# 供應鏈資安防護與趨勢

提報單位：漢翔公司

會議日期：112年11月28日

主講人： 資訊處 方一定 處長

# 目　錄

# 壹、資安威脅與事件從未中斷過

## 世界經濟論壇(WEF)2023全球風險報告

2022~2023 年全球風險報告中皆指出**網路犯罪的威脅日益嚴重**，其中包括**供應鏈攻擊**等，通常會給組織帶來數千萬甚至數億美元的損失。

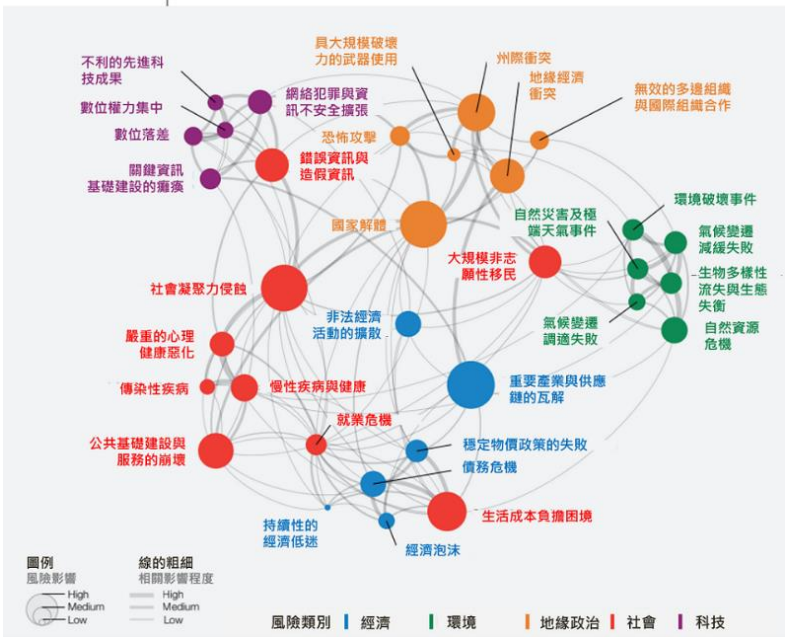
### 未來短期與長期全球風險感知排名

依影響嚴重程度評估未來2年及10年內的十大風險

| | 未來2年內 | 未來10年內 |
|---|---|---|
| 1 | 生活成本負擔困境 | 氣候變遷減緩失敗 |
| 2 | 自然災害及極端天氣事件 | 氣候變遷調適失敗 |
| 3 | 地緣經濟衝突 | 自然災害及極端天氣事件 |
| 4 | 氣候變遷減緩失敗 | 生物多樣性流失與生態系統失衡 |
| 5 | 社會凝聚力侵蝕及兩極化 | 大規模非志願性移民 |
| 6 | 大規模環境破壞事件 | 自然資源危機 |
| 7 | 氣候變遷調適失敗 | 社會凝聚力侵蝕及兩極化 |
| 8 | 網絡犯罪與資訊不安全的擴張 | 網絡犯罪與資訊不安全的擴張 |
| 9 | 自然資源危機 | 地緣經濟衝突 |
| 10 | 大規模非志願性移民 | 大規模環境破壞事件 |

風險類別 | 經濟 | 環境 | 地緣政治 | 社會 | 科技

FIGURE C 全球風險格局：風險關聯圖




https://rsprc.ntu.edu.tw/zh-tw/m01-3/en-news/1775-1120323-wef.html

# 漢翔 遭網路勒索病毒攻擊的企業，日益嚴重

## 曾勒索台積電供應商22億 波音、名古屋港全遭LockBit毒手

根據**趨勢科技**統計，今年**上半年遭網路勒索病毒攻擊**的企業、組織，**較去年下半年增加47%**，勒索軟體組織LockBit 就佔了26%。

這個具有俄羅斯背景的駭客組織最新盯上的目標，竟是中國最大銀行-中國工商銀行在美子公司，害慘中國工銀緊急拿出90 億美元（約台幣2907 億），支付拖欠美國梅隆銀行的款項。今年年中還曾爆出勒索台積電供應商擎昊科技7000 萬美元（約台幣22.6 億），美商波音及日本名古屋港也慘遭LockBit 下毒手。

全球資安拉警報，台灣2023上半年的惡意威脅數量急遽成長。（Fortinet提供）

Lockbit會先竊走組織資料並予以加密，若不給付贖金就將資料公布於TOR暗網上，這導致資料恐被競爭者買走，Lockbit藉此達到雙重威脅，台灣超過一半的攻擊就是來自Lockbit。

**波音則在今年11月2日坦言，駭客取得內部資料**，正配合執法機構調查，並通知客戶及供應商。LockBit 聲稱擁有這家飛機製造商的大量敏感資料，並使用了零日漏洞來存取資料，但沒有具體說明從波音竊取多少數據，也沒有提供贖金的詳細資訊。

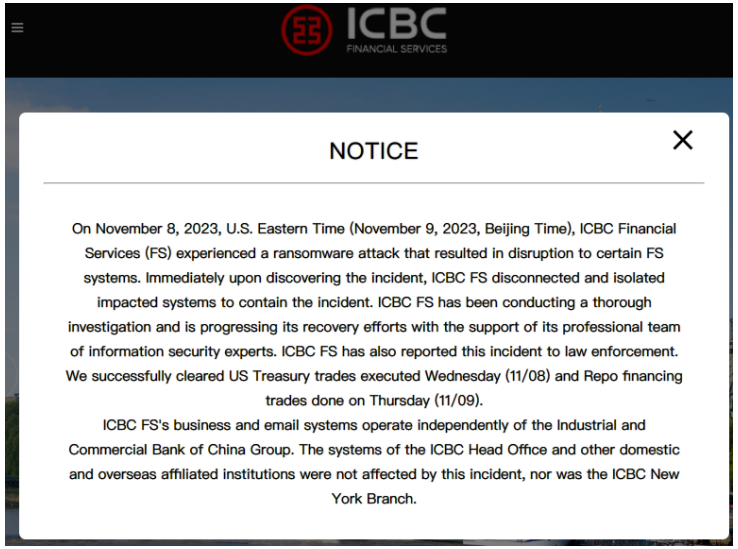


自由時報(發布日民國112 年11 月12 日)

# 漢翔 遭網路勒索病毒攻擊的企業，日益嚴重

## ICBC遭勒索軟體LockBit鎖定Citrix Bleed漏洞發動攻擊

從11月8日以來，勒索軟體駭客LockBit再度因為攻擊**中國工商銀行（ICBC）**而登上媒體版面，他們之所以攻入這家公司的關鍵，是未修補Citrix NetScaler設備的漏洞Citrix Bleed（CVE-2023-4966，CVSS風險評分為9.4）




該漏洞8月下旬就遭到利用，已有政府機關與科技業者受害，隨後Citrix證實該漏洞被用於攻擊行動的情形。但究竟還有多少伺服器尚未套用更新程式？Kevin Beaumont指出，截至11月14日，仍有大約5千個組織尚未修補Citrix Bleed。

Lockbit利用Citrix Bleed入侵目標企業，並部署遠端管理工具，以便後續接手的攻擊者能持續存取網路環境，而這一組人員會再利用各種手法提升權限，擺脫EDR系統控制、竊取資料，最終部署勒索軟體將檔案加密。

