בס"ד

Securing the **Supply Chain**

Partnering for **CMMC Compliance** in Defense Contracting

CYBERSECURITY MATURITY MODEL
CERTIFICATION

JACO
AEROSPACE & INDUSTRIAL

Why Are We Writing this Whitepaper

In today's increasingly demanding cybersecurity environment, companies working with the U.S. Department of Defense (DoD) must adhere to rigorous security standards to safeguard sensitive information. Compliance with frameworks such as CMMC and NIST 800-171 can be challenging, but it is critical to ensuring the security and resilience of the nation's most sensitive data.

Jaco Aerospace, a woman-owned small business, recently achieved a perfect score of 110 in the Joint Surveillance Voluntary Assessment (JSVA), earning the prestigious 'DIBCAC High' rating and advancing to CMMC Level 2 Certification. This accomplishment is exceedingly rare, with only around 100 companies—just 0.1% of the Defense Industrial Base (DIB)—reaching this level. The vast majority of these companies are defense primes, manufacturers, or service providers directly to the DoD, who are required to meet these stringent standards. Notably, very few aerospace distributors, like Jaco Aerospace, have attained this level of certification.

At Jaco Aerospace, we recognize the significance of these regulations for both our customers and suppliers.

How Jaco Supports Our Customers

This achievement represents more than just maintaining compliance for our customers; it reflects our commitment to protecting your business from unnecessary risks and liabilities. As cybersecurity regulations become mandatory across the defense supply chain, partnering with a trusted and certified supplier like Jaco Aerospace is essential.

With the capability to supply over 7 million parts and consumable materials, Jaco Aerospace ensures that your procurement needs are securely and efficiently met while adhering to all regulatory requirements. As a recognized supplier for major defense contractors, including Northrop Grumman, where we were named Supplier of the Year in 2024, we have the expertise and infrastructure to support even the most complex needs.

As cybersecurity becomes a standard component of DoD acquisitions, it is crucial to work with a supplier who not only meets your material needs but also guarantees full regulatory compliance. Many authorized distributors and OEMs lack the necessary certifications, making it difficult for end users to find compliant suppliers within their networks. Jaco Aerospace addresses this challenge by maintaining full regulatory compliance, expanding our product offerings, and increasing stock levels to ensure you meet your contractual obligations—positioning us as a trusted and secure partner for defense contractors.

How Jaco Supports Manufacturers

For manufacturers of aerospace products and materials, the number of companies that have successfully passed the stringent cybersecurity assessment is limited, greatly reducing the pool of reliable suppliers for defense contractors. This challenge extends beyond distribution, as many OEMs and manufacturers lack the required certifications, leaving customers with few options for sourcing compliant products.

Additionally, many authorized distributors lack the necessary cybersecurity infrastructure, further limiting the availability of compliant suppliers. Jaco Aerospace solves these problems by fully meeting all regulatory requirements.

As a trusted partner to major brands, we consistently demonstrate our ability to exceed expectations, ensuring that the distribution of your products meets the highest standards. Additionally, we are continuously expanding our product offerings and increasing stock levels to better serve your needs.

For our audience this whitepaper will demystify key terms, assessments, and standards in defense cybersecurity and explain why NIST 800-171, AS9120 certifications, and CMMC requirements are critical for securing DoD contracts. Our goal is to provide you with clear, actionable insights to confidently navigate cybersecurity compliance.

By understanding these cybersecurity frameworks and achieving early compliance, your business can unlock new opportunities in defense contracting.

If you have any questions, feel free to contact us at cmmc@e-aircraftsupply.com.

Jaco Aerospace Inc.

Ensuring Data Security through CMMC Compliance

Introduction

In today's digitally driven world, cyber threats such as ransomware, hacking, and sophisticated advances in computational power are rising at unprecedented levels. The U.S. government has taken increasingly stringent steps to address these threats and safeguard critical information. While high-priority efforts focus on securing the nation's defense secrets, the scope of data protection has expanded. Today, federal agencies, contractors, and subcontractors must protect not only classified data but also Federal Contract Information (FCI) [1] and Controlled Unclassified Information (CUI) [2].

