯模式介面，則執行以下步驟。

(3) 根據文件所述連接相應之實體介面。

(4) 測試電腦連接產品之 UART 埠，並開啟相應之管理介面連接工具。

(5) 透過 UART 埠存取之除錯模式。

(6) 測試電腦連接產品之 JTAG 埠，並開啟相應之管理介面連接工具。

(7) 透過 JTAG 埠存取之除錯模式。

(8) 測試電腦連接產品之 USB 埠，並開啟相應之管理介面連接工具。

(9) 透過 USB 埠存取之除錯模式。

(g) 測試結果：

(1) 產品不存在進入除錯模式之介面。(根據 5.2.2.4 安全要求)

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援實體介面。

(四) 測試結果：

(a) 測試依據：通過：(一)~(三)三項結果皆符合。

(b) 不通過：(一)~(三)三項結果不符合其一。

(c) 不適用：(一)~(三)三項介面產品皆不支援。

5.4.2.5 安全設定測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.5

(b) 測試資料：

產品之系統管理者帳密。

(c) 測試目的：

驗證產品安全相關設定功能進行變更時是否具備身分驗證機制。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供本地端管理介面。

(3) 廠商應提供變更設定需進行身分驗證機制之產品功能說明文件作為審查依據。

(e) 測試佈局：

如圖 3。

(f) 測試方法：

(1) 審閱廠商提供之說明文件。

(2) 將測試電腦連接產品。

(3) 根據說明文件對產品安全相關功能進行變更，包括但不限於近登入本地端管理介面、實體介面執行通行碼變更或權限角變更。

(4) 檢視產品在開啟功能設定時，是否執行身分驗證機制。

(g) 測試結果：

(1) 產品於進行變更安全相關設定功能執行身分驗證機制與廠商宣告相符。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(h) 不適用：產品使用 ARP、DHCP、DNS、ICMP 和 NTP。

5.4.2.6 關鍵安全參數傳輸安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.6

(b) 測試資料：

產品之系統管理者帳密。

(c) 測試目的：

驗證產品之關鍵安全參數於傳輸中是否加密。

(d) 測試條件：

(1) 廠商應提出產品使用傳輸加密演算法書面資料作為審查依據。

(2) 廠商應提出所有關鍵安全參數傳輸的邏輯介面之書面資料，邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據廠商提供之書面資料，使用安全通道掃描工具。

(3) 於相應之邏輯介面輸入產品之系統管理者帳密，同時側錄封包。

(4) 比對側錄封包的結果。

(g) 測試結果：

(1) 與測試電腦之間的帳號密碼資訊傳輸，使用的加密技術採用 NIST SP 800-140C 所核可的同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.4.2.7 遠端指令介面安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.7

(b) 測試資料：

產品之系統管理者帳密。

(c) 測試目的：

驗證遠端指令介面之關鍵安全參數於傳輸中是否加密或使用安全通道。

(d) 測試條件：

(1) 廠商應提出產品使用傳輸加密演算法或安全通道書面資料作為審查依據。

(2) 產品應提供遠端指令介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 審閱廠商之書面資料，開啟相應之遠端指令介面。

(3) 對產品使用安全通道掃描工具。

(4) 於遠端指令介面輸入產品之系統管理者帳密，同時側錄封包。

(5) 檢視所側錄之封包。

(g) 測試結果：

(1) 遠端指令介面的帳號密碼資訊傳輸證實以加密方式傳輸。

(2) 遠端指令介面的帳號密碼資訊傳輸證實採用安全通道。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：產品不支援遠端指令介面。

5.4.2.8 關鍵安全參數安全管理測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.4.2.8

(b) 測試資料：

產品之系統管理者帳密。

(c) 測試目的：

驗證產品之關鍵安全參數是否遵循國際標準要求之安全管理程序。

(d) 測試條件：

廠商應提供產品關鍵安全參數及其安全管理程序之證明文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱關鍵安全參數與其安全管理程序之宣告文件。

(g) 測試結果：

(1) 關鍵安全參數與其安全管理程序之作法符合國際標準要求，例如：金鑰管理生命週期符合 NIST SP 800-57 之要求。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.5 系統完整性測試

