

國防供應鏈安全升級戰 - 從*CMMC*合規到自主防衛

Taiwan's Defense Supply Chain Security Upgrade from CMMC Compliance to Self-Reliant Defense

黃希儒
委任資深研究員 備役中將
國防安全研究院

CYBERSEC 2025 臺灣資安大會
中華民國 114 年 4 月 17 日

國防安全研究院
Institute for National Defense and Security Research

美國 *CMMC* 推動政策延續性
- Long Journey of CMMC

November 2010

EXECUTIVE ORDER 13556
NOVEMBER 4, 2010
CONTROLLED UNCLASSIFIED INFORMATION

June 2015

NIST National Institutes of Standards and Technology SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

October 2016

Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.204-7012

May 2016

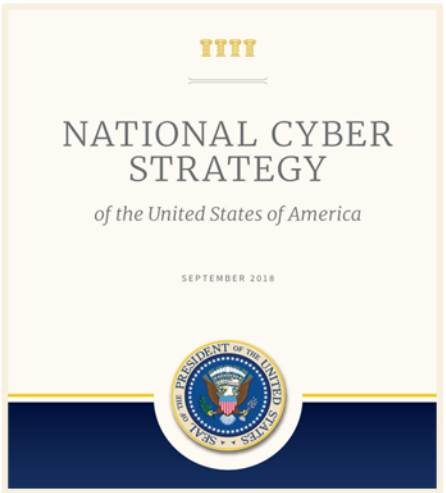
Security Controls
FAR 52.204.21
FCI

Basic Safeguarding of Covered Contractor Information Systems

December 2019

FY20 NDAA, Section 1648
Requires DoD to develop a framework to enhance cybersecurity

September 2018



February 2020

NIST National Institutes of Standards and Technology SP 800-171 R2

January - September 2020

CMMC Model 1.0

- LEVEL 5 ADVANCED — *CUI, critical programs*
- LEVEL 4 PROACTIVE — *Transition Level*
- LEVEL 3 GOOD — *CUI*
- LEVEL 2 INTERMEDIATE — *Transition Level*
- LEVEL 1 BASIC — *FCI only*

December 2020

SolarWinds breaches and the U.S. federal government cyber-espionage incidents

SOLARWINDS SUPPLY CHAIN ATTACK

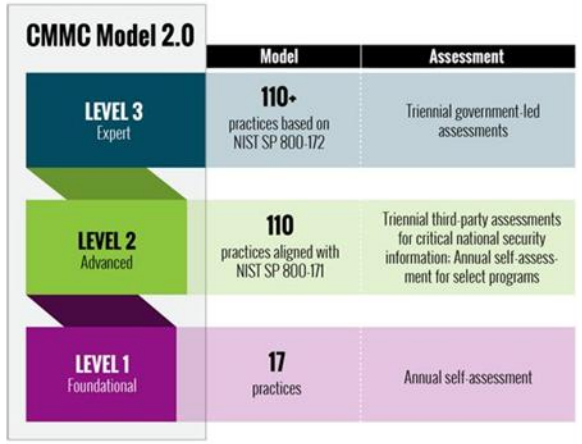
December 2020

FY21 NDAA, Section 1738
Assistance for manufacturers In DIB Supply Chain

FY21 NDAA, Section 1742
Cyber security practices and capabilities in DoD

Barack Obama Administration | *Donald Trump Administration*

美國 *CMMC* 推動政策延續性
- Long Journey of CMMC



November 2021

January - December 2022

Rule making underway *while DIB contractors prepare for CMMC 2.0 requirements*

March 2023

December 2023

32 CFR CMMC 2.0 DFARS rules released for public comment*, along with supporting documentation*

March 2024

January - December 2024

Review public comments on ***32 CFR*** *and* ***48 CFR*** *proposed rules*

32 CFR final rule *has been* ***effective*** *on December 16, 2024*

January - December 2025

CMMC phase 1 rollout begins*, only requiring self-assessment and attestation for all new contracts.*

48 CFR final rule *expected to early* ***mid-2025***

January - December 2026

CMMC phase 2 rollout begins*, requiring third party (certification) assessment requirements introduced at Level 2*