The implications of mishandling this sensitive data are significant. Beyond jeopardizing national security, cybersecurity failures can result in severe regulatory penalties, contract loss, and potential legal actions. The introduction of the Cybersecurity Maturity Model Certification (CMMC) underscores the government's emphasis on creating a regulatory framework that mandates compliance from every federal contracting supply chain level.

[1] FCI is very broad. Contractors focused on maintaining compliance should adopt an inclusive approach to what they consider FCI

[2] CUI is particular and marked with "Controlled Unclassified Information," making it much more distinct than FCI. The DOD estimates that under 80,000 contractors handle CUI.

Unauthorized use or replication of this document is strictly prohibited and subject to legal penalties. Any such actions are a violation of applicable law.

The Nature of the Risk: Understanding FCI and CUI [3]

Federal Contract Information (FCI) refers to non-public information that is provided by or generated for the government under a contract. This information might not be classified, but it remains critical to the performance of government services. **Controlled Unclassified Information (CUI)** includes information that requires legal or regulatory safeguarding. CUI must adhere to stringent safeguarding guidelines to protect against unauthorized access and dissemination.

The distinction between FCI and CUI is crucial because it dictates the cybersecurity obligations placed on contractors and subcontractors. Under the CMMC, compliance requirements increase as the data sensitivity rises, making a clear understanding of these terms essential for every organization that handles government information.

Federal Contract Information (FCI)

"Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public web sites) or simple transactional information, such as necessary to process payments."

Controlled Unclassified Information (CUI)

"Controlled Unclassified Information (CUI) requires safeguarding or dissemination controls according to and consistent with applicable law, regulations, and government-wide policies but is not classified. CUI must adhere to stringent safeguarding guidelines to protect against unauthorized access and dissemination.

The Defense Industrial Base and Cybersecurity Breaches

The Defense Industrial Base (DIB), consisting of over 100,000 [4] contractors and subcontractors, forms the backbone of the U.S. defense supply chain. The DIB represents approximately 972,000 employees, many of whom deal with FCI in some capacity. The increasing frequency of cyberattacks targeting these entities—driven by nation-states, organized crime, and cyber terrorists—has highlighted the vulnerabilities in the defense sector's cybersecurity posture.

[3] Information Security Oversight Office. (2020, June 19). What is the difference between FCI and CUI? Retrieved from ISO: https://isoo.blogs.archives.gov/2020/06/19/%E2%80%8Bfci-and-cui-what-is-the-difference/

[4] The defense industrial base (DIB; also, sometimes referred to as a defense industrial and technological base) is the network of organizations, facilities, and resources that provides a government with materials, products, and services for defense purposes (especially the supply of its armed forces).

Table 2. Selected Reported FY2023 DOD Component Contractor FTEs [5]

Funding Agency	Reported FTEs
Department of the Army	**97,745**
Department of the Navy	**576,139**
Department of the Air Force	**254,861**
Defense Advanced Research Projects Agency (DARPA)	**547**
Defense Information Systems Agency (DISA)	**9,875**
U.S. Special Operations Command (USSOCOM)	**6,028**
Defense Health Agency (DHA)	**5,001**
Office of the Secretary of Defense (OSD)	**5,108**
Missile Defense Agency (MDA)	**3,705**
Defense Counterintelligence and Security Agency (DCSA)	**3,400**

Prime Contractors and Subcontractors for Contracts Required to be Reported Under 10 U.S.C. §4505, by DOD Component CRS analysis of DOD FY2023 Inventory of Contracted

Source: (Information Security Oversight Office, 2020)

Government reports and recent incidents illustrate the tangible risks posed by cyberattacks[6]. Hostile actors seeking to undermine U.S. national security have compromised sensitive defense-related technologies, intellectual property, and operational details. These incidents expose contractors to business risks and create significant regulatory risks.

[5] Prime Contractors and Subcontractors for Contracts Required to be Reported Under 10 U.S.C. §4505, by DOD Component Source: CRS analysis of DOD FY2023 Inventory of Contracted

[6] Cybersecurity & Infrastructure Security Agency. (n.d.). Defense Industrial Base Sector. Retrieved from CISA: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/defense-industrial-base-sector

Regulatory Landscape: The Introduction of CMMC

To address the escalating threats to national security, the Department of Defense (DoD) introduced the Cybersecurity Maturity Model Certification (CMMC). Based on the guidelines set forth by the National Institute of Standards and Technology (NIST) Special Publication 800-171 [7], the CMMC establishes a tiered certification framework that sets security standards according to the sensitivity of the data handled by contractors. This framework has direct regulatory implications for every contractor and subcontractor in the defense supply chain, with the most significant aspect being its mandate for compliance.

The Stakes: Regulatory Risk and the Cost of Non-Compliance

The CMMC represents more than just a cybersecurity protocol; it is a comprehensive regulatory requirement. Federal contractors and subcontractors must comply with the prescribed security controls at the risk of facing severe legal and financial penalties. This framework echoes other regulatory compliance standards like the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in healthcare. The potential consequences of failing to comply with CMMC go beyond simple contract loss:

Financial Penalities[8]

Non-compliance can lead to significant financial losses, including fines and penalties for breach of contract. The **False Claims Act (FCA)** [9] gives the government broad authority to take legal action against companies that misrepresent their compliance status. In FY2023, the Department of Justice recovered over $2.68 billion from cases related to fraud and false claims. This figure represents a stark reminder of the financial ramifications of non-compliance.

Loss of Federal Contracts

Failure to meet the required CMMC level by critical implementation deadlines can result in immediate disqualification from future contracts. Prime contractors are already implementing strict compliance checks, ensuring subcontractors within their supply chains adhere to CMMC standards.

Legal Risks

Contractors who fail to comply with CMMC requirements face legal exposure besides financial penalties. The **False Claims Act** is a potent enforcement tool for the government, which can impose heavy legal consequences on companies found guilty of misrepresenting their compliance.[10] Lawsuits could drag a company into lengthy legal battles, resulting in reputational damage and future contract exclusions.

Loss of Funding

Non-compliance with CMMC standards may lead to the government pulling funding from ongoing contracts or research projects.[11] Federal agencies reserve the right to terminate funding for contractors that fail to meet cybersecurity requirements, potentially halting critical projects and research. This loss of funding can cripple a company's operations, as government-backed initiatives are often key revenue sources. In addition to immediate financial consequences, losing government funding can damage long-term partnerships and make it harder to secure future projects.

[7] DFARS. (n.d.). Safeguarding Covered Defense Information and Cyber Incident Reporting. Retrieved from Acquisition: Safeguarding Covered Defense Information and Cyber Incident Reporting

[8] U.S. Department of State Concludes $51 Million Settlement ...

[9] Office of Public Affairs | Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts | United States Department of Justice

[10] https://www.eyeonenforcement.com/2024/09/government-contractors-beware-doj-pursuing-cybersecurity-failures-under-the-false-claims-act/

[11] Cyber Fraud Alleged by Former CIO for Purported Noncompliance With DoD Cyber Requirements | Insights | Skadden, Arps, Slate, Meagher & Flom LLP

The Necessity of Compliance: A Tiered Framework

Cybersecurity Maturity Model Certification (CMMC) and Security Requirements

CMMC Maturity	Impacted Contractors	Security Requirements
Level 1	Contractors and subcontractors who will process, store, or transmit FCI on unclassified contractor information systems.	15 basic safeguarding requirements and procedures designed to protect covered contractor information systems. All 15 requirements are currently required under FAR Clause 52.204-21.
Level 2	Contractors or subcontractors responsible for processing, storing, or transmitting CUI on unclassified contractor information systems.	110 security requirements specified in NIST SP 800-171.
Level 3	As determined by DoD on a contract-by-contract basis, based on the sensitivity of the CUI involved in the performance of that contract.	110 security requirements specified in NIST SP 800-171. AND 24 selected security requirements from NIST SP 800-172.

