

第6期

物聯網下供應鏈資安 對於公共建設的價值

毛敬豪 財團法人資訊工業策進
會資安鑄造廠總經理



“ 資安價值展現在於提供信賴穩定的數位轉型基石；而資安信賴將是公務員在進行數位轉型時的核心價值。 ”

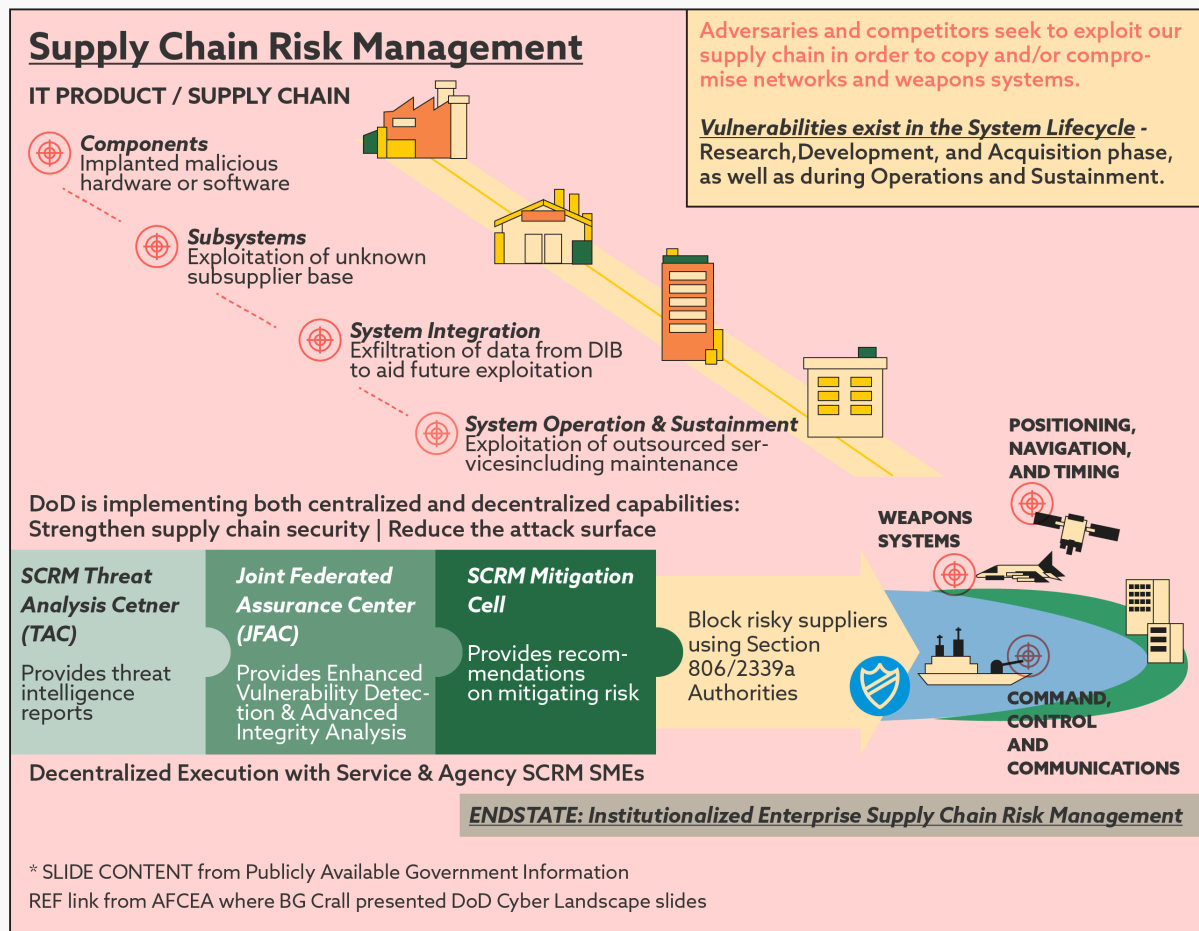
COVID-19疫情改變工作型態，不論公私部門均採取遠距工作或居家辦公模式，打破過去資安實體防護疆界；同時COVID-19也大幅推升網路購物等線上消費型態，在5G與物聯網持續推波助瀾下，垂直領域技術整合所衍生出的資安風險，零信任的資安（Zero Trust）成為重要的關鍵。此外，近年高科技大廠陸續遭駭客勒索，在攻防資訊不對稱下，資安威脅與風險提升，隨著美中貿易戰影響，資訊安全更成為供應鏈信賴重要一環，各個領域資通訊應用在設計階段就須考量國際供應鏈資安規範與檢測機制，而資安價值展現則在於提供信賴穩定的數位轉型基石。

乾淨供應鏈下的資安合規需求

美國於2020年開始，建立全球5G網路加入乾淨網路（clean network），隨著網通設備被運用在重要的場域，尤其是國防軍事用途，美國國防部於2020年1月公布了網路安全成熟度模型認證框架，目的是確保美國國防工業基礎供應鏈中的30多萬家公司，具有足夠能力保護敏感的國防資訊，該框架利用成熟度模型，由第三方