檢視消費性物聯網產品之系統完整性安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.5.1 實體入侵防護測試

5.5.1.1 安全啟動功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.5.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證產品於開機階段是否能確保產品之完整性及可信度。

(d) 測試條件：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供安全啟動功能之設計文件。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱具備安全啟動功能證明之書面資料。

(2) 確認產品在開機過程中是否驗證韌體與作業系統的簽章。

(g) 測試結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 書面資料證實產品在開機過程中驗證韌體與作業系統的簽章。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.5.2 輸入驗證測試

5.5.2.1 輸入驗證功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.5.2.1

(b) 測試資料：

產品之 IP 位址。

(c) 測試目的：

驗證產品使用者介面是否有對使用者輸入的資料進行驗證。

(d) 測試條件：

產品支援使用者介面，包括但不限於本地端管理介面、網路服務介面、應用程式介面(APIs)。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦與產品連接。

(2) 開啟使用者介面。

(3) 使用模糊工具檢測。

(g) 測試結果：

(1) 無法登入使用者介面。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.6 資源可用性測試

檢視消費性物聯網產品之資源可用性安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.6.1 資源管理測試

5.6.1.1 備援功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.6.1.1

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否設置因應網路或電源中斷的彈性機制。

(d) 測試條件：

廠商應提供設置預防網路和電源中源的彈性機制書面文件作為審查依據。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 審閱預防網路和電源中斷彈性機制書面文件。

(2) 中斷網路，檢視產品運作情況。

(3) 中斷電源，檢視產品運作情況。

(g) 測試結果：

(1) 產品運作情況與產品自我宣告相符，彈性機制包括但不限於:設置備用電源、資料即時備份。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.6.1.2 網路中斷測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.6.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證當網路異常中斷時是否可保持本地端運作，且在網路恢復後能回復正常運作。

(d) 測試條件：

無。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 開啟遠端管理介面監控產品，觸發網路連線中斷(例:拔除產品網路線路)。

(2) 檢視產品運作情況。

(3) 恢復產品網路連線。

(g) 測試結果：

(1) 遠端管理介面失去監控能力，但產品仍可正常運作。

(2) 恢復產品網路連線，遠端管理介面回復監控狀態。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.6.1.3 持續運作測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.6.1.3

(b) 測試資料：

無。

(c) 測試目的：

驗證產品是否具備保持連線穩定與功能持續正常運作的運作機制。

(d) 測試條件：

廠商應提供設置保持產品穩定連線與功能持續運作的運作機制書面文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱運作機制之書面文件。

(g) 測試結果：

(1) 運作機制證實讓產品保持連線與功能正常運作，運作機制包括但不限於產品分批線上更新、產品於恢復網路連線時隨機依序連線。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7 隱私保護測試

檢視消費性物聯網產品之隱私保護安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.7.1 隱私保護能力測試

5.7.1.1 個人資料傳輸安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品之個人資料於傳輸中是否加密。

(d) 測試條件：

(1) 廠商應提出產品個人資料傳送所使用的加密演算法書面資料作為審查依據。

(2) 廠商應提出所有關鍵安全參數傳輸的邏輯介面之書面資料，邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 對產品使用安全通道掃描工具。

(3) 於相應之邏輯介面輸入產品所需之個人資料(例如:生物辨識資料、電話號碼)，同時側錄封包。

(4) 檢視所側錄之封包。

(g) 測試結果：

(1) 與測試電腦之間的個人資料以加密傳輸，使用的加密技術採用 NIST SP 800-140C 所核可的同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.2 個人資料傳輸安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.2

(b) 測試資料：

無。

(c) 測試目的：

驗證產品之敏感性個人資料於傳輸中是否加密。

(d) 測試條件：

(1) 廠商應提出產品敏感性個人資料傳送所使用的加密演算法書面資料作為審查依據。

(2) 廠商應提出所有關鍵安全參數傳輸的邏輯介面之書面資料，邏輯介面包括但不限本地端管理介面、網路協定和 API 介面。

(e) 測試佈局：

如圖 2。

(f) 測試方法：

(1) 將測試電腦連接產品。

(2) 對產品使用安全通道掃描工具。

(3) 於相應之邏輯介面傳送產品運作所需之敏感性個人資料(例如:影像串流)，同時側錄封包。

(4) 檢視所側錄之封包。

(g) 測試結果：

(1) 與測試電腦之間的敏感性個人資料以加密傳輸，使用的加密技術採用 NIST SP 800-140C 所核可的同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.3 外部感測功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.3