January - December 2027

CMMC phase 3 begins*, requiring Level 2 C3PAO certification for the renewal or extension of existing contracts*

January 2028

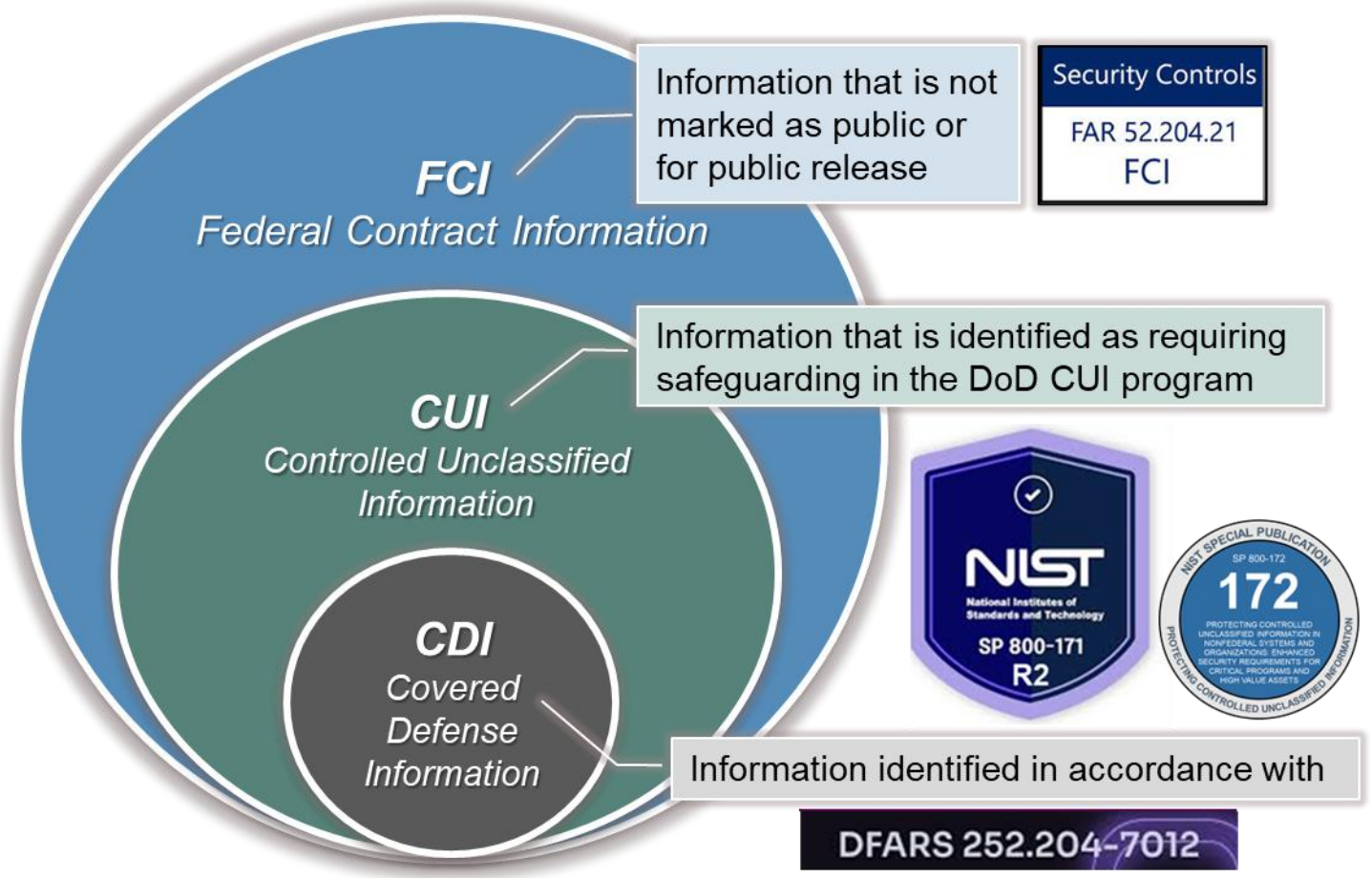
CMMC phase 4 rollout concludes*, with requirements Included in all DoD solicitations and contracts*

