IoT-3001-1 V1.0

物聯網設備共通資安指引

行動應用資安聯盟

中華民國 112 年 9 月

目錄

引言

全球物聯網應用急速發展，利用聯網設備漏洞發動的資安攻擊事件更是層見疊出，例如：2022 年美國官員來台訪問期間，我國政府及企業之網站、數位看板相繼遭到駭客入侵，以阻斷攻擊、竄改網站和數位看板內容以散布惡意言論。

我國政府及民間企業之聯網設備頻頻遭受駭客攻擊，再再顯示了資安防禦能力有待改善，使目的主管機關迫切需要對其監管之聯網設備，加快腳步規劃相關資通安全政策與規範。自 2017 年起，已累積 16 項物聯網設備之資安產業標準，包括影像監控系列產品、智慧巴士車載機、智慧路燈及感測設備等。雖然，資安產業標準的制定仍持續拓展至新的物聯網應用上，但受限於物聯網應用與科技環境的快速變遷，而資安標準的制定流程是一套嚴謹制度的程序，逐項制定已緩不濟急。

基於國際物聯網相關資安基準（如：NISTIR 8259A）與我國資安政策及法規（如：資通安全管理法）等，建立符合聯網設備共通性與安全實務作法之物聯網設備共通資安指引，旨在提供各單位可依本指引為基礎，作為在保護資訊與網路安全時之參考作法，並透過實際使用情形與事涉相關規範，予以應用及增調。

本指引安全要求內容為非強制、非規定性事項，若各單位採用本指引要求事項另有規格要求或施行作法時，應按其規定。關於本指引之實作運用，詳見附錄 C。

1. 適用範圍

本指引規定物聯網設備之通用的資安基本要求。廣泛適用於國內公務機關所採購或使用之物聯網設備，包括中央目的事業主管機關、場域主管機關及地方政府。

物聯網設備係指具備連網功能之資訊設備，可獨立運行，亦可透過連接其他設備或系統，以實現該物聯網設備之功能應用，例如：文化部設置於展演場域的互動式資訊服務站(KIOSK)、自來水公司布建於住所或廠辦之智慧水表等。物聯網設備之應用架構如圖 1。

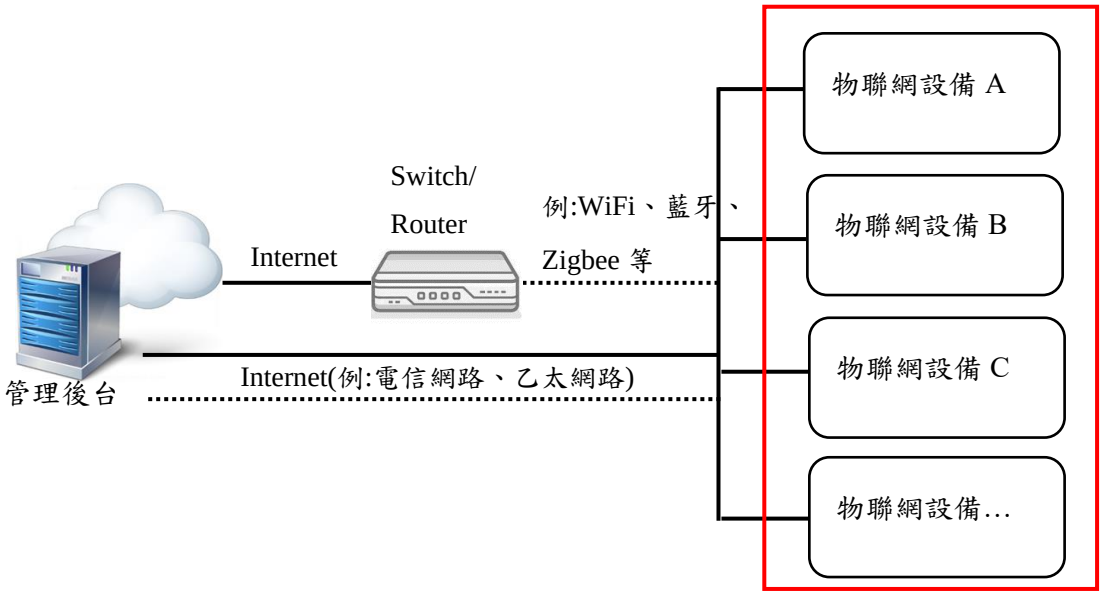

圖 1 物聯網設備適用範圍示意圖

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] NISTIR 8259A-2020 IoT Device Cybersecurity Capability Core Baseline

[2] IEC 62443-4-2-2019 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

[3] ETSI EN 303 645 V2.1.1(2020-06) Cyber Security for Consumer Internet of Things: Baseline Requirements

3. 用語及定義

下列用語及定義適用於本指引。

3.1 物聯網設備(IoT devices)

本指引係指可連接網路之設備，包括感測器、控制設備及智慧建築及智慧家居等聯網設備。

3.2 敏感性資料(Sensitivity data)

本指引之敏感性資料為，安全敏感性資料、敏感性個人資料與個人資料的統稱。

3.3 安全敏感性資料(Security-sensitive data)

指與設備或服務之安全性相關的資料，例如通行碼、金鑰等系統運行所需之機敏資料，或設備運用於特殊、機敏之應用情境所收集、利用、處理之感測資料等。例如：當設備透過無線更新(Over-the air, OTA)更新韌體時，如果更新伺服器發送之憑證金鑰遭惡意人士竄改，可能造成更新失敗或安裝了帶有惡意程式之韌體。

3.4 敏感性個人資料(Sensitive personal data)

係指其被揭露後極有可能對個人造成人身傷害或財產損害的資料。敏感性個人資料之內容因產品和使用案例而異，例如：家用影像攝影機(IP camera)的視訊串流、支付資訊、通訊資料內容帶有時間戳記的位置座標。

3.5 個人資料(Personal data)

係指對於已識別或可識別自然人有關的任何資訊，包括識別個人身分之隱私資料，例如：身分證字號、電話號碼、住址、車牌及生物辨識相關之影像等。

3.6 最小權限(Least privilege)

係一種資訊安全的概念，以使每個使用者都獲得該使用者執行其任務所需之最低存取資源和授權。

3.7 美國國家弱點資料庫(National Vulnerability Database, NVD)[2]

指美國國家標準技術研究所(National Institute of Standards and Technology, NIST)提供的美國國家弱點資料庫，負責常見弱點與漏洞(如 3.8 所述)之資料的發布及更新。

3.8 常見弱點與漏洞(Common Vulnerabilities and Exposures, CVE)

由美國國土安全部贊助之弱點管理計畫，針對每一弱點項目給予全球認可之唯一共通編號，CVE 對每一漏洞皆賦予專屬編號，編號格式為 CVE-YYYY-NNNN，CVE 為固定前綴字、YYYY 為西元年及 NNNN 為流水編號。

3.9 通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)

使用 IT 漏洞的特點與影響進行評分，由美國資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)發展至第 3.1 版[3]。包括威脅所造成損害的嚴重性、資安漏洞的可利用程度與攻擊者不當運用該漏洞的難易度，都被列入評比。評比從 0 分到 10 分，0 代表沒有漏洞不嚴重，而 10 則代表最最嚴重。