(b) 測試資料：

無。

(c) 測試目的：

查驗產品存在外部感測功能是否告知使用者。

(d) 測試條件：

廠商應提供產品之外部感測功能說明文件作為審查依據(包括但不限於產品使用手冊、包裝說明等)。

(e) 測試佈局：

無。

(f) 測試方法：

查驗產品之外部感測功能宣告。

(g) 測試結果：

(1) 產品之外部感測功能說明以包括但不限於記載於產品使用說明書、產品包裝、產品官網。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.4 刪除使用者資料測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.4

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否告知使用者如何刪除使用者資料(user data)的方法。

(d) 測試條件：

廠商應提供產品之刪除使用者資料的功能與操作方法說明文件作為審查依據(包括但不限於產品使用手冊、產品官網等)。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱產品之刪除使用者資料之說明文件。

(2) 根據說明文件之操作方式，查驗刪除使用者資料功能。

(g) 測試結果：

(1) 產品之刪除使用者資料功能說明證實足以協助使用者刪除使用者資料，且產品提供使用者友善介面執行刪除資料。

(2) 使用者資料刪除功能說明記載於包括但不限於產品使用手冊。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.7.1.5 刪除關聯服務之個人資料測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.5

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否提供使用者將存在關聯服務的個人資料之刪除功能。

(d) 測試條件：

廠商應提供產品刪除存於關聯服務之個人資料的功能與操作方法說明文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱刪除存於關聯服務之個人資料的功能與操作之說明文件。

(2) 根據說明文件之操作方式，查驗刪除關聯服務中個人資料的功能。

(g) 測試結果：

(1) 產品提供的使用者友善介面執行刪除功能，足以協助使用者以簡便的方式刪除存於關聯服務的個人資料。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.6 刪除個人資料方法測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.6

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否告知使用者如何刪除個人資料的方法。

(d) 測試條件：

廠商應提供產品之刪除個人資料的功能與操作方法說明文件作為審查依據(包括但不限於產品使用手冊)。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱產品之刪除個人資料之說明文件。

(2) 根據說明文件之操作方式，查驗刪除個人資料功能。

(g) 測試結果：

(1) 產品之刪除個人資料之方法說明文件證實足以協助使用者刪除個人資料。

(2) 個人資料刪除功能說明記載於包括但不限於產品使用手冊、產品官網。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.7.1.7 回報刪除狀態測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.7

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否具備回報使用者個人資料刪除狀態之機制。

(d) 測試條件：

廠商應提供產品刪除個人資料機制之說明文件作為審查依據(包括但不限於產品使用手冊)。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱刪除個人資料機制之說明文件。

(2) 根據說明文件之操作方式，從產品、關聯服務、應用程式等處刪除個人資料。

(3) 驗證產品是否回報刪除狀態。

(g) 測試結果：

(1) 收到產品回報的刪除狀態，例如:個人資料已自關聯服務刪除。

(2) 產品回報刪除狀態的方式與廠商說明文件相符，包括但不限於本地端管理介面顯示、電子郵件、簡訊通知等。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.7.1.8 個人資料管理機制

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.8

(b) 測試資料：

無。

(c) 測試目的：

查驗廠商是否具備收集、利用、處理使用者個人資料的管理機制。

(d) 測試條件：

廠商應提供針對使用者個人資料之收集、利用、處理的管理機制，與管理機制實施範圍宣告之書面文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商提供之使用者個人資料管理機制之說明文件。

(g) 測試結果：

(1) 使用者個人資料收集、利用與處理管理機制中應對於收集哪些個人資料、使用目的、提供哪些廠商以外的第三方單位使用及資料保存的政策詳細記載於書面文件。

(2) 管理機制適用範圍包括但不限於產品開發商、系統整合商、第三方廠商和廣告商。

(3) 通過：(1)、(2)二項結果皆符合。

(4) 不通過：(1)、(2)二項結果不符合其一。

(5) 不適用：無。

5.7.1.9 個人資料授權機制

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.9

(b) 測試資料：

無。

(c) 測試目的：

驗證廠商是否具備使用者個人資料之使用授權機制。

(d) 測試條件：

(1) 廠商應基於使用者同意的基礎下才能處理個人資料。

(2) 廠商應提供針對使用者個人資料之使用授權機制，與授權機制實施範圍宣告之書面文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱使用者個人資料之使用授權機制之書面文件。