# 貳、航太供應鏈資安合規要求

## 一、航太產業與國防二大資安評級

**航太與國防供應鏈Exostar管理平台，2大驗證要求。**

**1.Cybersecurity Questionnaire**
**(供應商網路安全控制自評問卷)**

**2.NIST SP 800-171 Cybersecurity Compliance Questionnaire(美國國防承包商和分包商網路安全自評問卷)**

Exostar公司於2000年由波音、洛克希德•馬丁、雷神、BAE及R&R等航太大廠合資成立，主要提供航太產業的供應鏈管理及網路協同平台。

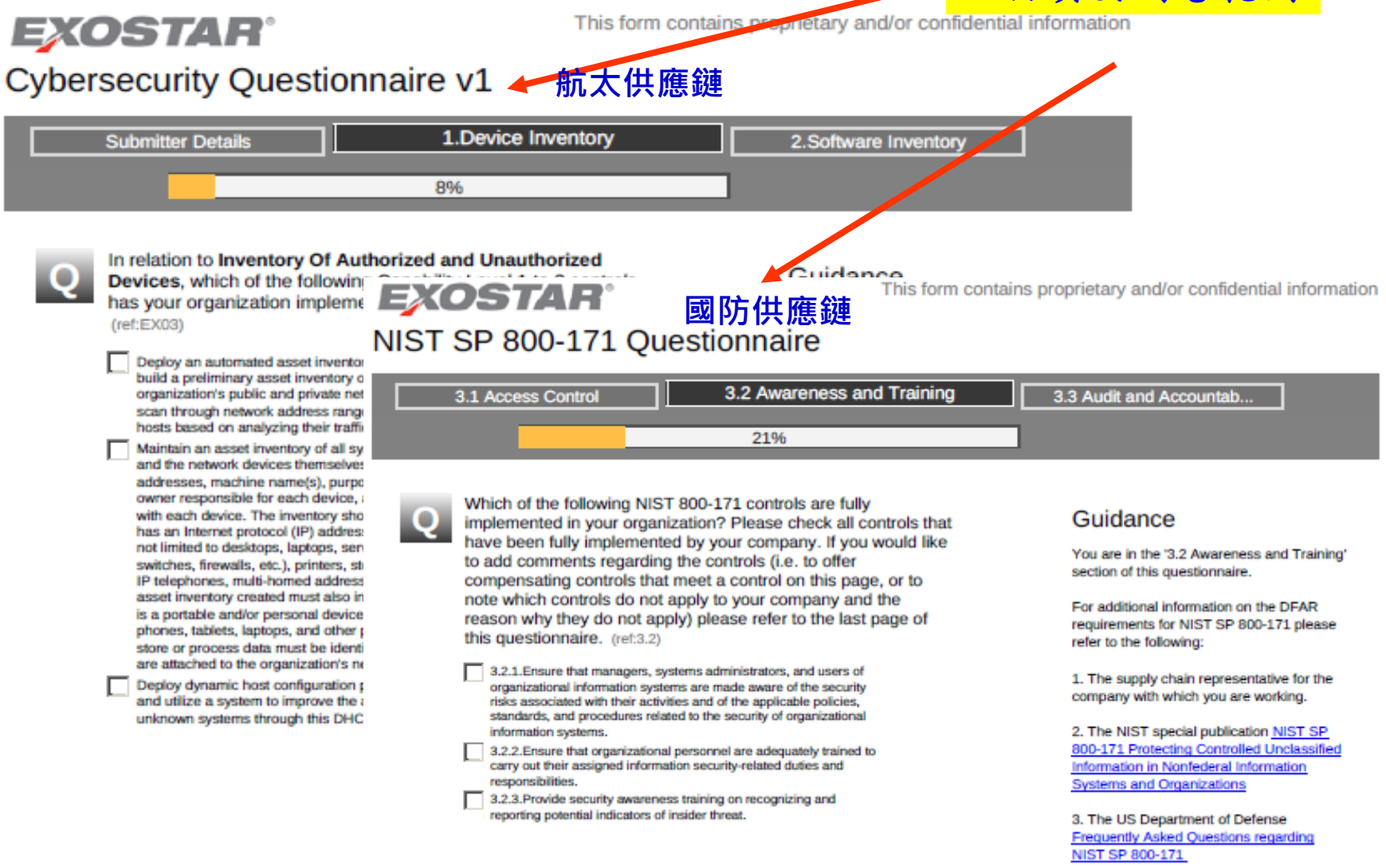
NIST：the National Institute of Standards and Technology(美國國家標準與技術研究所)

SP 800-171：規定如何保護非聯邦資訊系統和機構中受管制的非保密資訊 (CUI) 之安全，並定義了實現這項目標所需遵循的安全性規範。

# 貳、航太供應鏈資安合規要求

## 一、航太產業與國防二份資安問卷

二份資安問卷範例



# 貳、航太供應鏈資安合規要求

## 二、航太產業資安評級

**Cybersecurity Questionnaire**：採用美國系統與網路安全協會（SANS Institute）CIS Critical Security Controls（CIS CSC)

1.分成22項控制群組，包含194個控制項。

2.各個控制措施對應不同的網絡安全能力級別(Capability levels)，從0級到5級定義如下：

| | |
|---|---|
| **Level 0** | Indicates no or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigations must be implemented |
| **Level 1** | Indicates a basic level cyber risk management program; some protections in place but additional risk mitigations must be implemented |
| **Level 2** | Indicates a moderate level cyber risk management program; good protections in place but additional risk mitigations are required to protect sensitive information |
| **Level 3** | Indicates a solid performing cyber risk management program; strong protections have been implemented; Advanced threats are understood and taking steps to address with specific controls; Additional risk mitigations are likely needed to protect against advanced attacks |
| **Level 4** | Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented |
| **Level 5** | Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; Specific advanced controls are implemented and optimized on an ongoing basis |

# 貳、航太供應鏈資安合規要求

參考國際資安組織SANS 發布資安控制項目指引 ( CSC, Critical Security Controls)：22控制項群組，194控制項

| Control Family | Control Number | Total Controls |
|---|---|---|
| Device Inventory | CSC 1 | 7 |
| Software Inventory | CSC 2 | 9 |
| Secure Configurations | CSC 3 | 10 |
| Assess/Remediation | CSC 4 | 10 |
| Malware Defenses | CSC 5 | 11 |
| In-house SW Security | CSC 6 | 9 |
| Purchased SW Security | CSC 6a | 5 |
| Wireless Access | CSC 7 | 10 |
| Data Recovery | CSC 8 | 4 |
| Skills/Training | CSC 9 | 5 |
| Network Devices | CSC 10 | 6 |
| Network Controls | CSC 11 | 7 |
| Admin Privileges | CSC 12 | 14 |
| Boundary Defense | CSC 13 | 13 |
| Audit Logs | CSC 14 | 10 |
| Controlled Access | CSC 15 | 4 |
| Account Monitoring | CSC 16 | 17 |
| Data Protection | CSC 17 | 15 |
| Incident Management | CSC 18 | 7 |
| Network Engineering | CSC 19 | 4 |
| Penetration Tests | CSC 20 | 8 |
| Governance | CSC 21 | 6 |
| Mobile Device | CSC 22 | 3 |