Joseph Biden Administration | ***Donald Trump Administration***

美國 *CMMC* 推動現況綜覽

安全政策目標

- 透過一套安全基準與評鑑認證機制，確保存取於非聯邦組織的「受控非具分類保密等級資訊（***Controlled Unclassified Information, CUI***）」與「聯邦合約資訊（***Federal Contract Information, FCI***）受到完整保護；要求所有參與涉有***CUI*** 或***FCI*** 國防供應的主、次合約商，均須取得相對應的網路安全級別認證。
- 針對國防工業基礎（***DIB***）整體供應鏈網攻安全威脅預警、情資分享、事件回報、技術支援及損害控管等，建構政府與業界完整的聯防機制與處置模式。



美國 *CMMC* 推動現況綜覽

法律授權情況

- ***Title 32 CFR*** **- National Defense, *Part 170*《聯邦法規彙編，編目32：國防篇》第170節：**

  「授權」美國防部（DoD）可透過《聯邦採購規則國防增補規定》（*DFARS*）暨其他政策指令，制定*CMMC*框架並對業界進行評鑑與認證（*CMMC Program*）；最終版*CMMC*執行計畫（*final rule*）已於2024年10月15日公告於美國聯邦公報（*Federal Register*）並自同年12月16日起生效。

- ***Title 48 CFR*** **- Federal Acquisition Regulation System, *Parts 204*, *212*, *217* and *252*** 修訂《聯邦法規彙編，編目48：聯邦採購規則體系篇》第 204.75 等節：

  「授權」美國防部（DoD）等聯邦機構可將*CMMC*評鑑與認證需求條件，納入聯邦採購招（決）標程序暨契約條款規範（*CMMC Acquisition Rule*）；此部分擬案，前於2024年8月15日公告並完成公眾意見蒐集，惟最終版迄今尚未定案。美國政府原設定*CMMC*的全面正式施行日，即為此規則定案公布後的60天內，按時程推估概為今（2025）年的第二季。

美國 CMMC 推動現況綜覽

安全認證級別劃分情況

資料來源：整理自美國防部資訊長辦公辦（DoD CIO）網頁，https://dodcio.defense.gov/cmmc/About/

安全級別	維護標的	評鑑者/效期		安全基準/評鑑控制項目		紀錄系統	影響廠家/比例 (合計 22 萬 1,286 家)	
第一級 Level 1	FCI Basic safeguarding	自評	1 年	FAR 52.204-21	15	SPRS	139,201	63%
第二級 Level 2	CUI Broad protection	自評	3 年	• DFARS 252.204-7012 • NIST SP 800-171 R2	110	SPRS	4,000	2%
		C3PAO				eMASS	76,598	35%
第三級 Level 3	CUI Higher-level protection from APT (Advanced Persistent Threat)	DIBCAC	3 年	• DFARS 252.204-7012 • NIST SP 800-171 R2 • NIST SP 800-172	134	eMASS	1,487	1%

- SPRS（Supplier Performance Risk System）指「供應商績效風險系統」；eMASS（Enterprise Mission Assurance Support Service）為「企業任務確保支援服務系統」。
- 除第一級外，餘第二及第三級，未達合規要求評估項目，允許受評廠商有條件提出「改善行動期程管制計畫（POA&Ms）」並於180日之內完成改善（相關條件，參照 32 CFR CMMC 計畫最終規則第 170.21 條）。
- 第二及第三級，無論自評或經C3PAO或DIBCAC評鑑合規認證後，於三年效期內，每年仍須自行驗證（Annual Affirmation）合規保持情況並回饋於系統，若未能及時完成確認，認證將提早失效。

