SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

Understanding DFARs, NIST and CMMC Compliance Requirements for DIB Contractors

"Safeguarding Covered Defense Information and Cyber Incident Reporting"

Role of the DIB

Effective November 30, 2020, a DoD interim rule amends the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain. More than at any time in history, the Federal Government is relying on the Defense Industrial Base (DIB) to help carry out a wide range of federal missions and business functions using information systems. Many Federal contractors process, store, and transmit sensitive federal information to support the delivery of essential products and services to Federal agencies ranging from financial services to communications and weapons systems. Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. This interim rule solidifies the DoD's commitment to a secure DIB/ Supply Chain to protect our national interests.

Cybersecurity is a critical challenge facing these organizations. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, equating up to $1.09 trillion dollars over ten years. With all of its other challenges, according to a recent study from cloud computing company Iomart, large-scale breaches are growing in intensity and frequency in 2020, with the number of breaches increasing 273% in the first quarter, compared to the same time last year. The theft of intellectual property (IP) from all U.S. industrial sectors due to malicious cyber activity threatens U.S. economic and national security. In addition, the aggregate loss of IP and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation. Federally granted research led to the development of the MRI, modern communication devices, and the internet. The protection of sensitive Federal information while residing in non-Federal systems and organizations is of paramount important to Federal agencies and can directly impact the ability of the federal government to carry out its designated missions and business operations.

In response, the Department of Defense (DoD) is working to enhance the protection of controlled unclassified information (CUI) within the supply chain. CUI is Federal Government information routinely processed, stored, or transmitted by a contractor during its work providing essential products and services to federal agencies. In addition, contractors must include the clause in subcontracts for which performance will involve covered Defense information or operationally critical support. On September 29, 2020, guidance from the Undersecretary of Defense for implementing DFARS Clause 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting" is no longer optional.

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

Defense Security Compliance Requirements

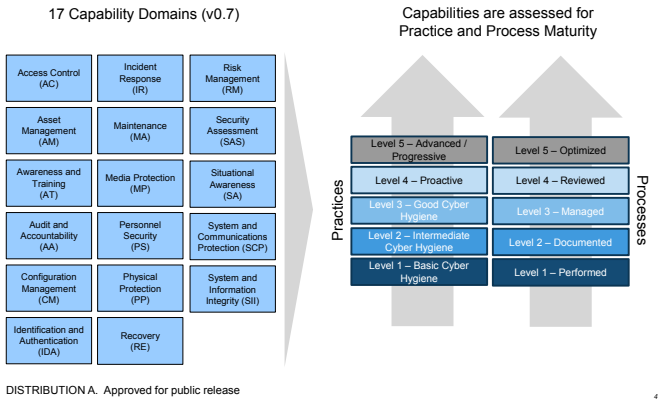
This ruling expands on the existing DFARS clauses and further clarifies the requirements of DIB contractors to be NIST SP 800-171 and Cybersecurity Maturity Model information flowed down to subcontractors in a multi-tier supply chain.

DFARS Clause 252.204-7012 requires contractors to apply the security requirements of NIST SP 800-171 to "covered contractor information systems," as defined in the clause, that are not part of an IT service or system operated on behalf of the United States Government (USG). NIST SP 800-171 introduces a set of requirements in access control, maintenance, system and information integrity, and more to ensure the security of CUI on nonfederal information systems.

DIB contractors will be assessed based on 48 CFR 52.204-21, NIST SP 800-171r1 & Draft -171B and other sources, separated into five levels (shown in the graphic below). Each level reflects the depth of assessment performed and the Maturity of an organizations Practices and Processes. The Assessments are completed for each/ all covered contractor's information system that is relevant to the officer, contract, task order or delivery order.

Building upon the NIST SP 800-171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect sensitive unclassified information such as CUI accounting for information flow down to its subcontractors in multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or segments or enclaves depending on where the protected information is processed, stored, or transmitted.

The CMMC model consists of cumulative maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC model adds an additional five processes and 61 practices across levels 2-5 that demonstrate a progression of cybersecurity maturity. In order to achieve a specific CMMC level, a DIB company must demonstrate both process institutionalization or maturity and the implementation of practices commensurate with that level.



CMMC assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs) and upon completion, a company is awarded a certification by an independent CMMC Accreditation Body at the appropriate CMMC level. CMMC certifications are valid for three years.

By October 1, 2025, all entities receiving DoD contracts and orders, other than contracts or orders exclusively for commercially available off-the-shelf items or those valued at or below the micro-purchase threshold, will be required to have the CMMC Level identified in the solicitation. However, the DoD has already begun a five-year phased rollout strategy. While this rollout is intended to minimize the financial impacts to the industrial base, some contracts will include the CMMC requirement in the statement of work.

How SPYRUS Can Help with Compliance

Ensuring your organization is DFARS Clause 252.204-7012 and CMMC compliant is critical to preparing for the future of DoD work. SPYRUS Solutions has more than 20 years of experience defending classified information and protecting the DIB. We have experts on staff and ecosystem partners who understand the compliance requirements. SPYRUS Solutions can help your organization meet all NIST SP 800-171 standards and be CMMC level 3 compliant. To learn more about how SPYRUS can help your organization, visit our website for more information on our CMMC solutions.

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

About SPYRUS

SPYRUS develops and deploys cryptographic operating systems in innovative ways, providing the strongest protection for data in motion, data at rest and data in process. For more than 20 years, SPYRUS has delivered encryption, authentication, and digital content security products to government, financial, and healthcare enterprises. SPYRUS solutions enable customers to meet stringent regulatory requirements for data protections across industries.