(2) 驗證產品是否提供個人資料授權功能。

(g) 測試結果：

(1) 廠商沒有未經使用者同意下處理個人資料。

(2) 授權內容應詳細描述使用個人資料的目的，並提供使用者選擇是否同意授權。

(3) 使用者個人資料之使用授權機制應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網、產品包裝。

(4) 通過：(1)~(2)二項結果皆符合。

(5) 不通過：(1)~(2)二項結果不符合其一。

(6) 不適用：無。

5.7.1.10 撤銷個人資料授權

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.10

(b) 測試資料：

無。

(c) 測試目的：

驗證廠商是否具備使用者個人資料之使用授權撤銷機制。

(d) 測試條件：

廠商應提供針對使用者個人資料使用授權之撤銷機制，與機制實施範圍宣告之書面文件作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

(1) 審閱撤銷使用者個人資料之使用授權機制之書面文件。

(2) 驗證產品是否提供撤銷個人資料授權之功能。

(g) 測試結果：

(1) 撤銷機制書面文件應詳細說明撤銷方法，且產品可透過取消授權的功能撤銷個人資料授權。

(2) 使用者個人資料使用授權之撤銷機制應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網、產品包裝。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：無。

5.7.1.11 個人資料收集最小化測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.11

(b) 測試資料：

無。

(c) 測試目的：

查驗產品是否存在收集預期以外的個人資料。

(d) 測試條件：

(1) 產品應支援收集遙測數據。

(2) 廠商應提供產品所收集遙測數據之個人資料之使用目的與實施範圍之宣告作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱收集遙測數據之個人資料之使用目與實施範圍的之宣告文件。

(g) 測試結果：

(1) 產品宣告所列收集個人資料之項目符合該類產品必要之所需，實施範圍包括但不限於產品開發商、系統整合商、第三方廠商和廣告商應遵守收集原則。

(2) 收集遙測數據之個人資料之使用目的與實施範圍之宣告應公開告知使用者，告知方式包括但不限於產品使用手冊、產品官網、產品包裝。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援收集遙測數據。

5.7.1.12 個人資料管理機制

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.7.1.12

(b) 測試資料：

無。

(c) 測試目的：

查驗廠商是否具備收集、利用、處理遙測數據及遙測數據使用者之宣告。

(d) 測試條件：

(1) 產品應支援收集遙測數據。

(2) 廠商應提供針對遙測數據之收集、利用、處理與遙測數據使用者之說明資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱廠商對於遙測數據收集、利用、處理與遙測數據使用者之說明資料。

(g) 測試結果：

(1) 廠商遙測數據之宣告應對於遙測數據種類、使用目的、提供包括但不限於產品開發商、系統整合商、第三方廠商和廣告商使用及資料保存的政策詳細記載於書面文件，並告知使用者。