評估人員審核公司的網路安全措施，並訂一個級別，該級別分為五級，一代表該公司已經具備基本的網路保護成熟度。從2020年9月開始美國國防部的計畫書需求中要求承包商獲得網路安全成熟度模型認證（CMMC），其內容涵蓋美國NIST-SP 800-171、NIST SP 800-53、ISO 27001與ISO27032等，框架涵蓋面廣泛且明確，資安的信任完全具體落實在CMMC規範上。其中，CMMC供應鏈資安風險管理，涵蓋從元件、次系統、系統整合與系統運作維運，鑒於整個國防資訊系統、不同次系統、甚至元件，其相關的供應商多元，且管理也頗為複雜，因此整體CMMC框架精神在於實作強化供應鏈資安，並且降低攻擊遭受面向。

圖1 美國CMMC在供應鏈風險管理的視野圖^[1]



資料來源：<https://www.afcea.org/content/cyber-needs-be-integrated-not-treated-uniquely>

資安規範朝向領域化發展

國內外資安檢測規範持續發展中，供應鏈資安考量到領域技術特性，同時考量到軟體安全的需求，也開始發展。例如國內從工業局行動應用APP檢測開始，分別針對物聯網、IP CAM、DVR、車載機、智慧路燈等訂出資安檢測規範與指引^[2]，無論是國內外，產業資安規範已從通用合規規範，落實到各垂直領域，包含醫

療、工控等，而這些規範在政府推動下，除了作為資通安全產業標準外，亦成為供應鏈資安合規檢測的基礎，而檢測基礎的建立則有助於建立整體安全供應鏈的具體評估基礎。

表1 國內物聯網相關檢測基準

標準	現況
工業局APP資安檢測基準	工業局委託資策會針對行動應用APP資安所建立之資安規範與檢測基準，目前已經進入第3年。已經建立完整實驗室與APP認證制度。目前由行動應用資安聯盟維護。
NCC 手機內建軟體資安檢測規範	由NCC發布之手機內建軟體資安檢測規範，針對手機出廠內建軟體的資安檢測規範。目前已公布實驗室與產品認證，2018開始實施。
工業局影像監控系統系列-IP CAM/DVR/NAS 資安標準與檢測規範	2017由工業局委託資策會研擬之IP CAM資安標準，為我國首度研擬之物聯網資安標準。2018開始推動實驗室與產品認證制度。
NCC無人機資安檢測規範	NCC於2018發展之無人機資安檢測規範。
工業局巴士車載機資安標準	工業局於2018年推動之巴士車載機與智慧站牌資安標準。

資料來源：作者自行整理

縱觀國際物聯網、工業控制等檢測規範，規範本質取決於推動單位欲倡議的資安價值，以ISA/IEC組織而言，以工控安全延伸到工控資安的IEC62443^[3]，IEC62443也是從領域驅動的資安合規規範，又例如UL 2900，以物聯網產品安全測試為主，主要以消費者裝置市場為主。從資安領域以威脅角度發展的OWASP IoT Top 10^[4]以及GSMA IoT security guides，皆為物聯網檢測基準的重要關鍵。

表2 國際物聯網資安相關檢測基準與參考指引

標準/指引	目的
ISA/IEC 62443	強化工業控制物聯網元件或系統的安全性、可用性、完整性與保密性，解決工業自動化系統採購資訊安全需求。
OWASP IoT top 10	協助物聯網的製造商、開發者與消費者更佳瞭解IoT資安問題，同時讓各方使用者可以在建置、部署或評估IoT技術時可以做出最好的決策。
UL 2900	美國UL公司發展之物聯網資安標準為連網產品與系統提供網路安全測試準則，以評估軟體漏洞與弱點。並陸續發展成UL資安保障計畫，涵蓋工業控制、醫療設備、汽車、智慧家電等不同範疇產業。
GSMA IoT security guides	提供 IoT 服務從安全設計、開發與測試的最佳實踐，安全措施の評価方法。涵蓋總論，端點，網路與雲端的安全指引。
ISO 15408(CC)	又稱為共通準則，為世界各國進行資通安全產品評估及驗證時所遵循之共同標準，依其定義之評估保證等級(Evaluation Assurance Level, 簡稱EAL)來判定產品之安全等級，EAL共有7個等級提供申請者/贊助者、檢測實驗室與驗證，機關(構)評估及驗證資通安全產品安全性與功能性之依據。

資料來源：作者自行整理

資安信賴是公務員在數位轉型的核心

面對全球經濟劇烈變動和供應鏈加速重組，在5+2產業創新的既有基礎上，打造「六大核心戰略產業」，並透過建立臺灣品牌、提供靈活多元的金融支援、打造安全的產業發展環境、匯聚及培養數位和雙語人才等，讓臺灣成為未來全球經濟的關鍵力量，5G、物聯網、人工智慧、區塊鏈等資訊科技已持續地落實於智慧城市、智慧製造、智慧醫療等垂直領域的應用，資安信賴則是公務員在以資訊科技進行數位轉型時的基礎，供應鏈資安發展趨勢以及物聯網檢測則須考慮**資安成熟度** (maturity)，可在數位科技與政府發展建設中，奠定穩定信賴的數位轉型下創造，而資安信賴將會是公務員在數位轉型發展中的核心價值之一。

[1]Cybersecurity Maturity Model Certification,

<https://www.afcea.org/content/cyber-needs-be-integrated-not-treated-uniquely> 

[2] 台灣資通產業標準協會, <https://www.taics.org.tw/eng/> 

[3] Understanding IEC 62443, <https://www.iec.ch/blog/understanding-iec-62443> 

[4] OWASP IoT Top 10, <https://owasp.org/www-project-internet-of-things/> 

上一篇

回前頁