The Cybersecurity Maturity Model Certification (CMMC)

The Department of Defense (DoD) has developed the Cybersecurity Maturity Model Certification (CMMC) to address this growing need for standardized protocol protection. This framework is based upon the National Institute of Standards and Technology (NIST) Special Publication 800-171cyber security requirements.

CMMC establishes cybersecurity standards tailored to the sensitivity of the data handled by government contractors and subcontractors. CMMC Level 1 compliance mandates 15 security controls to safeguard non-public government information for companies interacting with FCI.[12] These foundational cybersecurity practices are essential for protecting FCI.

In contrast, companies handling CUI are subject to more advanced cybersecurity requirements. CMMC Level 2, which applies to companies working with CUI, mandates compliance with 110 security controls outlined in the National Institute of Standards and Technology (NIST) Special Publication 800-171.[13] This heightened level of protection reflects the sensitive nature of CUI and the legal obligations associated with safeguarding this data. The distinction between FCI and CUI highlights the CMMC framework's tiered approach, which ensures that security measures are proportionate to the risks posed by different types of information.

[12] DFARS. (n.d.). Safeguarding Covered Defense Information and Cyber Incident Reporting. Retrieved from Acquisition: Safeguarding Covered Defense Information and Cyber Incident Reporting

[13] U.S. Office Of Public Affairs. (2024, February 22). False Claims Act Settlements and Judgments Exceed $2.68 Billion in Fiscal Year 2023. Retrieved from Department of Justice.

Flow-Down Requirement for Subcontractors

One of the most significant aspects of the CMMC is its "flow-down" requirement. This rule ensures that CMMC compliance is not restricted to companies directly contracting with the government. Subcontractors working under a prime contractor with a CMMC requirement must also meet the appropriate CMMC level, even if their work seems unrelated to sensitive government operations.

This flow-down requirement ensures that cybersecurity measures are applied consistently across the entire supply chain, reducing the risk of vulnerabilities introduced by subcontractors. Consequently, all subcontractors, regardless of their involvement in core services, must be prepared to meet CMMC requirements. Non-compliance in any supply chain link can lead to breaches, underscoring the importance of widespread adherence to CMMC regulations.

Implementation Timeline and Phased Rollout

The CMMC's phased implementation begins in early 2025. Companies handling FCI must achieve CMMC Level 1 certification during this initial phase. As the rollout continues, CMMC Level 2 certification or attestation will become mandatory for contractors handling CUI. There will be a small subset of contracts involving less sensitive CUI that will require contractors to self-assess and attest, rather than certify with a C3PAO. The insertion of the 252.204-7021 CMMC certification requirements will increase over the next 5-7 years. Ultimately, all contracts involving CUI will enforce the requirement to be compliant. Contractors should plan for the highest level of CUI they intend to interact with. They will not be eligible to win contracts with requirements higher than what they attain.

Failing to meet these compliance deadlines can have serious consequences, including the loss of eligibility to win or participate in DoD contracts. Prime contractors are increasingly adopting a proactive stance, ensuring that their subcontractors prepare for compliance immediately to prevent disruptions and avoid regulatory penalties.

Preparing for Compliance: Mitigating Regulatory Risk

Self-attestation can achieve compliance for companies seeking contracts requiring CMMC Level 1 certification. However, most contracts involving CUI have the CMMC Level 2 requirement for a full third-party assessment to verify compliance. While the self-attestation process may seem straightforward, companies must approach it cautiously, as non-compliance carries significant legal risks.

The False Claims Act grants the government authority to act against companies that misrepresent their compliance status. There is precedent for such cases, and the financial consequences can be severe. In fiscal year 2023 alone, the Department of Justice secured over $2.68 billion in settlements and judgments related to fraud and false claims against the government. Therefore, companies must take their compliance obligations seriously to avoid potential legal action and the loss of valuable government contracts.

For companies operating within the Defense Industrial Base and the broader federal contracting space, CMMC compliance is not merely a regulatory requirement but a critical business imperative. To effectively mitigate regulatory risks, organizations must take several proactive steps.