美國 *CMMC* 推動現況綜覽

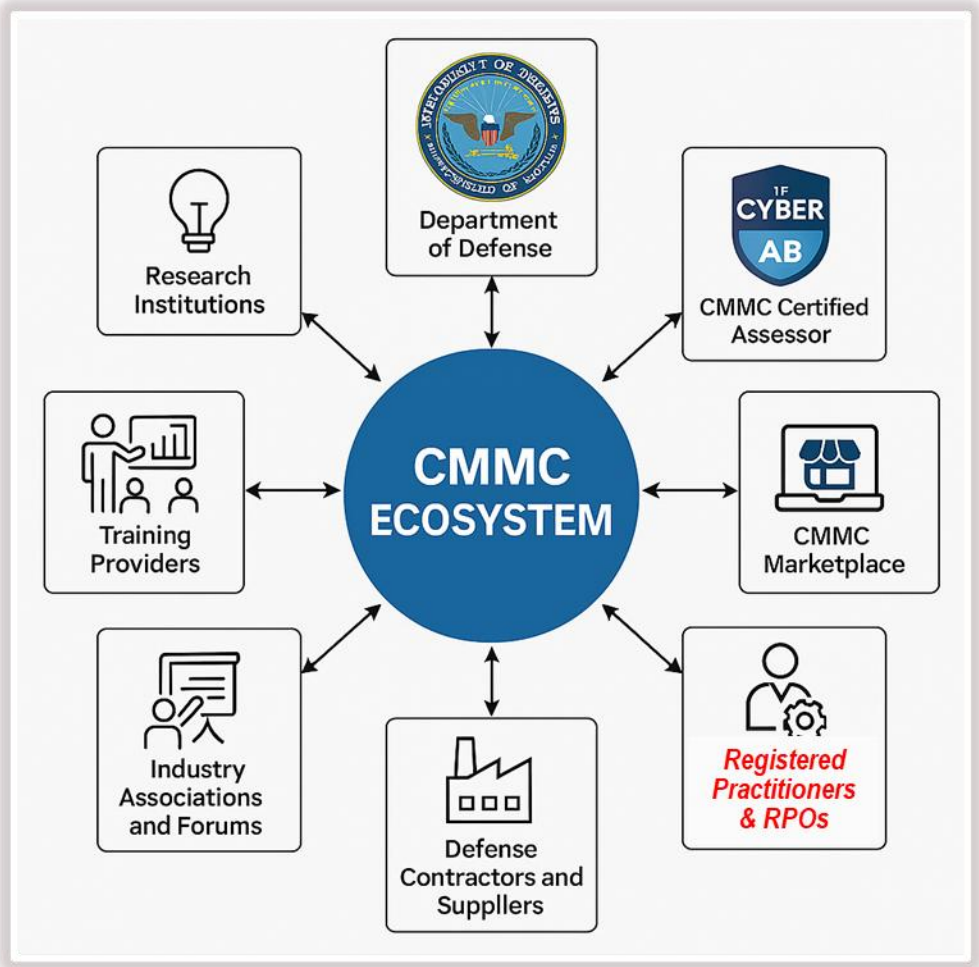
分階段施行規劃

資料來源：整理自美國防部資訊長辦公辦（*DoD CIO*）網頁，*https://dodcio.defense.gov/cmmc/About/*

階段	期程	條件
第一階段	2025 第二季 （假設生效日）	第一級及第二級自評列為採購決標條件 ***L1 and L2 self-assessments as condition of awards***
第二階段	2026年 第一季	第二級C3PAO評鑑列為採購決標條件 ***L2 C3PAO assessments as condition of awards***
第三階段	2027年 第一季	• 第二級C3PAO評鑑擴及至前期已決標合約 ***L2 C3PAO assessments for all option period for previously awarded contracts*** • 第三級DIBCAC評鑑列為決標條件 ***L3 DIBCAC assessments as condition of awards***
第四階段	2028年 第一季	所有適用合約均須符合CMMC相對等級要求條件 ***All contracts and options will have the applicable CMMC requirements***

- 俟*Title 48 CFR*（*CMMC Acquisition Rule*）最終規則生效後，維持三年四個階段施行；其中第一階段係聚焦於要求承包商自我評估的全面實施，第二至四階段，逐步擴及至*C3PAO*及*DIBCAC*評鑑，並將涉及資訊保護要求事項的相對應*CMMC*安全認證級別，納為採購個案招、決標必要條件與契約規範事項。
- 雖是分年、分階段施行，但法律亦授予美國防部（*DoD*）有調整（提前）推行進程權利；因此對於須符合第一、二級自評合規的主、次合約商而言（依前揭統計表約佔 *65 %*），完成整備工作其實均已就緒。