SANS :System Administration, Networking and Security

# 貳、航太供應鏈資安合規要求

## 三、美國國防供應鏈資安問題日增，已影響國安

產品風險

2018因海康威視監視器產品有淪為間諜工具之虞陸軍基地全數拆除

承商風險

2018中國從承包商處竊取了敏感的美國海軍潛艇計畫

承商風險


2021美方指控中國大陸透過下游承包商竊取洛馬的 F-35 技術，以建造先進的 J-31 戰機

1. 來自國外對立方 、 產業競爭方和國際犯罪分子等對美國國防部( 供應鏈的全球網路攻擊是美國國家安全關注的首要議題 。

2. 美國國防部負責採購事務的副部長 **Ellen Lord** 指出： 中國大陸 、俄羅斯和朝鮮等國家向美國竊取資訊已造成超過 **6000** 億美元佔全球 **GDP** 的 **1%** 的損失

資料來源：SIPRI 、 LBMC ；網路媒體、資策會資安所

# 貳、航太供應鏈資安合規要求

## 四、美國如何在採購流程包含資通訊安全

美國總統拜登2021 年 發布了 14017 及 14028 號行政命令 EO 14028 重點在於改善國家的網路安全 。 其中 14028 命令專注於**透過採購流程來確保資通安全**特別是針對軟體供應鏈的安全性

### 1. FAR (Federal Acquisition Regulation)

美國政府採購的主要法規，各政府機構購買和租賃商品和服務時**將資通安全標準納入合約中確保承包商和供應商符合要求** 。 指定使用**特定的加密技術** 、 **網路安全措施**或其他安全標準 。

### 2. DFARS (Defense Federal Acquisition Regulation Supplement)

補充FAR 的規定專門針對**美國國防部的採購活動** 。 DFARS 252.204-7012 是具體針對受控非機密資訊 Controlled Unclassified Information, **CUI 的保護要求並要求供應商遵循 NIST SP 800-171 標準** 。

### 3. CMMC (Cybersecurity Maturity Model Certification)「 網路安全成熟度模型驗證 」

重視上下游供應鏈業者的資訊服務和生態安全性

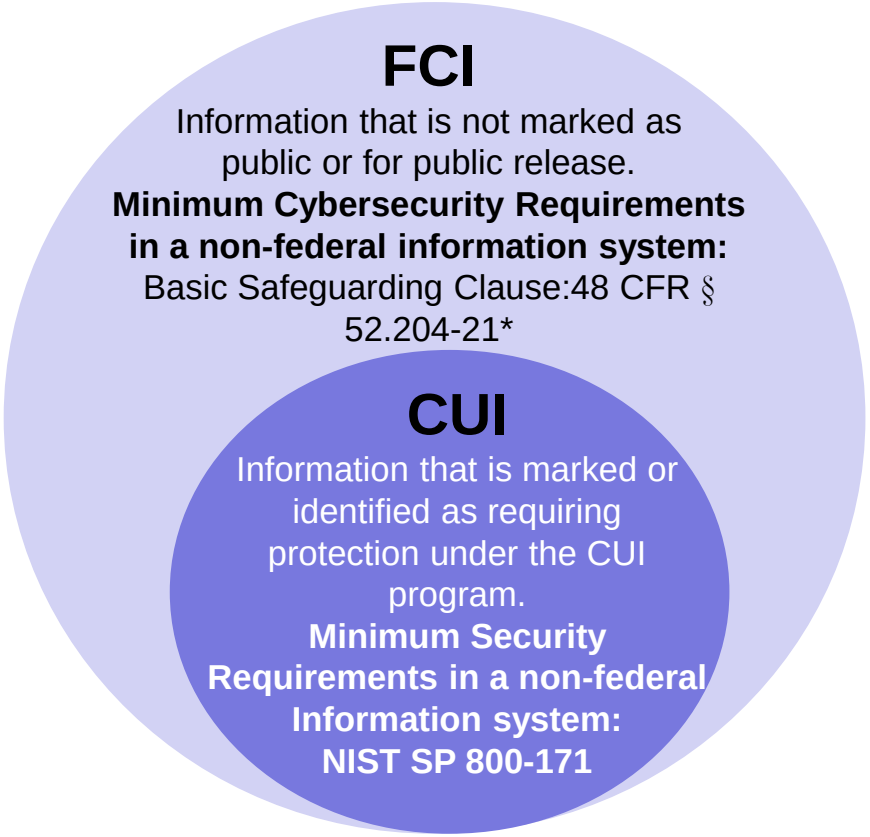
重視網路安全實踐和運營過程的成熟度 CMMC要求**國防承包商和分包商符合相關的驗證級別後並經過第三方審核機構的驗證才能進入美國國防供應鏈並承包其業務** 。

# 貳、航太供應鏈資安合規要求

## 五、美國防DoD DFARS/CMMC 資安評鑑標準

**加強保護聯邦合約資訊（Federal Contract Information，FCI），以及更進一步保護受控的非機密資訊（Controlled unclassified information，CUI）。**




### FCI：聯邦政府的合約資訊

- 來自 48 CFR 52.204-21
- 非公開發布的政府合約相關資訊，如交貨期、時程表等或依合約交付政府的資訊

### CUI:受控的非機密資訊

- 來自32 CFR 2002.4
- 未被列為機密但屬不能公開的敏感資訊
- 如果洩露這些資料,可能會顯示漏洞或給對手帶來優勢,從而對國家安全產生負面影響
- 包括: 法律資料/知識產權/**技術圖紙/藍圖**·國際武器貿易條例(ITAR)控制的文件/產品

## 五、美國防DoD DFARS-7012/CMMC 2.0 資安評鑑標準

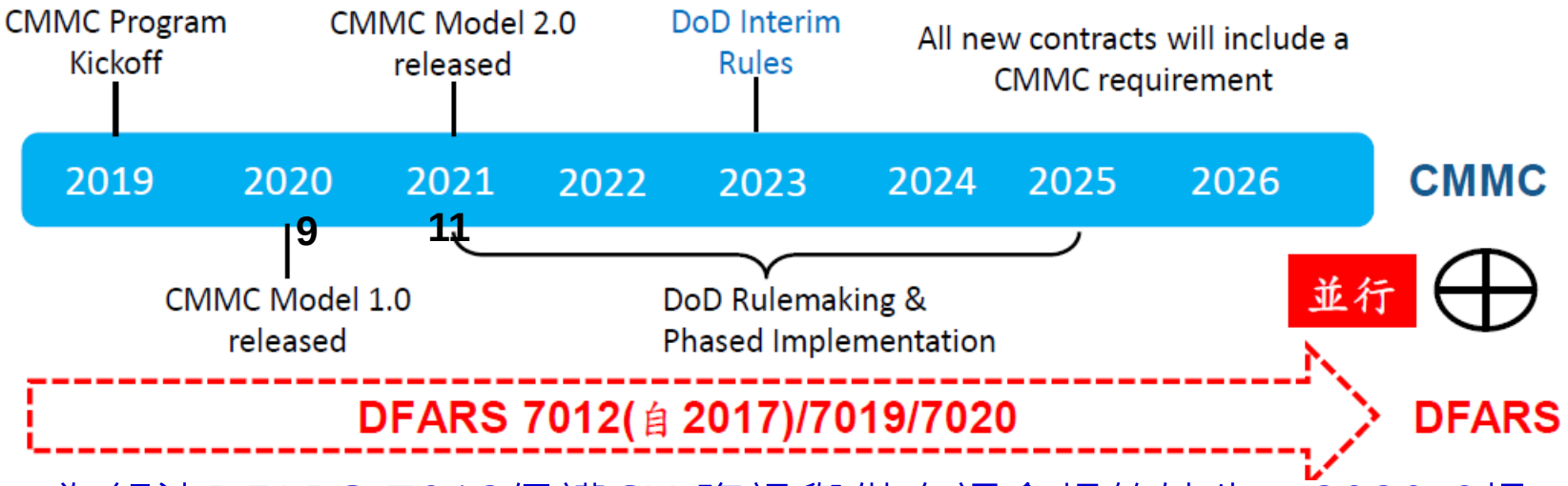
- **二者均採用NIST SP 800-171**
- 規定如何**保護**非聯邦資訊系統和機構中受控的非機密資訊(CUI)之安全，並定義了實現這項目標所需遵循的安全性規範。
- 14控制項群組，110控制項。

| Family | Family |
|---|---|
| 1.AC : Access Control 存取控制 | 8.MP：Media Protection 媒體保護 |
| 2.AT：Awareness And Training 認知與訓練 | 9.PS：Personnel Security 人員安全 |
| 3.AU：Audit and Accountability稽核與可歸責性 | 10.PE：Physical Protection 實體保護 |
| 4.CM：Configuration Management組態管理 | 11.RA：Risk Assessment 風險評估 |
| 5.IA：Identification and Authentication識別和鑑別 | 12.CA：Security Assessment 安全評估 |
| 6.IR：Incident Response事故應變 | 13.SC：System and Communications Protection 系統和通訊保護 |
| 7.MA：Maintenance維護 | 14.SI：System and Information Integrity 系統和資訊完整性 |

# 貳、航太供應鏈資安合規要求

## 五、美國防DoD DFARS-7012/CMMC 2.0 資安評鑑標準

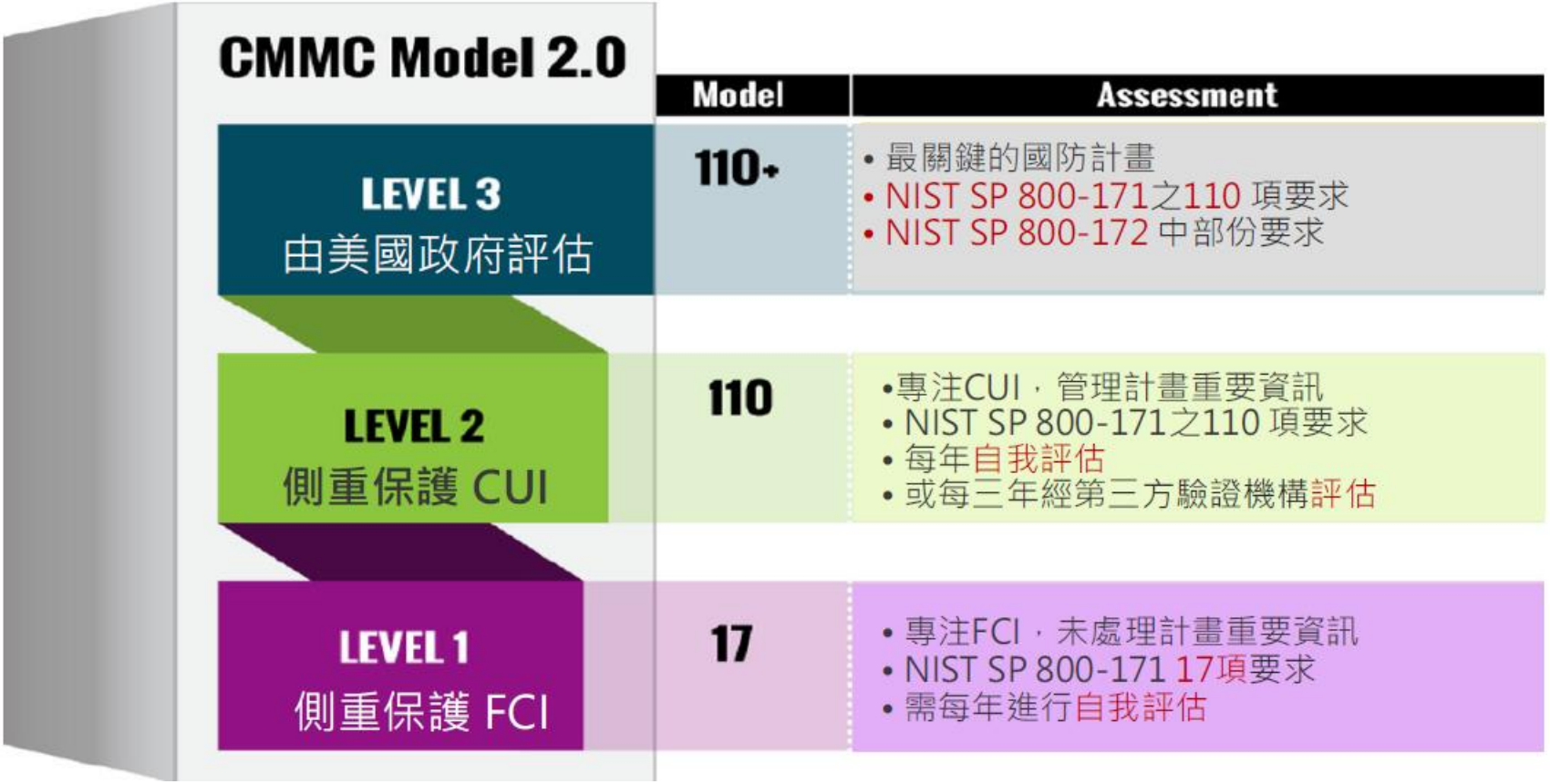



1. 為解決DFARS-7012保護CUI資訊與僅自評合規的缺失，2020-9提出CMMC 1.0框架，於2021-11 CMMC 2.0，框架中包含自評、第三方評鑑與政府主導評鑑。CMMC防護的標的包含聯邦合約資訊(FCI)與受控的非機密資訊(CUI)

2. 依美國國防部CMMC 2.0法制化最新訊息，預估2023年12月底前完成(最快2023/9)所有規則制定要求，將在2026財年（2026年9月30日）時，規範所有新的國防部採購案（合約）都將納入CMMC的要求。

# 貳、航太供應鏈資安合規要求

## CMMC 2.0 模型介紹




NIST SP 800 171 r2 : Assessing Security Requirements for Controlled Unclassified Information 評估受控非機密資訊的安全要求

NIST SP 800 172 : Enhanced Security Requirements for Protecting Controlled Unclassified Information 受控非機密資訊的進階安全要求

# 漢翔參、漢翔通過LM/DCMA資安合規經驗

## 一、LM兩份資安問卷AIDC自評歷程

2016/11/26

洛馬(LM)通知填2份資安問卷
1.供應商網路安全控制自評問卷
2.美國國防承包商和分包商網路安全自評問卷 NIST SP 800-171

2019/11/13

洛馬(LM)針對兩份問卷召開2次技術討論電話會議逐項進行驗證，認定符合洛馬(LM)公司資安要求。

2020起

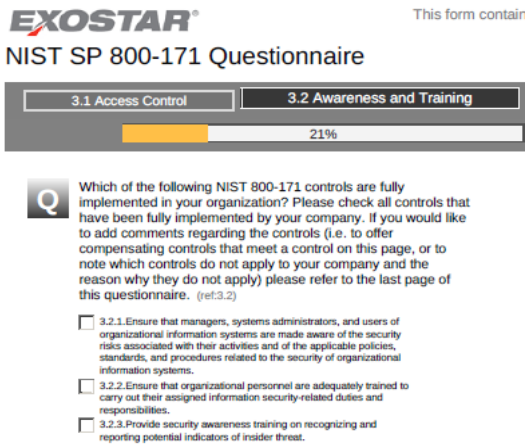
洛馬(LM)供應商網路安全自評問卷納入採購流程中

2020/10/30

針對DFARS 7012條款和CMMC認證要求自評公司資安現況

2021/3/18

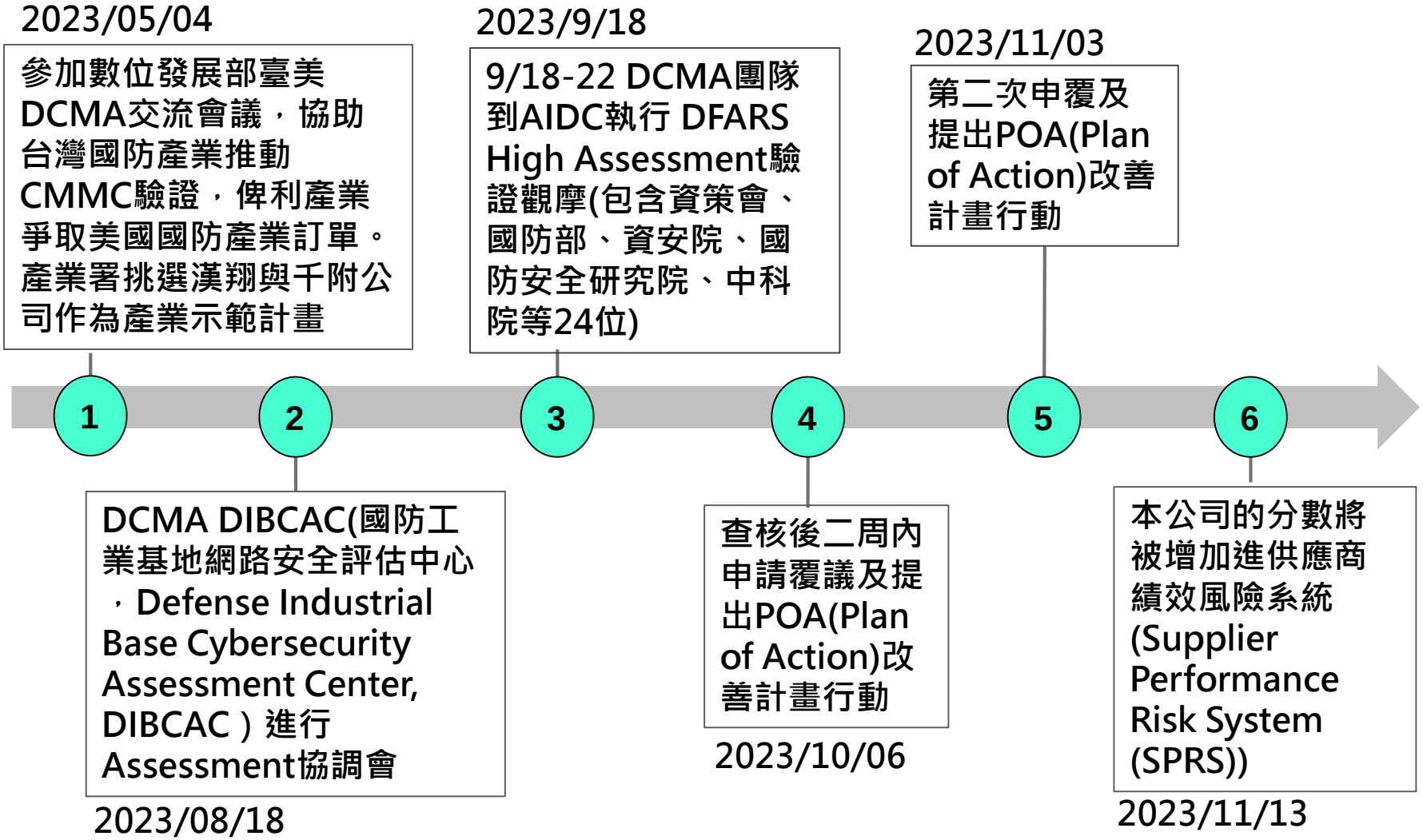
完成NIST SP 800-171資安自評更新，並於SPRS上傳更新分數




SPRS : Supplier Performance Risk System (檢索供應商和產品[性能信息] 評估的權威來源，供 DoD [國防部] 採購用於識別、評估和監控未分類的性能

# 漢翔參、漢翔通過LM/DCMA資安合規經驗

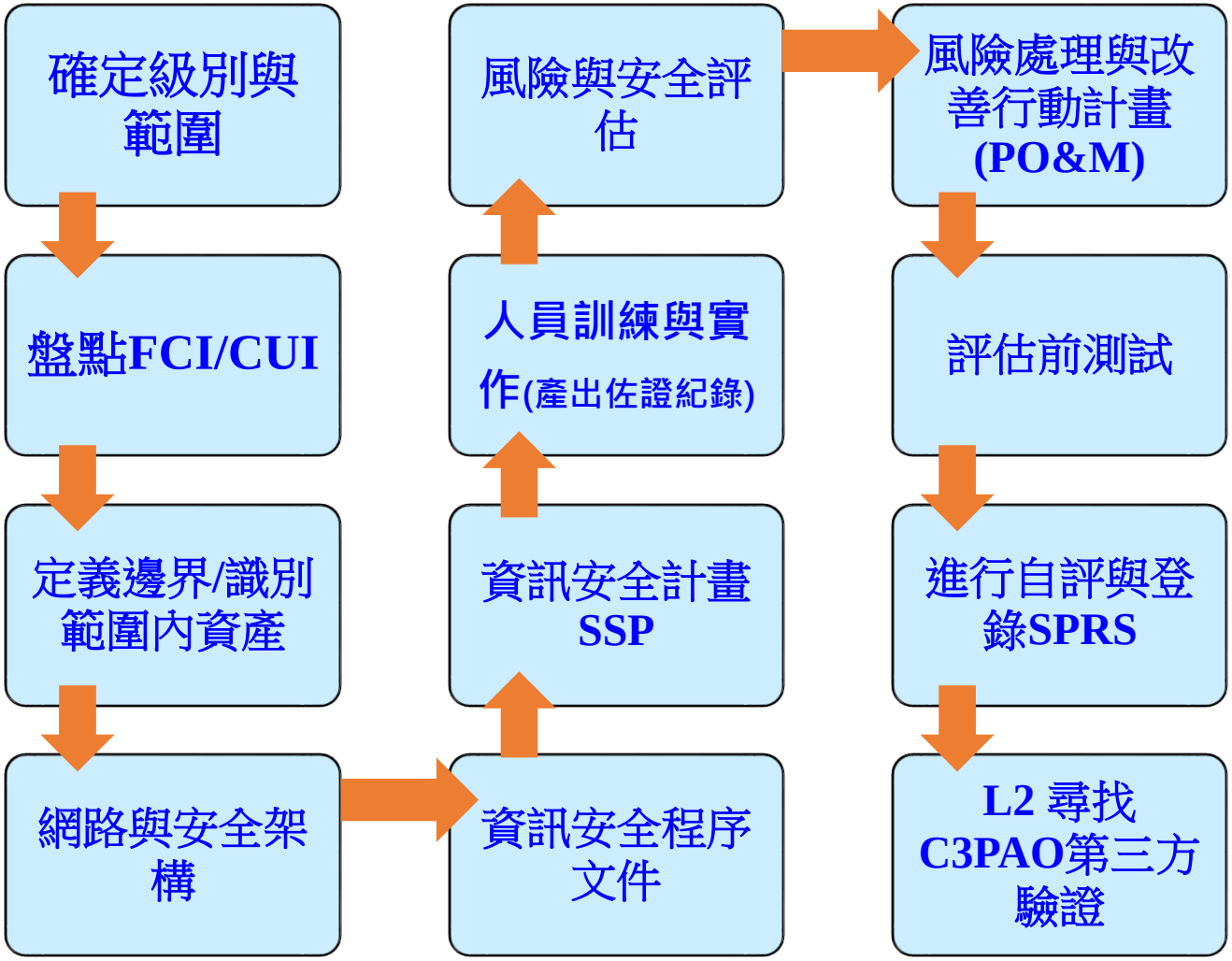
## 二、DCMA DFARS 7012 High Assessment驗證觀摩



# 漢翔參、漢翔通過LM/DCMA資安合規經驗

## 三、如何準備與通過CMMC驗證



# DoD Assessment Methodology

## NIST 800-171 & NIST800-171A

| AC | AT | AU | CM | IA | IR | MA | MP | PS | PP | RA | SA | SC | SI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3.1.1* | 3.2.1 | 3.3.1 | 3.4.1 | 3.5.1* | 3.6.1 | 3.7.1 | 3.8.1 | 3.9.1 | 3.10.1* | 3.11.1 | 3.12.1 | 3.13.1* | 3.14.1* |
| 3.1.2* | 3.2.2 | 3.3.2 | 3.4.2 | 3.5.2* | 3.6.2 | 3.7.2 | 3.8.2 | 3.9.2 | 3.10.2 | 3.11.2 | 3.12.2 | 3.13.2 | 3.14.2* |
| 3.1.3 | 3.2.3 | 3.3.3 | 3.4.3 | 3.5.3 | 3.6.3 | 3.7.3 | 3.8.3* | | 3.10.3* | 3.11.3 | 3.12.3 | 3.13.3 | 3.14.3 |
| 3.1.4 | | 3.3.4 | 3.4.4 | 3.5.4 | | 3.7.4 | 3.8.4 | | 3.10.4* | | 3.12.4 | 3.13.4 | 3.14.4* |
| 3.1.5 | | 3.3.5 | 3.4.5 | 3.5.5 | | 3.7.5 | 3.8.5 | | 3.10.5* | | | 3.13.5* | 3.14.5* |
| 3.1.6 | | 3.3.6 | 3.4.6 | 3.5.6 | | 3.7.6 | 3.8.6 | | 3.10.6 | | | 3.13.6 | 3.14.6 |
| 3.1.7 | | 3.3.7 | 3.4.7 | 3.5.7 | | | 3.8.7 | | | | | 3.13.7 | 3.14.7 |
| 3.1.8 | | 3.3.8 | 3.4.8 | 3.5.8 | | | 3.8.8 | | | | | 3.13.8 | |
| 3.1.9 | | 3.3.9 | 3.4.9 | 3.5.9 | | | 3.8.9 | | | | | 3.13.9 | |
| 3.1.10 | | | | 3.5.10 | | | | | | | | 3.13.10 | |
| 3.1.11 | | | | 3.5.11 | | | | | | | | 3.13.11 | |
| 3.1.12 | | | | | | | | | | | | 3.13.12 | |
| 3.1.13 | | | | | | | | | | | | 3.13.13 | |
| 3.1.14 | | | | | | | | | | | | 3.13.14 | |
| 3.1.15 | | | | | | | | | | | | 3.13.15 | |
| 3.1.16 | | | | | | | | | | | | 3.13.16 | |
| 3.1.17 | | | | | | | | | | | | | |
| 3.1.18 | | | | | | | | | | | | | |
| 3.1.19 | | | | | | | | | | | | | |
| 3.1.20* | | | | | | | | | | | | | |
| 3.1.21 | | | | | | | | | | | | | |
| 3.1.22* | | | | | | | | | | | | | |

- ✓ CMMC 2.0 要求，參照 NIST SP 800-171 要求，共計 14 個 Domain 、 110 項控制措施
- ✓ 執行面需參考NIST SP 800-171A的320項評估目標AO，認證稽核的檢查要點更是發展到 975項，而所有的控制、檢查都是前後呼應環環相扣的
- ✓ 算分：基本分110分，不符合項扣分，最低 -203分

| Must Do (SSP) | 5 | 5 or 3 | 3 | 1 |
|---|---|---|---|---|

*** FAR 52.204.21 /CMMC Level 1**

# 漢翔 3.14 SYSTEM AND INFORMATION INTEGRITY

| | | |
|---|---|---|
| **3.14.1** | **SECURITY REQUIREMENT** 識別、報告、糾正系統缺陷<br>Identify, report, and correct system flaws in a timely manner. | |
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.14.1[a]** | *the time within which to identify system flaws is specified.* |
| | **3.14.1[b]** | *system flaws are identified within the specified time frame.* |
| | **3.14.1[c]** | *the time within which to report system flaws is specified.* |
| | **3.14.1[d]** | *system flaws are reported within the specified time frame.* |
| | **3.14.1[e]** | *the time within which to correct system flaws is specified.* |
| | **3.14.1[f]** | *system flaws are corrected within the specified time frame.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records].<br>**Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility].<br>**Test:** [*SELECT FROM:* Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates]. | |

# L2：SSP資訊安全計畫撰寫範例

**3.14 System and Information Integrity**
**SI.L1-3.14.1**
**Identify, report, and correct system flaws in a timely manner.**
及時識別、通報和矯正系統缺陷。

## 公司作法說明

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

1. 依公司《CUI資料安全管控操作程序》為確保CUI內相關資訊資產的安全，**每月對CUI內所有資訊資產進行漏洞掃描**。漏洞掃描完成後，如果有嚴重漏洞，在**三天內**使用電子管理表單的「主機漏洞掃描處理清單」將漏洞資訊通知系統管理員，開始修補系統漏洞，並**30天內完成漏洞修補**。
2. 期限內無法完成漏洞修補的，後續修補流程計畫或其他加強系統漏洞防護的資訊安全保護措施須經單位主管說明並批准。
3. 根據《電腦設備安全防護工作指引》Windows更新，公司擁有自己的WSUS主機。所有伺服器主機和使用者電腦都設定為自動更新系統，並由專人負責檢查和處理更新。故障或無法自動更新的電腦，依據《電腦設備安全防護工作細則》處理
4. 公司收到**資訊安全相關情資**後，資訊安全人員認定該情資對公司構成資訊安全風險時，則執行**資訊安全風險處置計劃**，將資訊安全處置計劃記錄《電腦系統操作記錄》中，並經單位主管批准後，進行資訊安全風險處置。風險處理完成後，將風險處理結果記錄在《電腦系統操作記錄》中，並提交給單位主管核閱。

# L2：SSP資訊安全計畫撰寫範例

每個控制項下，會有不同的**評估目標AO**小項須提供佐證資料，以證明符合

| 控制說明與<br>評估目標(AO) | 符合度 | 可提供之證明<br>available proof |
|---|---|---|
| 3.14.1[a] **規定識別**系統漏洞的**時間期限**。 | I | 參考公司CUI資料資安管控作業規定-弱點掃瞄執行**規定每月掃瞄一次** |
| 3.14.1[b] 在規定的時間範圍內辨識系統漏洞。 | I | CUI範圍內資產，**每月掃瞄一次，完成辨識系統漏洞** |
| 3.14.1[c].**規定通報**系統漏洞的**時間期限**。 | I | 參考公司CUI資料資安管控作業規定-弱點掃瞄執行3天內將漏洞資訊通知系統管理員 |
| 3.14.1[d] 在規定的時間範圍內通報系統漏洞。 | I | 查看“電腦運作紀錄”是否有通報 |
| 3.14.1[e] **規定矯正**系統漏洞的**時間期限**。 | I | 30天內**完成漏洞修補** |
| 3.14.1[f] 在規定的時間範圍內矯正系統漏洞。 | I | 查看“電腦運作紀錄”是否有完成修補 |

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

# L2：SSP資訊安全計畫撰寫範例

**IA.L2-3.5.3**

**Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.對特權帳號的本地和網路存取以及對非特權帳號的網路存取使用多因子身份驗證。**

## 公司作法說明

☒ Implemented ☐ Planned to be Implemented ☐ Not Applicable

特權帳號公司使用CyberArk，非特權帳戶使用虛擬桌面基礎設施（VDI）存取CUI

- ✓ 建置僅供內部使用的VDI平台，提供MFA多重身分驗證
- ✓ 設定防火牆僅允許VDI網段存取CUI（F16VES）

| 控制說明與評估目標 | 符合度 | 可提供之證明 available proof |
|---|---|---|
| 3.5.3[a] 特權帳號已被識別。 | I | 特權帳號清冊 |
| 3.5.3[b] 對特權帳號的本地存取實施了多因子身份驗證。 | I | 特權帳號本地存取認證MFA畫面 |
| 3.5.3[c]為特權帳號的網路存取實施了多因子身份驗證。 | I | 特權帳號的網路存取認證MFA畫面 |
| 3.5.3[d]對非特權帳號的網路存取實施了多因子身份驗證。 | I | 非特權帳號的網路存取認證MFA畫面 |

# 漢翔 最常發生：前十項未符合(OTS)之要求

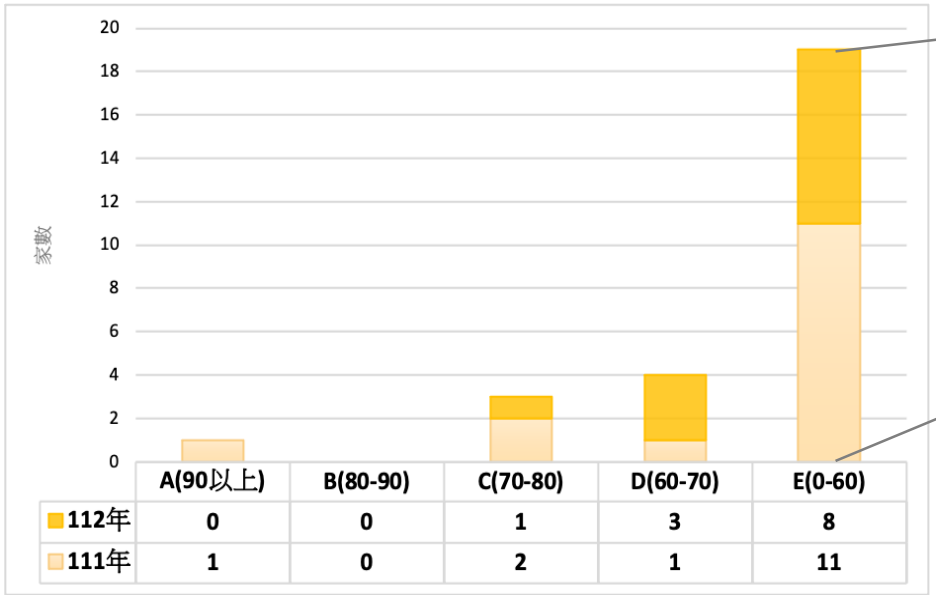
1) 3.13.11 *FIPS 驗證的加密* [系統和通信保護 (SC)]
2) 3.5.3 *多因素認證* [身份認證(IA)]
3) 3.14.1 *識別、報告、糾正系統缺陷* [系統和資訊完整性(SI)]
4) 3.11.1 *定期評估風險* [風險評估(RA)]
5) 3.11.2 *掃描漏洞* [風險評估(RA)]
6) 3.3.3 *查看和更新記錄的事件* [審計與問責(AU)]
7) 3.3.4 *審計日誌流程失敗警報* [審計與責任(AU)]
8) 3.3.5 *審計紀錄審查、分析和報告流程* [審計與問責制 (AU)]
9) 3.6.3 *測試事件響應能力* [事件響應（IR)]
10) 3.4.1 *建立/維護基線配置* [配置管理 (CM)]

註： OTS：Other than satisfied

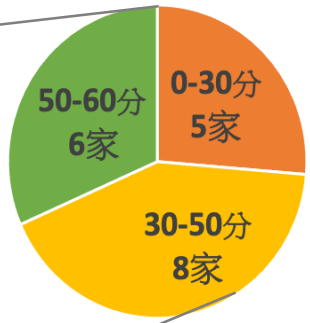
 

# 肆、漢翔推動供應鏈資安聯防計畫

## 一、持續推動航太公會與A-Team4.0成員參加數發部產業署資安SIG計畫：SECPASS資安評級




| | A(90以上) | B(80-90) | C(70-80) | D(60-70) | E(0-60) |
|---|---|---|---|---|---|
| 112年 | 0 | 0 | 1 | 3 | 8 |
| 111年 | 1 | 0 | 2 | 1 | 11 |




分數級距調整說明 V2023.05

| 分數 | 級距 before 2023.05.12 | 分數 | 級距 from 2023.05.12 |
|---|---|---|---|
| 90-100 | A | 90-100 | A |
| 75-90 | B | 80-90 | B |
| 40~75 | C | 70~80 | C |
| 20-40 | D | 60-70 | D |
| 0-20 | E | 0-60 | E |

- 111年開始直至112年有**27家航太相關廠商進行企業評級**。
- 資安加強勢不可擋，作答171題過程中，檢視資訊安全相關流程及做法，協助資訊人員**掌握資安現況及缺口**。
- 分數級距對照去年度有所調整較為嚴苛，藉由分析建議評估風險，企業能夠討論解決風險之優先順序並規劃改善。
- 完成改善後再次進行問卷複測，走向良好循環，逐步接軌國內外資安規範。

## 二、協助供應商瞭解外部資安風險評等

漢翔透過**企業資安風險評等**服務（Security Rating Services），以及**供應商風險管理工具**(Security Scorecard軟體)，以非侵入性的方式，從外部網路監看公司的資安風險及瞭解委外第三方供應商的安全狀況


分析各個企業的10大風險類別，包括

1. 網路安全（Network Security）
2. DNS健康狀況（DNS Health）
3. 漏洞修補（Patching Cadence）
4. 端點安全（Endpoint Security）
5. 惡意IP連線信譽評等（IP Reputation）
6. 應用程式安全（Application Security）
7. Cubit score
8. 駭客情資（Hacker Chatter）
9. 資訊洩漏（Information Leak）
10. 社交平臺分析（Social Engineenring）

漢翔

# 肆、漢翔推動供應鏈資安聯防計畫

1. AIDC SecurityScorecard綜合性分數99、評級等級A
2. 每月挑選5家供應鏈廠商，協助瞭解其資安成熟度
3. 計畫將資安風險評估分數列入廠商合作條件之一

| COMPANY | V1 | V2 | V3 | V4 | V5 | V6 | V7 | V8 |
|---|---|---|---|---|---|---|---|---|
| GRADE | D | D | B | B | A | A | C | B |
| PERCENTILE | 69 | 69 | 82 | 87 | 91 | 95 | 74 | 82 |
| APPLICATION SECURITY | F | F | F | D | D | B | F | F |
| CUBIT SCORE | A | A | A | A | A | A | A | A |
| DNS HEALTH | A | A | A | A | A | A | A | A |
| ENDPOINT SECURITY | A | A | A | A | A | A | A | A |
| HACKER CHATTER | A | A | A | A | A | A | A | A |
| IP REPUTATION | A | A | A | A | A | A | A | A |
| NETWORK SECURITY | F | F | A | A | A | A | D | C |
| INFORMATION LEAK | A | A | A | A | A | A | A | A |
| PATCHING CADENCE | A | A | A | A | A | A | A | A |
| SOCIAL ENGINEERING | A | A | A | A | A | A | A | A |

## 三、漢翔備便CMMC 2.0 Level 2 驗證

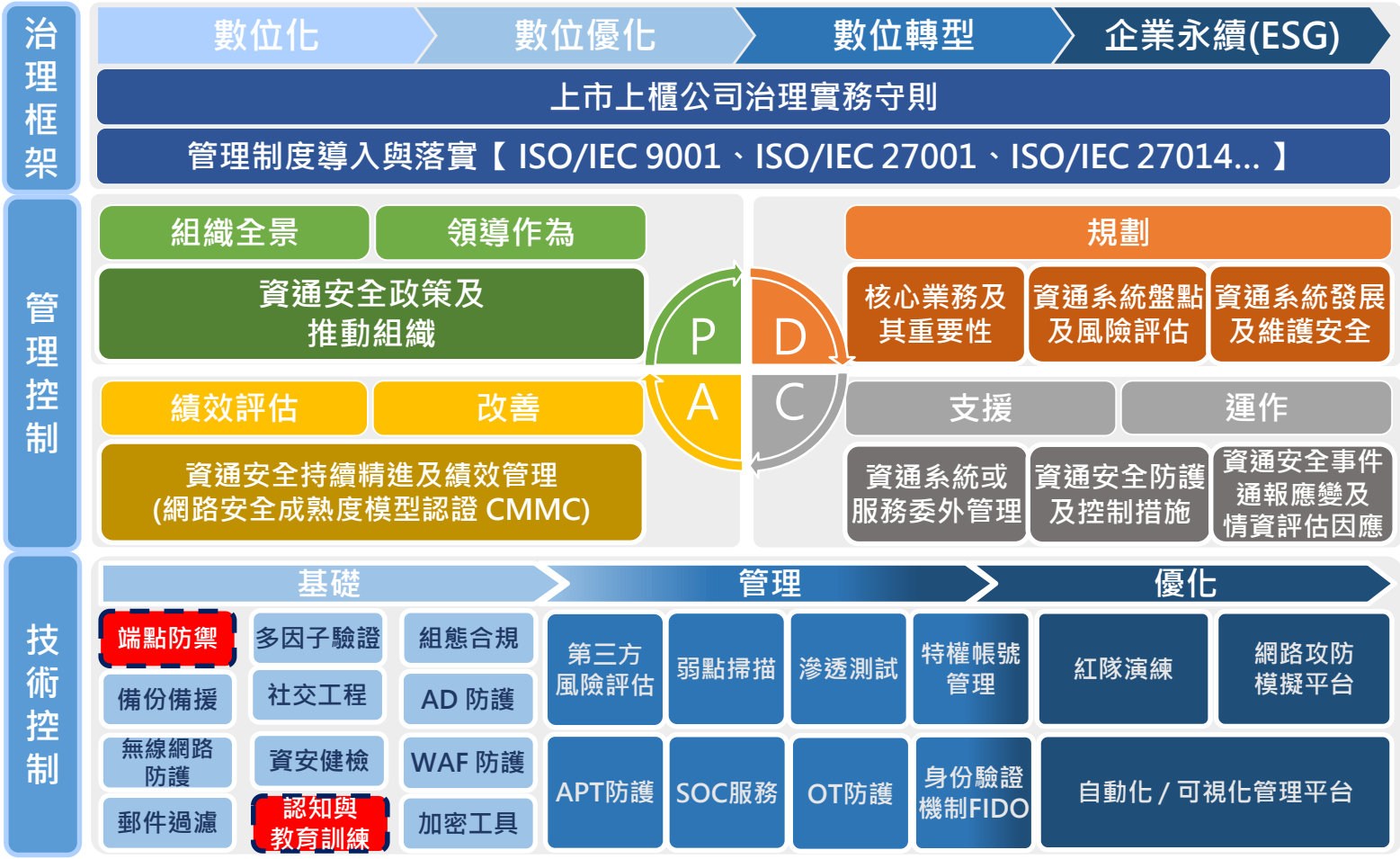
1. 美國將在2026財年（2026年9月30日）時，規範所有新的國防部採購案（合約）都將納入CMMC的要求。

2. 漢翔目前已通過DFARS 7012(NIST SP 800-171)自評與覆核，但因CMMC 2.0 Level 2 第三方C3PAO驗證會更嚴謹，因此配合數位發展部產業署協助台灣產業推動CMMC，美國防部合約管理局DCMA已於9/18-22前來漢翔執行DFARS High (等同CMMC Level 2)稽核驗證觀摩。

3. 另外數位發展部委託資策會成立輔導團及偕同台中市電腦同業公會，以漢翔及F16維修中心6家供應商為範疇，辦理「國防供應鏈體系資安合規專案輔導」以作為未來推動到國內航太供應鏈通過CMMC驗證之參考

# 四、漢翔具備完整資安服務能量，可提供各企業資安輔導與諮詢服務

## 公司資安治理藍圖



# 伍、總結

## 以「預想被駭」強化資安偵測應變能力

**頂尖網路攻擊者**

Apex Attacker：如名列**網駭五大寇**（Big Five）的中國、蘇聯、北韓、伊朗與網路犯罪集團

**頂尖網路攻擊手法**

1. 利用**零時差漏洞發動攻擊**，或在軟體漏洞被揭露後，於一日內就能發動攻擊；他們也已採用軟體開發框架，有系統、有規模地開發惡意程式與攻擊軟體。
2. 採取寄生攻擊（Live off the Land）手法，運用作業系統內建合法程式進行滲透，有效躲避資安軟體偵測
3. 混淆入侵行徑的網路連線、命令控制系統等發動攻擊所需的基礎設施，以掩飾其真實身分，逃避究責
4. 隨著資訊科技快速發展，需要資安防護的領域越來越多，而且資訊系統肩負越來越多重要功能，系統架構也變得日益龐大且複雜，導致攻擊面大幅增加，然而，需要資安防護的系統變多了，但資安人員卻嚴重短缺，跟不上防護需求。

**資安新思維**

**現行資安防護無法阻擋駭客入侵已是必然趨勢**，強化第二道資安防線：偵測、應變與控制的能力，升級至現代化資安防禦架構已成為關鍵。

https://www.ithome.com.tw/news/159828

# 感謝聆聽