Supply Chain Provenance[1]

How ITAR and CMMC is supported by Lockular's NFT Marketplace platform

Gary Mawdsley CTO/CEO Lockular Limited

April 2024

[1] Facilitated by Lockular's NFT Marketplace platform

This document outlines how US standards of ITAR and CMMC for US defence contractors are addressed using a Lockular NFT marketplace.

ITAR restricts the export of defense-related articles and services.

What are ITAR and CMMC

ITAR

ITAR has significant implications for the operations of material suppliers to the US defense industry:

- Registration Requirement: Suppliers to the defense and space sectors involved in manufacturing or exporting items listed on the United States Munitions List (USML) must register with the Directorate of Defense Trade Controls (DDTC) to comply with ITAR regulations.
- Export Controls: ITAR restricts the export of defense-related articles and services. Any products or technologies that are classified under the USML must obtain the appropriate export licenses before transferring these items to foreign entities or nationals. This includes physical products, technical data, and even certain types of verbal or electronic communications.
- Technical Data Controls: ITAR controls not only physical goods but also technical data related to defense articles, including blueprints, drawings, photographs, plans, instructions, or documentation. Sharing this technical data with foreign nationals (even within the same company or on U.S. soil) is considered an export under ITAR and requires authorization.
- Supply Chain Management: Suppliers must ensure that their entire supply chain complies with ITAR regulations. This includes vendors, subcontractors, and partners who might come into contact with ITAR-controlled articles or data. Due diligence and compliance clauses in contracts are common practices to manage this risk.
- Training and Compliance Program: To mitigate the risk of unintentional violations, it's crucial for suppliers to implement a robust

ITAR compliance programs and supporting software. This should include regular training for employees on ITAR regulations and compliance procedures, conducting internal audits, and maintaining accurate records of exports and ITAR-controlled transactions.

- Penalties for Non-Compliance: Violations of ITAR can result in severe penalties, including substantial fines, revocation of export privileges, and even criminal charges. Ensuring compliance is not just about avoiding penalties but also about maintaining the trust and security of the U.S. defense and space sectors.

Given the complexity of ITAR and the severe consequences of non-compliance, it's imperitive that a comprehensive system is in place allowing collaboration between customers and suppliers with particular reference to ITAR and export controls. This will help provide comprehensive record of activity to aid navigation of the regulations effectively and maintain their operations within legal boundaries.

29th February 2024, the Boeing Company announced a 51 million USD settlement with the Department of State, Directorate of Defense Trade Controls (DDTC) for numerous violations of the Arms Export Control Act and the International Traffic in Arms Regulations (ITAR).

Specifically the sources of constituents components for things like alloys would all need to be accounted for. In turn this can lead to circular relationships with partners where clients can become suppliers for part of the process. Under ITAR regulations, the sources of constituent components for items like alloys, especially when these alloys are used in defense-related applications, need to be carefully accounted for. This is due to several reasons:

- Traceability: ITAR compliance requires the ability to trace the origin of materials and components used in the manufacture of defense articles. This ensures that all elements of the supply chain adhere to the regulations and that no prohibited materials or components from restricted countries or entities are used.
- End-Use and End-User Restrictions: ITAR controls are not only about the items themselves but also about their end use and end users. Knowing the source of components helps in assessing the risk of diversion to unintended users or uses that could compromise U.S. national security.
- Supply Chain Compliance: Suppliers and subcontractors involved in the production of ITAR-controlled items must also comply with ITAR. This includes suppliers of raw materials, components, and alloys. Ensuring that these suppliers are compliant requires a clear understanding of where and how these materials are sourced.
- Record-Keeping Requirements: ITAR mandates rigorous record-keeping practices, including documentation related to the manufacture, acquisition, and disposition of defense articles. This

documentation often needs to include details about the source of components used in these articles.

- Due Diligence: Companies involved in the defense sector must perform due diligence to ensure that their entire supply chain is ITAR-compliant. This includes verifying the legitimacy and compliance status of their suppliers and the materials they provide.