美國 *CMMC* 推動現況綜覽



來源：依***Cyber AB***網頁資訊繪製，*https://cyberab.org/CMMC-Ecosystem/The-Cybersecurity-Ecosystem*

***CMMC*認證成本預估（*Estimated Costs*）**

Level 1 - 自評約 ***$4,000***美元（每年）

Level 2 - 自評 ***$48,827***至***$104,670***美元（每3年，含兩年度自我確認）

- *C3PAO*認證 ***$104,670***至***$117,768***美元（每3年，含兩年度自我確認）

Level 3 - *DIBCAC*認證***$12,802***至***$44,445***美元（每3年，含兩年度自我確認）

資料來源：美國聯邦公告（***Federal Register***）***CMMC Program Final Rules & Regulations,*** *https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program*

美國 *CMMC* 推動現況綜覽

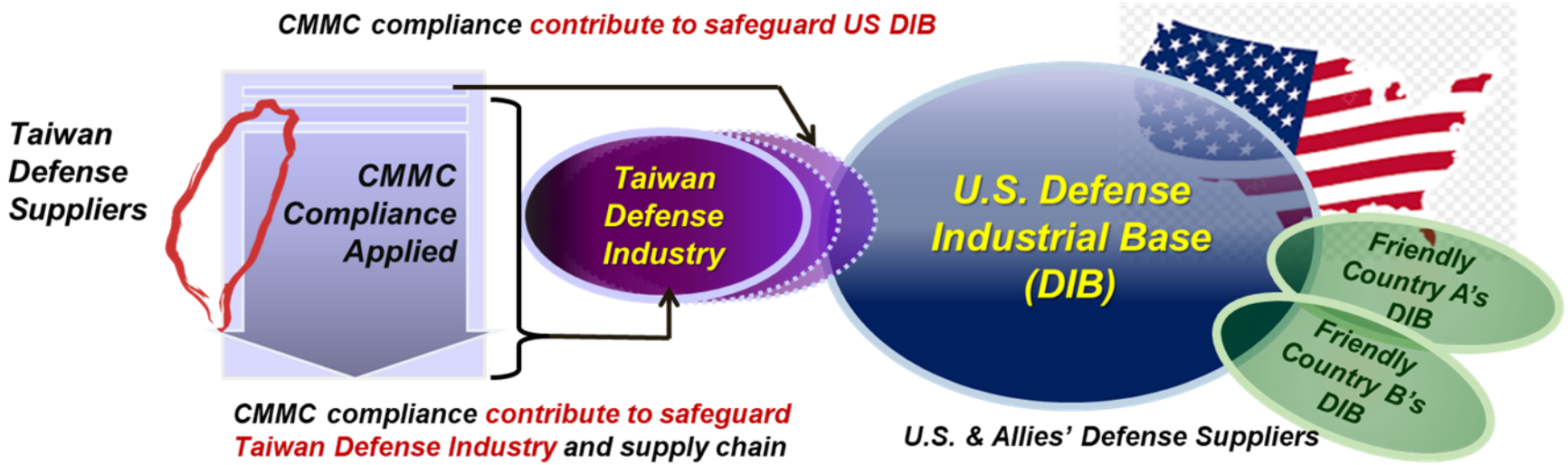
其他待關注發展

- ***CMMC***評鑑方法與安全標準，預判很快將漸次擴及至聯邦總務署（*GSA*）、國土防衛部（*DHS*）、能源部（*DOE*）、太空總署（*NASA*）等其他美國政府聯邦部門。
- 美政府一方面投入大量資源暨人力進行國防供應鏈網安建設、認證與管控；另一方面，亦擔憂繁複的資安評鑑認證程序、標準暨過高的合規成本，恐阻礙國內、外企業的持續參與，限縮未來商源多樣性與競爭力的發展。
- 配合*CMMC*針對供應鏈安全威脅預警、事件回報與損害管控，國防網路犯罪防制中心（*DC3*）、國防反情報暨安全局（*DCSA*）暨國家安全局（*NSA*）整合執行的「國防工業基礎網路安全計畫（*Defense Industrial Base Cybersecurity Program*）」及其運作平台「國防工業基礎資訊分享整合環境（*DoD-DIB Collaborative Information Sharing Environment, DCISE*）」聯防機制，相關具體作為，待進一步探究。
- 未來***CMMC***若結合零信任（*Zero Trust*）架構及人工智慧（*AI*）監測技術發展，進階強化供應鏈防禦，*CMMC 2.1* 或甚至 *3.0* 更新版本與相關安全標準，將應勢而生。