3.10 加密(Encryption)

指為了避免資訊的洩漏，明文資訊透過數學演算法進行改變，使原來的明文資訊變成不可讀而達到保密之目的。

3.11 安全通道(Security tunnel)

為網際網路通訊端點與端點(End-to-End)間，達到資料隱密性及完整性所建立之通道，例如：目前常見之實作傳輸層安全性(Transport Layer Security, TLS)。

3.12 安全事件日誌(Security event log)

係指記錄每個稽核規則所定義的活動，用以察覺威脅或攻擊事件的發生，本文之安全事件包括但不限於使用者登入、連線失敗、資源達警戒值等行為。

3.13 安全監控(Security monitoring)

係收集、分析潛在資安威脅之自動化過程，對該威脅進行分類、警示等適當的行動；安全監控功能泛指系統或設備提供產業實務普遍所接受(或建議)之網路安全持續監控的能力，包括提供及時偵測和回報安全漏洞等。例如：透過入侵偵測系統

(Intrusion Detection System, IDS)、入侵防護系統(Intrusion Prevention System, IPS)等各種監控技術和工具。

3.14 除錯模式(Debug mode)

係指一個以釐清產品故障原因為目的程式，其允許開發者透過該介面進行除錯或設定，亦稱作工程模式。

3.15 遙測數據(Telemetry data)

係指蒐集來自產品的資訊，可以提供廠商用以識別與產品相關的問題或改善產品服務所需之相關的訊息，例如：產品失效(crash)回報、產品座標(GPS)、使用習慣紀錄等資訊。

3.16 網路服務(Network service)

係指使用者對設備進行存取功能時，所使用之網路功能或介面，例如：設備開啟 TCP 22 埠以提供 SSH 遠端連線服務。

3.17 受限制設備(Constrained device)

係指此類設備預期用途受限於實體而產生的限制，包括但不限於處理資料的能力、通訊的能力、資料儲存的能力或與使用者互動的能力。例如：感測器，它可能是實體限制的設備，可能因電源、電池壽命、運算處理能力、實體的存取、功能有限、記憶體有限或網路頻寬有限，這些限制在設備運行時可能需要搭配另一設備來支援；或者，可能是透過同一實體線路供電與資料傳輸，此設備的通訊協定與加密方式就受限於該線路配置。

3.18 授權個體(Authorized entity)

係指獲得允許與特定物聯網設備相互存取之人類使用者、設備或組件等。本指引不指定以何種方式實現授權。

3.19 日誌滾動(Log rotation)

指系統管理中之自動化歸檔過期日誌檔的過程，每次新增日誌檔時，舊日誌檔名後的數字即遞增，當舊日誌檔後的數字超過設定之臨界值時，可刪除或存到他處

以釋放儲存空間。日誌滾動提供有效的方法限制日誌檔的大小，同時保留近期的日誌用於分析。

3.20 軟體組成清單(Software bill of materials, SBOM)

係記錄所有用於建構軟體時，所使用之各種組件(例如:商業軟體、開源軟體)的清單文件，文件內容包含各種組件之詳細資訊和供應鏈關係等。

4. 共通指引概述

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全要求總表

安全要求總表如表 1 所示，第一欄為安全構面，包括：(1)設備鑑別、(2)設備安全配置、(3)資料保護、(4)存取介面、(5)軟韌體更新及(6)資訊與網路安全狀態；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；第三欄為各安全要求分項之細部安全要求，作為設備安全評估參考。本安全總表各欄的關聯性，須依循本節 5.1 至 5.6 之安全要求內容。

表 1 安全要求等級總表

安全構面	安全要求分項	安全要求
5.1 設備鑑別	5.1.1 鑑別機制	5.1.1.1、5.1.1.2
5.2 設備安全配置	5.2.1 安全設定	5.2.1.1、5.2.1.2、 5.2.1.3、5.2.1.4
5.3 資料保護	5.3.1 加密功能	5.3.1.1、5.3.1.2
	5.3.2 儲存與傳輸資料保護	5.3.2.1、5.3.2.2
	5.3.3 軟體與資料的完整性	5.3.3.1、5.3.3.2
5.4 存取介面	5.4.1 存取介面安全	5.4.1.1、5.4.1.2、 5.4.1.3、5.4.1.4、 5.4.1.5、5.4.1.6
	5.4.2 通行碼鑑別	5.4.2.1、5.4.2.2、5.4.2.3
	5.4.3 權限控管	5.4.3.1
5.5 軟韌體更新	5.5.1 更新安全	5.5.1.1、5.5.1.2、5.5.1.3
5.6 資訊與網路安全狀態	5.6.1 已知漏洞	5.6.1.1、5.6.1.2
	5.6.2 安全事件日誌功能	5.6.2.1
	5.6.3 日誌管理	5.6.3.1、5.6.3.2、 5.6.3.3、5.6.3.4
	5.6.4 安全監控	5.6.4.1、5.6.4.2

4.1.1 安全構面：

(a)設備鑑別：設備應提供能與其他相連設備進行身分識別與鑑別的能力，以防止特定人士複製或偽冒。

(b)設備安全配置：設備應提供網路與組態之安全指南，以輔助使用者進行網路與資料備份等安全設置與資源管理，以預防網路攻擊或系統故障導致設備服務中斷時，在可容忍時間內恢復正常服務。

(c)資料保護：設備傳輸與儲存之資料應具備足夠的安全保護，避免遭受非授權的讀取或有心人士惡意竄改。

(d)存取介面：對於存取介面、韌體、軟體及作業系統之存取，是否具有身分鑑別與權限控管機制，不應開啟之存取介面、網路服務應預設為關閉。

(e)軟韌體更新：設備應提供更新機制，且執行作業系統及韌體版本更新服務，須具備足夠資安防護能力。

(f)資安與網路安全狀態：應對設備持續監控、修正安全漏洞，並在安全事件發生時具備記錄與警示功能。

4.1.2 安全要求分項：

依安全構面所設計對應之安全要求分項，其中每一安全要求分項包含一個或一個以上之安全要求。

5. 安全要求

本節載明物聯網設備須滿足之基本安全功能及建議採取之方法。

5.1 設備鑑別

5.1.1 鑑別機制

5.1.1.1 設備應支援讓相連之系統或其他設備進行身分鑑別的能力。

5.1.1.2 若設備與其他相連系統或其他設備相連時，應提供唯一識別。

5.2 設備安全配置

5.2.1 安全設定

5.2.1.1 設備應具備有關網路及安全組態設定之安全指南，且應提供網路及安全組態設定功能。

5.2.1.2 當設備服務中斷或失效後，設備應提供復原至已知安全狀態的能力。

5.2.1.3 設備應提供備份功能，且備份過程不能影響產品正常運作，以確保在可容忍時間內恢復正常運作狀態。

5.2.1.4 若設備支援透過遠端連線執行指令功能，設備應具備遠端會話終止(Remote session termination)功能。

5.3 資料保護

5.3.1 加密功能

5.3.1.1 設備所使用之加密演算法應為國際公認且經安全證實的加密安全機制，例如：NIST SP 800-140Cr1。

5.3.1.2 設備所使用之加密金鑰或憑證應具備管理機制，且管理機制應依循國際公認之加密金鑰管理指引之建議，例如：NIST SP 800-57。

5.3.2 儲存與傳輸資料保護

5.3.2.1 若設備具有儲存、傳輸安全敏感性資料的功能，應對安全敏感性資料提供機密性之保護。

5.3.2.2 若設備存在個人資料或敏感性個人資料時，應符合我國個資管理法之規範。

5.3.3 軟體與資料的完整性

5.3.3.1 設備應提供資料在儲存、使用、傳送及接收時完整性之保護。

5.3.3.2 設備應提供完整性檢查及警示功能，以確認設備軟體、組態和資料是否經未授權變更。

5.4 存取介面

5.4.1 存取介面安全

5.4.1.1 設備之所有存取介面應提供授權個體身分鑑別機制。

5.4.1.2 設備所提供之身分鑑別機制，應支援使用者唯一識別與鑑別之能力。

5.4.1.3 設備預設遠端存取應關閉；或若設備須開啟遠端存取功能時，應具備授權與鑑別機制。

5.4.1.4 設備應防止由實體介面進入除錯模式的功能；若設備須開啟實體介面存取除錯模式時，應具備鑑別機制。

5.4.1.5 設備應關閉非必要之管理介面與網路服務。

5.4.1.6 若設備支援收集遙測數據時，應提供所使用之網路服務，及收集之遙測數據種類、使用目的，及遙測數據收集和使用之對象。

5.4.2 通行碼鑑別

5.4.2.1 若設備使用通行碼身分鑑別，設定通行碼長度和強度應根據國際公認通行碼安全指引之建議，例如：NIST SP 800-63B。

5.4.2.2 若設備使用通行碼身分鑑別，應具備防止通行碼暴力攻擊之身分鑑別機制，例如：身分鑑別失敗達 5 次後，即鎖定登入。

5.4.2.3 若設備使用預設通行碼作為身分鑑別時，應提供每設備唯一通行碼，或強制更改預設帳號(若支援)及預設通行碼。

5.4.3 權限控管

5.4.3.1 若設備不為受限制設備，應提供設定使用者權限與控管的機制。

5.5 軟韌體更新

5.5.1 更新安全

5.5.1.1 設備應具備安全更新機制；若為無法更新軟韌體之受限制設備，應提供硬體更換等更新機制。

5.5.1.2 若設備支援線上更新軟韌體，應確保傳輸通道的完整性與真實性，所使用之加密演算法應符合 5.3.1.1 之加密演算法。

5.5.1.3 若設備支援本地更新軟韌體，安裝更新前應檢驗軟韌體之完整性與真實性，所使用之加密演算法應符合 5.3.1.1 之加密演算法。

5.6 資訊與網路安全狀態

5.6.1 已知漏洞

5.6.1.1 若設備提供使用者介面，應僅提供沒有可被攻擊利用之錯誤訊息或代碼，例如：無效使用者、通行碼輸入錯誤等明確提示錯誤之處的訊息。

5.6.1.2 設備不應存在美國國家漏洞資料庫(NVD)所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性評等為高。

5.6.2 安全事件日誌功能

5.6.2.1 設備應提供產生安全事件日誌之功能，安全事件日誌種類應包括但不限於：存取控制、請求錯誤、控制系統事件、備份及恢復事件、組態變更、安全事件日誌事件；若為受限制設備，則應提供補償性作法以達到記錄安全事件之能力。

5.6.3 日誌管理

5.6.3.1 安全事件日誌之存取應具備權限控管機制。

5.6.3.2 安全事件日誌應具備日誌保存期限與儲存容量配置之功能。

5.6.3.3 當安全事件記錄失敗時，應根據公認資安產業實務作法作出相對應之處理，例如：日誌滾動(Log rotation)。

5.6.3.4 安全事件日誌應具備時間同步之時間戳，且時間戳之格式須一致，例如：ISO/IEC 8601:2019[6]、CNS 7648[10]之格式。

5.6.4 安全監控

5.6.4.1 設備應可支援公認資安產業實務作法之安全監控功能，或以補償性作法以達到對設備持續安全監控，例如：支援 SNMP、部署 IDS、IPS 等。

5.6.4.2 設備應具備軟體組成清單(SBOM)，軟體組成清單內容欄位包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者。

附錄 A
（參考）
建立共通基本資安指引之程序

根據 NISTIR 8259C[1]建立資安基本要求方法論之步驟，分為四個階段逐步進行。

第一階段，確立欲建立之資安指引的範圍與主管機關所訂定的資安法規、資安準則等控制措施文件，本標準引用我國資通安全管理法之附表十 資通系統防護基準[7]。

第二階段，以方法論所提出之三個核心概念「以設備為中心(Device-centricity)」、「專注於資安(Cybersecurity focus)」和「最低安全性(Minimal securablity)」，對上述控制措施逐一過濾篩選，如表 A 1、表 A 2。

表 A 1 共通指引要求事項與資通安全管理法(控制措施)對照表

資通系統防護基準					資通安全責任等級分級辦法	共通指引
構面	措施內容	項次	等級	控制措施	技術面	項次
存取控制	帳號管理	1	普	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	-	5.3.2.2
		2	中	已逾期之臨時或緊急帳號應刪除或禁用。	-	非基本需求
		3	中	資通系統閒置帳號應禁用。		
		4	中	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。		
		5	高	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。		
		6	高	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。		
		7	高	應依機關規定之情況及條件，使用資通系統。		
		8	高	監控資通系統帳號，如發現帳號違常使用時回報管理者。		
	最小權限	9	中	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。	政府組態基準：網通設備 TWGCB-03-001-0009 TWGCB-03-001-0013	5.4.3.1
	遠端存取	10	普	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	政府組態基準：網通設備 TWGCB-03-001-0009	5.4.1.3

資通系統防護基準					資通安全責任等級分級辦法	共通指引
					TWGCB-03-001-0013	
		11	普	使用者之權限檢查作業應於伺服器端完成。	–	不適用
		12	普	應監控遠端存取機關內部網段或資通系統後臺之連線。	政府組態基準：網通設備 TWGCB-03-001-0016	5.6.4.1
		13	普	應採用加密機制。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.2.1
		14	中	遠端存取之來源應為機關已預先定義及管理之存取控制點。	–	非基本需求
事件日誌與可歸責性	記錄事件	15	普	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	–	5.6.3.2
		16	普	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	政府組態基準：網通設備 TWGCB-03-001-0015	5.6.2.1
		17	普	應記錄資通系統管理者帳號所執行之各項功能。	–	
		18	中	應定期審查機關所保留資通系統產生之日誌。	–	非基本需求
	日誌紀錄內容	19	普	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	政府組態基準：網通設備 TWGCB-03-001-0015	5.6.2.1
	日誌儲存容量	20	普	依據日誌儲存需求，配置所需之儲存容量。	–	5.6.3.2
	日誌處理失效之回應	21	普	資通系統於日誌處理失效時，應採取適當之行動。	–	5.6.3.3
		22	高	機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	–	非基本需求
	時戳及校時	23	普	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	–	5.6.3.4
		24	中	系統內部時鐘應定期與基準時間源進行同步。	–	非基本需求

資通系統防護基準					資通安全責任等級分級辦法	共通指引
	日誌資訊之保護	25	普	對日誌之存取管理，僅限於有權限之使用者。	–	5.6.3.1
		26	中	應運用雜湊或其他適當方式之完整性確保機制。	–	非基本需求
		27	高	定期備份日誌至原系統外之其他實體系統。	–	非基本需求
營運持續計畫	系統備份	28	普	訂定系統可容忍資料損失之時間要求。	政府組態基準：網通設備 TWGCB-03-001-0008	5.2.1.3
		29	普	執行系統源碼與資料備份。		
		30	中	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	–	非基本需求
		31	高	應將備份還原，作為營運持續計畫測試之一部分。	–	
		32	高	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	–	
	系統備援	33	中	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	–	5.2.1.2
		34	中	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。	–	
識別與鑑別	內部使用者之識別與鑑別	35	普	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	–	5.4.1.2
		36	高	對資通系統之存取採取多重認證技術。	–	非基本需求
	身分驗證管理	37	普	使用預設密碼登入系統時，應於登入後要求立即變更。	政府組態基準：網通設備 TWGCB-03-001-0004	5.4.2.3
		38	普	身分驗證相關資訊不以明文傳輸。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.2.1
		39	普	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	政府組態基準：網通設備 TWGCB-03-001-0019	5.4.2.2
		40	普	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。(對非內部使用者，可依機關自行規範辦理)	政府組態基準：作業系統 TWGCB-01-005-0003 TWGCB-01-005-0004	5.4.2.1

資通系統防護基準					資通安全責任等級分級辦法	共通指引
		41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)	政府組態基準：作業系統 TWGCB-01-005-0005	
		42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。	–	不適用
		43	中	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	–	非基本需求
		44	中	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	–	非基本需求
	鑑別資訊回饋	45	普	資通系統應遮蔽鑑別過程中之資訊。	–	5.6.1.1
	加密模組鑑別	46	中	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.2.1
	非內部使用者之識別與鑑別	47	普	資通系統應識別及鑑別非機關使用者 (或代表機關使用者行為之程序)。	–	5.4.1.1 5.4.1.6
系統與服務獲得	系統發展生命週期需求階段	48	普	針對系統安全需求(含機密性、可用性、完整性)，進行確認。	–	5.2、5.3
	系統發展生命週期設計階段	49	中	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	–	非基本需求
		50	中	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	–	非基本需求
	系統發展生命週期開發階段	51	普	應針對安全需求實作必要控制措施。	資通安全弱點通報機制	不適用
		52	普	應注意避免軟體常見漏洞及實作必要控制措施。	安全性檢測:弱點掃描	5.6.1.2
		53	普	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	–	5.6.1.1
		54	高	執行「源碼掃描」安全檢測。	–	非基本需求
		55	高	系統應具備發生嚴重錯誤時之通知機制。	–	非基本需求

資通系統防護基準					資通安全責任等級分級辦法	共通指引
	系統發展生命週期測試階段	56	普	執行「弱點掃描」安全檢測。	安全性檢測:弱點掃描	5.6.1.2
		57	高	執行「滲透測試」安全檢測。	–	非基本需求
	系統發展生命週期部署與維運階段	58	普	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	政府組態基準：網通設備 TWGCB-03-001-0009 TWGCB-03-001-0013	5.4.1.3
					–	5.4.1.4
					政府組態基準：網通設備 TWGCB-03-001-0002	5.4.1.5
					–	5.5.1.1
		59	普	資通系統不使用預設密碼。	政府組態基準：網通設備 TWGCB-03-001-0004	5.4.2.3
		60	中	於系統發展生命週期之維運階段，應執行版本控制與變更管理。	–	非基本需求
	系統發展生命週期委外階段	61	普	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。	–	不適用
	獲得程序	62	中	開發、測試以及正式作業環境應為區隔。	–	非基本需求
	系統文件	63	普	應儲存與管理系統發展生命週期之相關文件。	–	不適用
系統與通訊保護	傳輸之機密性與完整性	64	高	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.2.1
					–	5.3.3.1
					–	5.5.1.2
		65	高	使用公開、國際機構驗證且未遭破解的演算法。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.1.1
		66	高	支援演算法的最大長度金鑰。	–	5.3.1.2
		67	高	加密金鑰或憑證週期性更換。	–	
		68	高	伺服器端之金鑰保管應製定管理規則及實施應有之安全防護措施。	–	

資通系統防護基準					資通安全責任等級分級辦法	共通指引
	資料儲存之安全	69	高	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	政府組態基準：網通設備 TWGCB-03-001-0001*	5.3.2.1
					–	5.3.3.1
系統與資訊完整性	漏洞修復	70	普	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	–	5.5.1.1
		71	中	定期確認資通系統相關漏洞修復之狀態。	–	非基本需求
	資訊系統監控	72	普	發現資通系統有被入侵跡象時，應通報機關特定人員。	資通安全防護：入侵偵測及防禦機制 政府組態基準：網通設備 TWGCB-03-001-0016	5.6.4.1
		73	中	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	–	非基本需求
		74	高	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	–	非基本需求
	軟體及資訊完整性	75	中	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	–	5.3.3.2
					–	5.5.1.3
		76	中	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	–	不適用
		77	中	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	–	5.3.3.2
		78	高	應定期執行軟體和資訊完整性檢查。	–	非基本需求

(*表示部分相符)

資通安全管理法之資通安全責任等級B應辦事項中，技術面要求須符合政府組態基準，本指引所引用之網通設備政府組態基準[8]，如下表 A 2：

表 A 2 共通指引要求事項與網通設備政府組態基準(GCB)對照表

TWGCB-ID	類別	原則設定名稱	共通指引
TWGCB-03-001-0001	組態安全	使用 2 層或 3 層的 AES 加密方式	5.3.1.1
			5.3.2.1
TWGCB-03-001-0002		關閉未使用的網路設備管理埠	5.4.1.5
			5.4.1.7
TWGCB-03-001-0003		啟用連線逾時功能	5.2.1.4

TWGCB-ID	類別	原則設定名稱	共通指引
TWGCB-03-001-0004		變更出廠預設值的密碼內容	5.4.2.3
TWGCB-03-001-0005		變更預設 SSID	5.2.1.1
TWGCB-03-001-0006		關閉 SSID 廣播	
TWGCB-03-001-0007		降低無線網路設備發送訊號功率	
TWGCB-03-001-0008		啟用備份系統組態設定值	5.2.1.3
TWGCB-03-001-0009		限制重要功能操作	5.4.1.3
TWGCB-03-001-0010	存取控制	啟用 MAC 位置過濾	不適用:非共通要求
TWGCB-03-001-0011		關閉 DHCP 協定	不適用:非共通要求
TWGCB-03-001-0012		啟用允許存取網路時段	不適用:非共通要求
TWGCB-03-001-0013		啟用存取行為管控	5.4.1.3
TWGCB-03-001-0014		啟用黑名單管控	不適用:系統整體部署相關之設定
TWGCB-03-001-0015	連線監控	啟用並設定 log 紀錄	5.6.2.1
TWGCB-03-001-0016		啟用外部網路異常行為監控	5.6.4.1
TWGCB-03-001-0017		啟用流量偵測功能	不適用:系統整體部署相關之設定
TWGCB-03-001-0018		啟用流量調節功能	不適用:系統整體部署相關之設定
TWGCB-03-001-0019		啟用登入錯誤次數限制	5.4.2.2

第三階段，引用 NISTIR 8259A 之安全構面，包括設備鑑別、設備安全配置、資料保護、存取介面、軟韌體更新及資訊與網路安全狀態，將過濾篩選後之控制措施對應此六項安全構面，對應結果如下表 A 3。

表 A 3 控制措施對應 NISTIR 8259A 之六項安全構面對照表

六項安全構面	安全類別	資通系統防護基準			資通安全責任等級分級辦法	共通指引
		構面	措施內容	控制措施	技術面	項次編號
1.設備鑑別	鑑別機制	識別與鑑別	身分驗證管理(普)	使用預設密碼登入系統時，應於登入後要求立即變更 。	政府組態基準：網通設備 TWGCB-03-001-0004	5.4.2.3
		系統與服務獲得	系統發展生命週期部署與維運階段(普)	資通系統不使用預設密碼。		
2.設備安全配置	安全設定	–	–	–	政府組態基準：網通設備 TWGCB-03-001-0005 TWGCB-03-001-0006 TWGCB-03-001-0007	5.2.1.1
		營運持續計畫	系統備援(中)(無普級)	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務 。	–	5.2.1.2
		營運持續計畫	系統備份(普)	訂定系統可容忍資料損失之時間要求。 執行系統源碼與資料備份 。	政府組態基準：網通設備 TWGCB-03-001-0008	5.2.1.3
		–	–	–	政府組態基準：網通設備 TWGCB-03-001-0003	5.2.1.4
3.資料保護	加密功能	系統與通訊保護	傳輸之機密性與完整性(高)(無普、中級)	使用公開、國際機構驗證且未遭破解之演算法。	政府組態基準：網通設備 TWGCB-03-001-0001	5.3.1.1
		系統與通訊保護	傳輸之機密性與完整性(高)(無中、高級)	支援演算法最大長度金鑰。 加密金鑰或憑證應定期更換。 伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	–	5.3.1.2
	儲存與傳輸資	存取控制	遠端存取(普)	應採用加密機制。	政府組態基準：網通設備 TWGCB-03-001-0001	5.3.2.1
		識別與鑑別	身分驗證管理(普)	身分驗證相關資訊不以明文傳輸。		

六項 安全構面	安全 類別	資通系統防護基準			資通安全責任等級分級辦法	共通 指引
		構面	措施內容	控制措施	技術面	項次 編號
	料保護	識別與鑑別	加密模組鑑別(中)(無普級)	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		
		系統與通訊保護	傳輸之機密性與完整性(高)(無普、中級)	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更 。但傳輸過程中有替代之實體保護措施者，不在此限。		
		系統與通訊保護	資料儲存之安全(高)(無普、中級)	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。		
		存取控制	帳號管理(普)	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	-	5.3.2.2
	軟體和資料的完整性	系統與通訊保護	傳輸之機密性與完整性(高)(無普、中級)	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更 。但傳輸過程中有替代之實體保護措施者，不在此限。	-	5.3.3.1
		系統與通訊保護	資料儲存之安全(高)(無普、中級)	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	-	
		系統與資訊完整性	軟體及資訊完整性(中)(無普級)	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊 。 發現違反完整性時，資通系統應實施機關指定之安全保護措施 。	-	5.3.3.2
4.存取介面	存取介面安全	識別與鑑別	身分驗證管理(普)	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	-	5.4.1.1
		識別與鑑別	內部使用者之識別與鑑別(普)	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之之功能，禁止使用共用帳號。	-	5.4.1.2
		存取控制	遠端存取(普)	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	政府組態基準：網通設備 TWGCB-03-001-0009 TWGCB-03-001-0013	5.4.1.3
		系統與服務獲得	系統發展生命週期部署與維運階段(普)	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。		

六項 安全構面	安全 類別	資通系統防護基準			資通安全責任等級分級辦法	共通 指引
		構面	措施內容	控制措施	技術面	項次 編號
		系統與服務獲得	系統發展生命週期部署與維運階段(普)	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	政府組態基準：網通設備 TWGCB-03-001-0002	5.4.1.4 5.4.1.5
		識別與鑑別	非內部使用者之識別與鑑別(普)	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。		5.4.1.6
	通行碼鑑別	識別與鑑別	身分驗證管理(普)	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	政府組態基準：作業系統 TWGCB-01-005-0003 TWGCB-01-005-0004	5.4.2.1
			身分驗證管理(普)	密碼變更時，至少不可以與前三次使用過之密碼相同。	政府組態基準：作業系統 TWGCB-01-005-0005	
		識別與鑑別	身分驗證管理(普)	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	政府組態基準：網通設備 TWGCB-03-001-0019	5.4.2.2
	權限控管	存取控制	最小權限(中)(無普級)	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。	政府組態基準：網通設備 TWGCB-03-001-0009 TWGCB-03-001-0013	5.4.3.1
5.軟韌體更新	更新安全	系統與資訊完整性	漏洞修復(普)	系統之漏洞修復應測試有效性及潛在影響，並定期更新 。	-	5.5.1.1
		系統與服務獲得	系統發展生命週期部署與維運階段(普)	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。		
		系統與通訊保護	傳輸之機密性與完整性(高)(無普、中級)	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更 。但傳輸過程中有替代之實體保護措施者，不在此限。	-	5.5.1.2
		系統與資訊完整性	軟體及資訊完整性(中)(無普級)	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊 。	-	5.5.1.3
	已知漏洞	識別與鑑別	鑑別資訊回饋(普)	資通系統應遮蔽鑑別過程中之資訊。	-	5.6.1.1

六項 安全構面	安全 類別	資通系統防護基準			資通安全責任等級分級辦法	共通 指引
		構面	措施內容	控制措施	技術面	項次 編號
6.資訊與網路安全狀態		系統與服務獲得	系統發展生命週期開發階段(普)	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。		
		系統與服務獲得	系統發展生命週期測試階段(普)	執行「弱點掃描」安全檢測。	安全性檢測-弱點掃描	5.6.1.2
		系統與服務獲得	系統發展生命週期開發階段(普)	應注意避免軟體常見漏洞及實作必要控制措施。		
	安全事件日誌功能	事件日誌與可歸責性	記錄事件(普)	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 應記錄資通系統管理者帳號所執行之各項功能。	政府組態基準：網通設備 TWGCB-03-001-0015	5.6.2.1
	日誌管理	事件日誌與可歸責性	日誌紀錄內容(普)	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別 等資訊， 採用單一日誌機制，確保輸出格式之一致性 ，並應依資通安全政策及法規要求納入其他相關資訊。		
		事件日誌與可歸責性	日誌資訊之保護(普)	對日誌之存取管理，僅限於有權限之使用者。		5.6.3.1
		事件日誌與可歸責性	記錄事件(普)	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。		5.6.3.2
		事件日誌與可歸責性	日誌儲存容量(普)	依據日誌儲存需求，配置所需之儲存容量。		
		事件日誌與可歸責性	日誌處理失效之回應(普)	資通系統於日誌處理失效時，應採取適當之行動 。		5.6.3.3
		事件日誌與可歸責性	時戳及校時(普)	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間 (UTC)或格林威治標準時間 (GMT)。		5.6.3.4
	安全監控	系統與資訊完整性	資通系統監控(普)	發現資通系統有被入侵跡象時，應通報機關特定人員 。	資通安全防護：入侵偵測及防禦機制 政府組態基準：網通設備	5.6.4.1
		存取控制	遠端存取(普)	應監控遠端存取機關內部網段或資通系統後臺之連線。		