For companies that produce alloys for the defense and space technology sectors, it's crucial to establish and maintain a compliance program that includes vetting suppliers, maintaining detailed records of material sources, and ensuring that all components of their products meet ITAR requirements. Given the complexity of these regulations, consulting with experts in ITAR and export control laws is often necessary to navigate these requirements effectively and ensure compliance.

CMMC

The CMMC is a unified standard for implementing cybersecurity across the Defense Industrial Base (DIB), which includes over 300,000 companies in the supply chain. The Department of Defense (DoD) introduced CMMC to protect sensitive defense information on contractors' information systems from increasing cyber threats.

Key Points about CMMC:

- Levels of Certification: CMMC has five levels of certification, ranging from basic cyber hygiene practices at Level 1 to advanced processes for reducing the risk from Advanced Persistent Threats (APTs) at Level 5. Each level builds upon the previous one, adding more stringent cybersecurity practices.
- Requirement for Contracting: Starting from a specific date set by the DoD, all contractors and subcontractors must meet the appropriate CMMC level certification to be eligible for DoD contracts. The required CMMC level will vary depending on the sensitivity of the information involved and the specific work to be done.
- Assessment and Certification: Unlike previous self-assessment models, CMMC requires an assessment by an accredited and independent third-party assessment organization (C3PAO) to ensure compliance with the necessary cybersecurity practices and processes.
- Scope of Application: CMMC applies to all companies within the DIB, including small businesses, commercial item contractors, and foreign suppliers, that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

- Continuous Compliance: CMMC emphasizes the importance of continuous cybersecurity improvement and vigilance. Certification is not a one-time event but requires ongoing efforts to maintain and improve cybersecurity practices.

U.S. steel rolling mills and producers of alloys for the defense and space technology sectors will need to ensure compliance with the appropriate level of CMMC certification. This involves:

- Assessing Current Cybersecurity Practices: Understanding their current cybersecurity maturity and gaps in relation to the CMMC level required for their contracts.
- Implementing Required Controls: Adopting and implementing the necessary cybersecurity practices and processes to meet their target CMMC level.
- Undergoing Certification: Preparing for and undergoing an assessment by a C3PAO to obtain certification.
- Maintaining Compliance: Continuously monitoring, managing, and improving their cybersecurity posture to maintain compliance with CMMC requirements.

Achieving and maintaining CMMC certification is crucial to participate in DoD contracts and to protect sensitive defense information against cyber threats. It's advisable to consult with cybersecurity experts familiar with CMMC to guide them through the preparation, certification, and compliance process.

CMMC is a unified standard for implementing cybersecurity across the Defense Industrial Base (DIB).

Lockular Marketplaces

Lockular's NFT marketplace platform offers substantial support in meeting ITAR and CMMC compliance requirements. The foundation of Lockular's marketplace is an immutable ledger, utilizing Polkadot's parachain technology. Implemented with Web3 technology, the platform consists of two primary capabilities:

Web3 is a marketing term for uses of the World Wide Web which incorporate concepts such as decentralization, blockchain technologies, and token-based economics.

- A Shopify style Web3 based shop front
- A multi party signatory blockchain backend facilitating authenticated and audited collaboration by multiple parties

The blockchain (parachain) technology provides the immutable records of note recorded throughout the material's lifecycle as it passes through the collaborative workflow. The multi party signatory technology provides the means by which customers and suppliers authenticate and collaborate in the workflow via the blockchain

based marketplace. The multi party signatory capability is described below and implemented using well proven Multi-Party Computation (MPC) capabilities[2].