臺灣的挑戰與策略建議

合規

接軌DIB國防供應鏈商機



- ***Awareness*** ***vs Compulsory*** 主動認知或被動要求
- ***Complexity*** ***of standards*** **–** ***NIST vs ISO*** 標準複雜程度
- ***define CUI & its boundary*** 受控非分類保密資訊定義
- ***SSP & continuous monitoring*** 系統安全計畫暨持續改善
- ***Cost & learning curve*** 學習成本曲線
- ***cost effective Approaches for Life-cycle*** 全壽期方案
- ***Cloud + Enclaves*** 雲端暨安全隔離處理

establishing resource sharing platform
建構官網數位平台暨知識、案例分享資料庫

forming a compliance expert support team
整合政府民間資源，成立合規專家支援團隊

prioritizing potential compliance partners
盤點優先輔導對象，主動提供國防採購商機

formulating subsidy & incentive measures
制定政府輔導補助計畫與獎（激）勵措施

臺灣的挑戰與策略建議

臺灣因戰略政治地緣暨在全球科技供應鏈重要角色，加上敵對頻次密集的文攻武嚇與網路攻擊，使國防產業與相關高科技供應鏈，面對情蒐、竊取，甚至破壞的安全威脅未曾間斷。

- 95% 屬「資安入門生」仍欠缺安全意識與防護作為
- 5%「資安中等生」勉符合國際標準惟仍難擋APT

來源：財團法人工業技術研究院2021年盤點調查
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9772

2016 資安即國安1.0 **2021 資安即國安2.0**

國家資通安全戰略2025

- 供應鏈攻擊、鎖定關鍵基礎設施的破壞行動為「國家級資安威脅與挑戰」
- 「關鍵產業與供應鏈安全」列屬為「國家資通安全」四大根基之一

來源：黃彥棻，〈在全社會防衛的基礎上打造國家資安韌性_國家資通安全戰略2025即將正式公布〉，2025年3月14日，*iThome*
https://www.ithome.com.tw/news/167864

自主防衛

建構國防
供應鏈
安全韌性

- 以建構自主國防供應鏈安全防衛體系與韌性為前提，採取積極策略，發展一套肆應臺灣整體安全環境，符合本土國防暨高科技產業實需的供應鏈管控機制與資安標準。
- 即參酌美國推展*CMMC*及他國仿效建立類同機制歷程，藉鼓勵接軌盟友邦國防工業供應鏈契機，同步發展臺灣版*CMMC*。

- 整體國防供應鏈威脅與產業安全環境評估
- 安全保護目標資訊 *CUI* 的明確定義
- 適用法規與安全標準的審視與制定
- 政府與民間資安專業資源與聯防機制整合

臺灣的挑戰與策略建議（結語）

- *Tariff War* 貿易保護主義再起
- *Integrated DIB vs Buy America* 整合供應鏈變成國貨優先
- *Friend-shoring vs on-shoring supply* 友岸外包變成在岸供應
- *Technical source control & CUI boundary as Supply Chain Boundary* 重新定義的供應鏈邊界

Capability 能力		*Security* 安全
■ 技術 *Technical* ■ 品質 *Quality*	✚	■ 完整性 *Integrity* ■ 互信 *Mutual Trust*

因應國際地緣政治安全環境的局勢變化，臺灣須致力找到屬於國防與相關高科技產業供應鏈可同時在「能力（*Capability*）」與「安全（*Security*）」昇級的具體方案與續航力。

Thank you

國防安全研究院
Institute for National Defense and Security Research