六項 安全構面	安全 類別	資通系統防護基準			資通安全責任等級分級辦法	共通指引
		構面	措施內容	控制措施	技術面	項次編號
					TWGCB-03-001-0016	

第四階段，將對應結果參考國際資安標準(例：IEC 62443-4-2、ETSI EN 303 645)，建立該項目所需之資安能力與要求。

附錄 B
(參考)
共通指引要求事項與各標準規範對照表

共通指引要求項目	參考範例		
	IEC 62443-4-2	ETSI EN 303 645	國內產業標準
5.1.1.1	CR1.2	-	智慧路燈系統：5.1.1.6 門禁系統：5.1.1.6
5.1.1.2	CR1.2RE(1)	-	門禁系統：5.1.1.11
5.2.1.1	CR7.6	5.12-1* 5.12-2*	門禁系統：5.2.2.2 消費性網路攝影機：5.2.2.3
5.2.1.2	CR7.4	-	門禁系統：5.4.1.2
5.2.1.3	CR7.3	-	門禁系統：5.4.1.6
5.2.1.4	CR2.6	-	門禁系統(三)：5.1.2.4
5.3.1.1	CR4.3	5.1-3* 5.5-1* 5.3-7*	感測裝置：5.2.3.1 門禁系統：5.3.1.1
5.3.1.2	-	5.5-8	影像監控系統：5.2.4.3 智慧路燈系統：7.2.1.2 門禁系統：5.2.2.1
5.3.2.1	CR4.1	5.5-1 5.5-6	影像監控系統：5.2.4.2 智慧路燈系統：5.2.1.2、5.2.2.1 感測裝置：5.2.1.1 門禁系統：5.3.1.2 消費性網路攝影機 5.4.1.2、5.4.2.2 智慧巴士：5.2.2.1、5.1.5.2
5.3.2.2	-	5.11-2* 5.11-3* 5.11-4*	門禁系統：5.1.1.1*
5.3.3.1	CR1.5* CR3.1	5.4-1*	感測裝置：5.2.2.2 門禁系統：5.2.1.1、5.2.1.2
5.3.3.2	CR3.4 CR3.14	5.7-2	門禁系統：5.2.1.4 智慧巴士：5.1.1.2
5.4.1.1	CR1.1	5.5-4	影像監控系統：5.4.1.1 智慧路燈系統：5.1.1.2 感測裝置：5.1.1.2 門禁系統：5.1.1.9 消費性網路攝影機：5.1.1.3
5.4.1.2	CR1.1RE(1)	5.1-2	門禁系統：5.1.1.10
5.4.1.3	CR2.2	5.5-4* 5.6-1*	影像監控系統：5.3.2.2 智慧路燈系統：5.1.1.1

共通指引 要求項目	參考範例		
	IEC 62443-4-2	ETSI EN 303 645	國內產業標準
5.4.1.4	NDR2.13	5.6-3 5.6-4	影像監控系統：5.1.1.1 智慧路燈系統：5.3.1.1 消費性網路攝影機：5.5.1.1
5.4.1.5	CR7.7	5.6-1	影像監控系統：5.2.2.1 智慧路燈系統：5.6.2.1 感測裝置：5.5.1.1 門禁系統：5.2.2.3 消費性網路攝影機：5.2.2.1
5.4.1.6	-	6.5	門禁系統(六)：5.7.1.9
5.4.2.1	CR1.7	-	影像監控系統：5.4.2.2、5.4.2.3、5.4.2.6 智慧路燈系統：5.1.3.2、5.1.3.3
5.4.2.2	CR1.11	5.1-5	影像監控系統：5.4.2.4 消費性網路攝影機：5.1.2.2
5.4.2.3	CR1.5*	5.1-1	影像監控系統：5.4.2.1、5.4.1.4 智慧路燈系統：5.1.3.1 感測裝置：5.1.1.3 門禁系統：5.1.1.1 消費性網路攝影機：5.1.3.1
5.4.3.1	CR2.1 CR2.1RE(1)	5.1-4	影像監控系統：5.4.3.1 智慧路燈系統：5.1.2.1 感測裝置：5.1.2.1 門禁系統(二)：5.1.2.2 消費性網路攝影機：5.1.2.1
5.5.1.1	NDR3.10	5.3-1 5.3-2 5.3-8	影像監控系統：5.2.3.1 門禁系統：5.5.1.1
5.5.1.2	-	5.3-10	影像監控系統：5.2.3.3 智慧路燈系統：5.4.1.4、5.4.1.2 感測裝置：5.4.1.2 門禁系統：5.5.1.3 消費性網路攝影機：5.3.1.2
5.5.1.3	NDR3.10RE(1)	5.3-9	影像監控系統：5.2.3.4 感測裝置：5.4.1.3 門禁系統：5.5.1.2
5.6.1.1	CR3.7	-	影像監控系統：5.4.1.2 門禁系統：5.2.1.7、5.1.1.2
5.6.1.2	-	-	影像監控系統：5.2.1.2、5.2.5.1 智慧路燈系統：5.6.1.2、5.7.1.1 感測裝置：5.5.1.3 門禁系統：5.2.3.2、5.2.3.5 消費性網路攝影機：5.2.1.1 智慧巴士：5.1.1.1、5.1.6.1

共通指引 要求項目	參考範例		
	IEC 62443-4-2	ETSI EN 303 645	國內產業標準
5.6.2.1	CR2.8	-	影像監控系統：5.2.7.1 智慧路燈系統：5.5.1.1 感測裝置：5.6.2.1 門禁系統：5.6.1.1 智慧巴士：5.1.4.1
5.6.3.1	CR3.9 CR6.1	-	影像監控系統：5.2.7.2 智慧路燈系統：5.5.1.3 門禁系統：5.6.1.7、5.6.1.11
5.6.3.2	CR2.9	-	門禁系統：5.6.1.2
5.6.3.3	CR2.10	-	門禁系統：5.6.1.4
5.6.3.4	CR2.11	-	門禁系統：5.6.1.5
5.6.4.1	CR6.2	-	門禁系統(二、三、四、六)：5.2.3.2
5.6.4.2	-	-	門禁系統：5.2.2.9

(*表示部分相符)

附錄 C
（參考）
運用共通資安指引之建議作法

本指引係非強制、非規定性之安全要求，於各單位在衡量其列管物聯網設備之安全程度時，提供具彈性且符合實務之建議。

運用本指引之建議作法，分別為發證、檢測及自我評量三項作法，如下圖 C 1 所示。

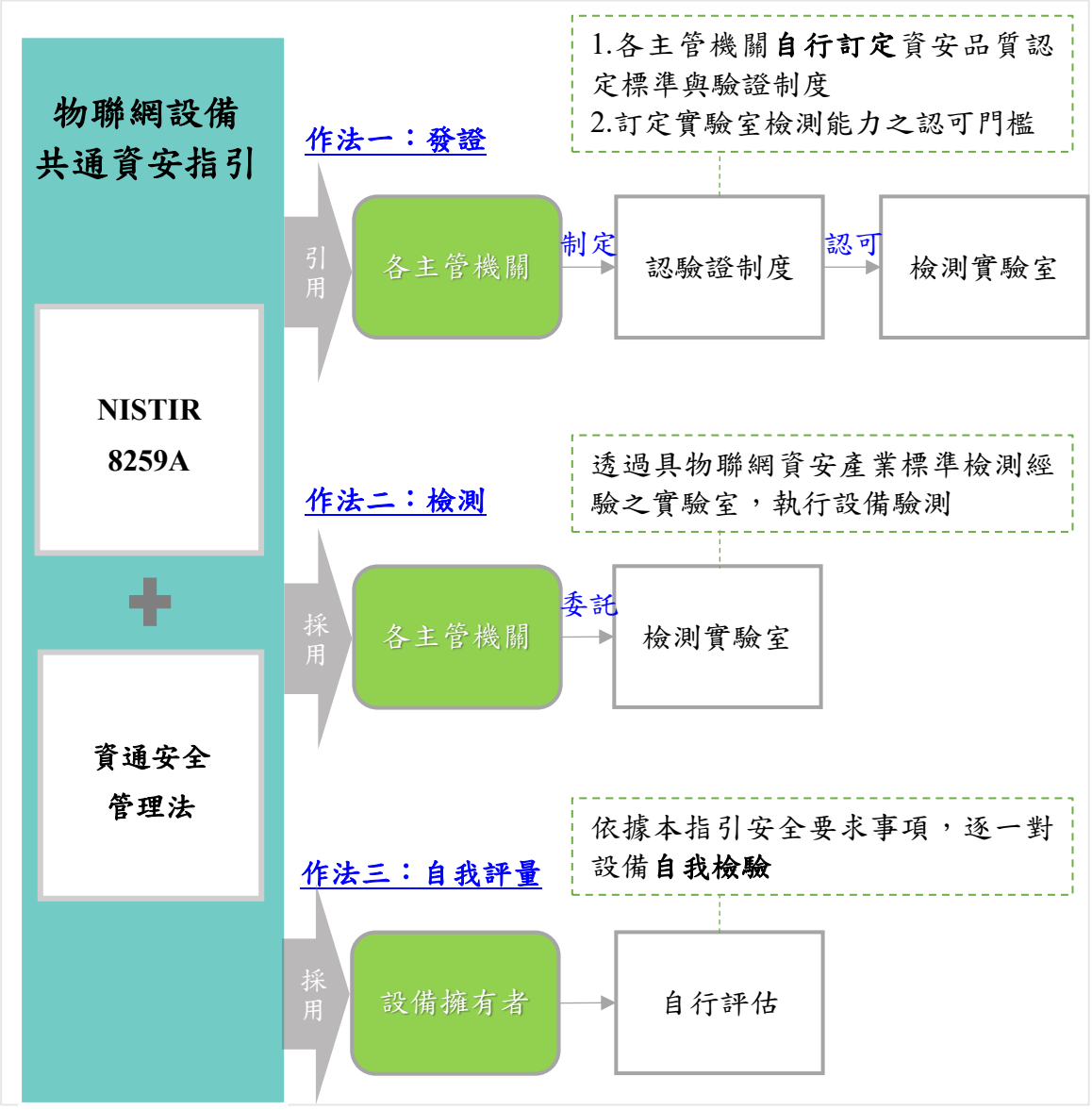

圖 C 1 運用本指引之三種建議作法

一、發證：各主管機關自行引用本指引，制定設備資安認驗證制度，以及對制度範圍內之物聯網設備訂定資安品質標準，包括但不限於檢測實驗室之檢測能力門檻、適用之設備類型、指引中各安全要求之認定標準等。設備檢測通過後，進而取得該主管機關所核發之資安證書。

二、檢測：各主管機關直接採用本指引，委託具備物聯網資安產業標準檢測經驗之實驗室，為其所列管之設備執行資安驗測，並提出驗測報告以茲佐證。例：物聯網資安產業標準認驗證制度所公告之認可檢測實驗室，截至 2023 年已有 11 家認可實驗室。

三、自我評量：設備擁有者(例：設備開發商、設備使用者等)以本指引所要求之安全事項，針對其所擁有之物聯網設備，逐一自我檢驗。目的為了解該項設備是否具備基本資安能力，以利後續的改善與資安品質之升級。例：供應商對其開發之物聯網產品進行資安能力評鑑。

上述作法僅供各單位運用本指引時之參考，若各目的主管機關採用本指引要求事項另有規格要求或施行作法時，應按其規定。

附錄 D
（範例）
資安防護評量表

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
5.1 設備鑑別			
5.1.1 鑑別機制	5.1.1.1 設備應支援讓相連之系統或其他設備進行身分鑑別的能力。		□符合 □不符合 □不適用，請說明：
	5.1.1.2 若設備與其他相連系統或其他設備相連時，應提供唯一識別。		□符合 □不符合 □不適用，請說明：
5.2 設備安全配置			
5.2.1 安全設定	5.2.1.1 設備應具備有關網路及安全組態設定之安全指南，且應提供網路及安全組態設定功能。		□符合 □不符合 □不適用，請說明：
	5.2.1.2 當設備服務中斷或失效後，設備應提供復原至已知安全狀態的能力。		□符合 □不符合 □不適用，請說明：
	5.2.1.3 設備應提供備份功能，且備份過程不能影響產品正常運作，以確保在可容忍時間內恢復正常運作狀態。		□符合 □不符合 □不適用，請說明：
	5.2.1.4 若設備支援遠端遠端連線執行指令功能，設備應具備遠端會話終止(Remote session termination)功能。		□符合 □不符合 □不適用，請說明：
5.3 資料保護			

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
5.3.1 加密功能	5.3.1.1 設備所使用之加密演算法應為國際公認且經安全證實的加密安全機制，例如：NIST SP 800-140Cr1。		□符合 □不符合 □不適用，請說明：
	5.3.1.2 設備所使用之加密金鑰或憑證應具備管理機制，且管理機制應依循國際公認之加密金鑰管理指引之建議，例如：NIST SP 800-57。		□符合 □不符合 □不適用，請說明：
5.3.2 儲存與傳輸資料保護	5.3.2.1 若設備具有儲存、傳輸安全敏感性資料的功能，應對安全敏感性資料提供機密性之保護。		□符合 □不符合 □不適用，請說明：
	5.3.2.2 若設備存在個人資料或敏感性個人資料時，應符合我國個資管理法之規範。		□符合 □不符合 □不適用，請說明：
5.3.3 軟體與資料的完整性	5.3.3.1 設備應提供資料在儲存、使用、傳送及接收時完整性之保護。		□符合 □不符合 □不適用，請說明：
	5.3.3.2 設備應提供完整性檢查及警示功能，以確認設備軟體、組態和資料是否經未授權變更。		□符合 □不符合 □不適用，請說明：
5.4 存取介面			
5.4.1 存取介面安全	5.4.1.1 設備之所有存取介面應提供授權個體身分鑑別機制。		□符合 □不符合 □不適用，請說明：
	5.4.1.2 設備所提供之身分鑑別機制，應支援使用者唯一識別與鑑別之能力。		□符合 □不符合 □不適用，請說明：

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
	5.4.1.3 設備預設遠端存取應關閉；或若設備須開啟遠端存取功能時，應具備授權與鑑別機制。		□符合 □不符合 □不適用，請說明：
	5.4.1.4 設備應防止由實體介面進入除錯模式的功能；若設備須開啟實體介面存取除錯模式時，應具備鑑別機制。		□符合 □不符合 □不適用，請說明：
	5.4.1.5 設備應關閉非必要之管理介面與網路服務。		□符合 □不符合 □不適用，請說明：
	5.4.1.6 若設備支援收集遙測數據時，應提供所使用之網路服務，及收集之遙測數據種類、使用目的，及遙測數據收集和使用之對象。		□符合 □不符合 □不適用，請說明：
5.4.2 通行碼鑑別	5.4.2.1 若設備使用通行碼身分鑑別，設定通行碼長度和強度應根據國際公認通行碼安全指引之建議，例如：NIST SP 800-63B。		□符合 □不符合 □不適用，請說明：
	5.4.2.2 若設備使用通行碼身分鑑別，應具備防止通行碼暴力攻擊之身分鑑別機制，例如：身分鑑別失敗達 5 次後，即鎖定登入。		□符合 □不符合 □不適用，請說明：
	5.4.2.3 若設備使用預設通行碼作為身分鑑別時，應提供每設備唯一通行碼，或強制更改預設帳號(若		□符合 □不符合 □不適用，請說明：

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
	支援）及預設通行碼。		
5.4.3 權限控管	5.4.3.1 若設備不為受限制設備，應提供設定使用者權限與控管的機制。		□符合 □不符合 □不適用，請說明：
5.5 軟韌體更新			
5.5.1 更新安全	5.5.1.1 設備應具備安全更新機制；若為無法更新軟韌體之受限制設備，應提供硬體更換等更新機制。		□符合 □不符合 □不適用，請說明：
	5.5.1.2 若設備支援線上更新軟韌體，應確保傳輸通道的完整性與真實性，所使用之加密演算法應符合 5.3.1.1 之加密演算法。		□符合 □不符合 □不適用，請說明：
	5.5.1.3 若設備支援本地更新軟韌體，安裝更新前應檢驗軟韌體之完整性與真實性，所用之加密演算法應符合 5.3.1.1 之加密演算法。		□符合 □不符合 □不適用，請說明：
5.6 資訊與網路安全狀態			
5.6.1 已知漏洞	5.6.1.1 若設備提供使用者介面，應僅提供沒有可被攻擊利用之錯誤訊息或代碼，例如：無效使用者、通行碼輸入錯誤等明確提示錯誤之處的訊息。		□符合 □不符合 □不適用，請說明：

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
	5.6.1.2 設備不應存在美國國家漏洞資料庫(NVD)所公開的常見弱點與漏洞資料，且漏洞評鑑系統 CVSS v3 嚴重性評等為高。		□符合 □不符合 □不適用，請說明：
5.6.2 安全事件日誌功能	5.6.2.1 設備應提供產生安全事件日誌之功能，安全事件日誌種類應包括但不限於：存取控制、請求錯誤、控制系統事件、備份及恢復事件、組態變更、安全事件日誌事件；若為受限制設備，則應提供補償性作法以達到記錄安全事件之能力。		□符合 □不符合 □不適用，請說明：
5.6.3 日誌管理	5.6.3.1 安全事件日誌之存取應具備權限控管機制。		□符合 □不符合 □不適用，請說明：
	5.6.3.2 安全事件日誌應具備日誌保存期限與儲存容量配置之功能。		□符合 □不符合 □不適用，請說明：
	5.6.3.3 當安全事件記錄失敗時，應根據公認資安產業實務作法作出相對應之處理，例如：日誌滾動(Log rotation)。		□符合 □不符合 □不適用，請說明：
	5.6.3.4 安全事件日誌應具備時間同步之時間戳，且時間戳之格式須一致，例如：ISO/IEC 8601:2019、CNS 7648 之格式。		□符合 □不符合 □不適用，請說明：

安全構面	安全要求	機關/供應商作法說明與佐證資料	檢視結果
5.6.4 安全監控	5.6.4.1 設備應可支援公認資安產業實務作法之安全監控功能，或以補償性作法以達到對設備持續安全監控，例如：支援SNMP、部署 IDS、IPS等。		□符合 □不符合 □不適用，請說明：
	5.6.4.2 設備應具備軟體組成清單(SBOM)，軟體組成清單內容欄位包括但不限於組件名稱、供應商、版本、組件唯一識別碼、與其他組件關聯、建立清單作者。		□符合 □不符合 □不適用，請說明：

參考資料

(1) NISTIR 8259C (Draft)：2020 Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline, https://csrc.nist.gov/publications/detail/nistir/8259c/draft

(2) NIST, National Vulnerability Database, https://nvd.nist.gov/vuln/full-listing

(3) FIRST, Common Vulnerability Scoring System version 3: Specification Document, https://www.first.org/cvss/specification-document

(4) NIST SP 800-140C Rev. 1:2022 CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/final

(5) NIST SP 800-92:2006 Guide to Computer Security Log Management, https://csrc.nist.gov/publications/detail/sp/800-92/final

(6) ISO 8601-1:2019 Date and time — Representations for information interchange — Part 1: Basic rules, https://www.iso.org/standard/70907.html

(7) 行政院，資通安全責任等級分級辦法：附表十 資通系統防護基準，https://www-api.moda.gov.tw/File/Get/3OcL9qFXX69sUwP

(8) 國家資通安全研究所，無線網路政府組態基準說明文件(v1.2)，https://www.nics.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1076

(9) 國家資通安全研究所，Microsoft Windows 10 政府組態基準說明文件(v1.4)，https://www.nics.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1074

(10) 中華民國國家標準 CNS 7648，資料元件及交換格式－資訊交換－日期及時間表示法，https://www.cnsonline.com.tw/?node=result&generalno=7648&locale=zh_TW

版本修改紀錄

版本	時間	摘要
V0.1	2023.04.24	草案
V0.2	2023.05.22	依據專家會議決議修改
V0.3	2023.06.29	依據第二次專家審閱意見修改
V1.0	2023.09.01	草案經 MAS 公告徵詢 1 個月後定版