[2]

Benefits

- Marketplace to buy, sell and transfer uniquely recognisable items in the physical World as NFTs where all tranbsactions are underpinned by an immutable audit
- Marketplace that supports authenticated collaboration and decision making via multi sig capability
- Representation of workflow outputs (Alloys) as NFTs

Polkadot Parachains

Parachains enable decentralized applications to scale beyond the limitations of a single blockchain by accessing the resources of the Polkadot network. They allow for specialized blockchains to be built for unique use cases while still being interoperable with other parachains and blockchains in the Polkadot ecosystem.

The decentralized nature of blockchain technology means that the ledger is distributed across multiple nodes, making it highly resistant to tampering and cyber attacks. This inherent security can contribute to the overall cybersecurity posture required by CMMC, reducing the risk of unauthorized access or disclosure of sensitive defense-related information.

The transparency and immutability of blockchain records can simplify the process of compliance auditing. Auditors can verify the integrity and security of the supply chain data directly on the blockchain, reducing the time and resources required for compliance audits. This can be particularly beneficial for meeting CMMC requirements related to documentation, record-keeping, and reporting.

MPC

Blockchain technology combined with Multi-Party Computation (MPC) provides the extreme rigour required for ITAR compliant supply chain management, offering a robust framework that aligns well with the Cybersecurity Maturity Model Certification (CMMC) requirements, especially in terms of safeguarding Controlled Unclassified Information (CUI) and enhancing cybersecurity practices.

How MPC Complements Blockchain for CMMC Compliance:

- Enhanced Data Security: MPC allows for the processing of data by multiple parties without any single party having access to the complete dataset. This can significantly enhance the security of sensitive information, such as CUI, by ensuring that it is never fully exposed, even during transactions or processing. This aligns with CMMC requirements for protecting sensitive information.

- Secure Access Control: By integrating MPC with blockchain, access to data or transactions can be controlled through a distributed consensus mechanism that requires agreement from multiple parties. This method of access control ensures that no single entity can unilaterally make decisions, enhancing the security and integrity of the supply chain data. This approach is in line with CMMC practices that emphasize limiting access to CUI to authorized individuals.
- Improved Privacy and Confidentiality: MPC can process encrypted data without decrypting it, thereby maintaining the confidentiality of the information. When combined with the immutable record-keeping capabilities of blockchain, this ensures that sensitive data remains confidential and secure throughout the supply chain. This capability supports CMMC requirements related to the privacy and protection of information.
- Auditability and Compliance Verification: The immutable ledger provided by blockchain technology, combined with the secure data processing of MPC, offers a transparent and verifiable record of all transactions and data processing activities. This facilitates easier compliance audits and verification processes, as auditors can reliably trace and verify the security and integrity of the supply chain operations, which is crucial for CMMC compliance.

There are a number of references describing the evolution of data usage and how it might be controlled,[3] Michele Finck's book elaborates in detail with its discussion of non financial applications of the BLOCKCHAIN, and with particular reference to individuals taking back control of their data.

[3]

Appendices

CMMC Domains Related to Privacy and Information Protection

The Cybersecurity Maturity Model Certification (CMMC) framework integrates various cybersecurity standards and best practices into a comprehensive set of requirements. The following domains specifically address the privacy and protection of information:

Table 1: CMMC Domains Related to Privacy and Information Protection

Domain	Description
Access Control (AC)	Ensures access to Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) is limited to authorized users, processes, or devices.
Identification and Authentication (IA)	Requires proper identification and authentication controls to ensure that only authorized individuals can access organizational systems.
Audit and Accountability (AU)	Mandates the creation, retention, and review of system logs to enable the monitoring and investigation of unauthorized system activity.
Configuration Management (CM)	Involves controlling changes to system configurations to maintain security and integrity.
Incident Response (IR)	Requires the development of an incident response capability to detect, respond to, and recover from cybersecurity incidents.
System and Information Integrity (SI)	Focuses on protecting systems and components from malware and unauthorized changes.
System and Communications Protection (SC)	Involves implementing controls to protect information transmitted or received by systems.
Media Protection (MP)	Addresses the protection of FCI and CUI on digital and non-digital media throughout its lifecycle.