The first step toward ensuring compliance is to conduct a thorough gap analysis. This assessment is essential for evaluating the current cybersecurity posture and pinpointing areas of non-compliance that need improvement through targeted security measures. Following this, it's crucial to design the future state required to meet contracts with CMMC requirements and develop a comprehensive compliance program. This program should incorporate regular internal audits, employee training, and stringent data protection protocols—key elements for achieving CMMC standards, particularly in safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Once a secure environment is established, companies seeking CMMC Level 2 or higher certification must undergo an independent assessment by certified third-party assessors to verify full compliance. Finally, continuous monitoring is essential to maintain cybersecurity. This includes regularly evaluating the company's security posture to mitigate potential risks and ensuring that subcontractors in the supply chain comply with appropriate CMMC levels, thereby preventing security vulnerabilities from non-compliant partners.

While third-party assessments will officially begin in Summer 2025, Jaco Aerospace Inc. has already scored a perfect 110 in the Joint Surveillance Assessment Program (JSVA), which allows companies to get assessed before rulemaking is finalized. Those scoring a 110 will be converted to CMMC L2 Certified once the rule is final. They will reap the benefits of early certification and be a secure choice for the DoD and primes.

The Future of CMMC Compliance

The Department of Defense introduced the CMMC framework in direct response to the growing cybersecurity threats faced by the federal government and its contractors. While CMMC compliance is currently specific to the DoD, these requirements are anticipated to expand to other federal agencies shortly. Given that the CMMC is based on the NIST standards, which apply across all federal branches, it is likely that the framework will become a government-wide standard.

As cybersecurity risks continue to evolve, companies working with non-DoD agencies must prepare to meet the stringent security requirements outlined in the CMMC. Contractors across various industries must be ready to implement robust cybersecurity practices to ensure compliance with future federal contracts. The need to safeguard critical data across all levels of government is clear, and the CMMC provides a structured approach to achieving this goal.

Conclusion

The U.S. government's introduction of CMMC marks a significant regulatory shift in the way federal contractors and subcontractors must approach cybersecurity. Compliance is no longer optional, but a requirement to protect sensitive government data, mitigate legal risks, and maintain eligibility for federal contracts. The consequences of non-compliance are severe, from financial penalties to legal action, contract loss, and reputational damage.

As the phased rollout of CMMC continues, federal contractors have a limited window of opportunity to achieve compliance. Companies that prioritize CMMC preparation today will safeguard their future business opportunities with the U.S. government, while those that fail to act risk losing their place in the federal marketplace. CMMC compliance is no longer just about cybersecurity; it's about survival in a highly competitive, heavily regulated industry.

Our Mission

Jaco Aerospace is a trusted mission-critical partner for customers. We provide what they want when they want it, with unwavering quality.

About Jaco Aerospace

Since 1971, Jaco Aerospace has been a leading distributor of high-quality chemicals, raw materials, and consumables for the commercial airline and aerospace industries. With over 50 years of experience as an authorized distributor for top manufacturers, we ensure prompt delivery of factory-new products to meet our customers’ needs.

Our facilities are tailored to accommodate our clients' specific requirements, consistently providing the products and service they expect. We go above and beyond to offer personalized solutions and meet even the most specialized demands.

In 2024, we were proud to be named Northrop Grumman Supplier of the Year, recognizing our commitment to excellence. We also received the CMMC Protector Award at the CMMC 2024 Implementation Conference (CIC 2024). These honors highlight our unwavering dedication to excellence and cybersecurity in the aerospace industry.

For inquiries, please contact us at cmmc@e-aircraftsupply.com.

Multiple Locations, One Mission: Serving You

- Jaco Aerospace Headquarters – Valencia, CA
- Jaco Aerospace Warehouse and Planning Facility – Santa Clarita, CA
- Los Angeles, CA
- Indianapolis, IN
- Dallas, TX

SUPPLIER EXCELLENCE AWARD WINNER
NG
NORTHROP GRUMMAN
2024