(2) 告知使用者方式包括但不限於產品使用手冊、產品官網。

(3) 通過：(1)、(2)二項結果皆符合。

(4) 不通過：(1)、(2)二項結果不符合其一。

(5) 不適用：產品不支援收集遙測數據。

5.8 異常警示測試

檢視消費性物聯網產品之警示與紀錄安全需求是否符合書面送審資料，並依下列各測試項目進行實機測試。

5.8.1 安全事件警示測試

5.8.1.1 產品安全事件警示功能測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.8.1.1

(b) 測試資料：

無。

(c) 測試目的：

驗證產品發生未經授權之軟體變更時，是否發出警示。

(d) 測試條件：

(1) 產品應提供軟體設定權限宣告與設定方法之書面文件作為審查依據。

(2) 廠商應提供安全事件告警機制之書面文件。

(e) 測試佈局：

如圖 4。

(f) 測試方法：

(1) 觸發產品以無權限使用者帳號變更執行中與非執行中的軟體設定。

(2) 根據安全事告警機制文件，檢視產品警示狀態。

(g) 測試結果：

(1) 產品發出之警示應符合產品自我宣告，包括但不限於向管理者或使用者發出告警訊息、電子郵件警示。

(2) 通過：(1)項結果符合。

(3) 不過：(1)項結果不符合。

(4) 不適用：無。

5.8.1.2 遙測數據安全測試

(a) 測試依據：

TAICS TS-0045 v1.0「消費性物聯網產品資安標準」5.8.1.2

(b) 測試資料：

產品支援收集遙測數據。

(c) 測試目的：

查驗產品是否可針對收集之遙測數據進行監控可能發生的安全事件。

(d) 測試條件：

(1) 廠商應提供產品收集遙測數據的種類與其用途之說明文件作為審查依據。

(2) 廠商應提供對於產品安全事件之監控機制書面資料作為審查依據。

(e) 測試佈局：

無。

(f) 測試方法：

審閱遙測資料說明文件與產品安全事件監控機制之宣告文件。

(g) 測試結果：

(1) 產品宣告所列之遙測數據種類符合該類產品安全異常監控必要之所需。

(2) 產品之監控機制證實能監控產品之安全事件。

(3) 通過：(1)~(2)二項結果皆符合。

(4) 不通過：(1)~(2)二項結果不符合其一。

(5) 不適用：產品不支援收集遙測數據。

附錄 A
(規定)
安全通道建議使用之密碼套件

安全通道(TLS)所選用的密碼套件應遵循下述幾項要求：

- TLSv1.2
    - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
    - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
    - TLS_ECDHE_RSA_WITH_AES256_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
    - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256
    - TLS_AES_128_CCM_SHA256
    - TLS_AES_128_CCM_8_SHA256

附錄 B
(參考)
產品概述說明(範例)

送測產品應檢附產品概述表，以供測試實驗室參閱：

表 B.1 設備概述表

製造商	XX 公司
設備名稱	XXX
廠牌	XXX
型號	XX-XXX
韌(軟)體版本	XX.XXX.XX
通訊介面	XXX
網路服務(埠號)	https (443)
網路服務平台(IP)	XX 雲端平台 (XX.XX.XX.XX)
日誌存取權限	User A : 唯讀
日誌檔保存期限	90 天
角色存取權限	Administrator : User A :
使用者帳密	Admin 帳號 : Admin 密碼 :
外觀	<picture>

附錄 C
(參考)
安全功能規格說明(範例)

送測產品應檢附安全功能規格表，以供測試實驗室參閱：

表 C.1 安全功能規格表

項目	說明	申請者填寫內容
1. 除錯模式	詳細描述進入產品除錯模式之方法，或提供佐證文件。	
2. 網路協定	詳細描述產品支援之網路協定，或提供說明文件。	
3. 加密演算法	列出產品所提供之加密演算法及其應用，及提供佐證文件。	
4. 日誌與警示機制	說明安全事件警示機制與警示方式，或提供佐證資料。	
5. 安全通道憑證	驗證安全通道安全要求項目之產品應提供。	
6. 安全開發證明	出示相關認證證明，或包括但不限於以下文件：開發人員安全培訓、軟體需求設計階段、安全編碼技術、實施階段的安全收費、安全測試、安全審查、與軟體安全維護有關的資產和資訊的保存、安全部署、安全事件應變流程和管理第三方軟體供應商。	

7. 個人資料收集	詳細描述收集哪些個人資料及其使用情境和提供誰利用、機密保護作法與存取/存放位置。	
8. 遙測數據收集	詳細描述收集哪些遙測數據及其使用目的和提供誰利用、個資/隱私資料保護作法與存取/存放位置。	

參考資料

(1) IEK 物聯網資安威脅與解決方案發展方向,
https://ieknet.iek.org.tw/iekppt/ppt_more.aspx?actiontype=ppt&indu_idno=14&domain=44&sld_preid=4997

(2) National Institute of Standards and Technology, NIST SP 800-140C, CMVP Approved Security Functions, available at URL: https://csrc.nist.gov/projects/cryptographic-module-validation-program

版本修改紀錄

版本	時間	摘要
v1.0	2021/11/25	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw