ARMIS FEDERAL

SOLUTION BRIEF

Armis Provides a Clear Path to CMMC Compliance

Protecting the DoD Supply Chain

Maintaining and modernizing the military forces needed to deter war and ensure our nation's security requires the coordination of a deeply interconnected service and supply chain. The Department of Defense (DoD) relies daily on businesses in nearly every sector of the U.S. economy, and nation-state actors have proven adept at mapping these connections and exploiting weakness to steal DoD data stored on non-federal networks or gain access to DoD networks directly.

Recognizing the peril of cybersecurity breaches within the Defense Industrial Base (DIB) and acknowledging the potential detrimental effect on the warfighter's mission, the Department of Defense formulated the Cybersecurity Maturity Model Certification (CMMC). The CMMC model is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) that is shared with contractors and subcontractors of the Department through acquisition programs. CMMC ensures that all DoD organizations competing for work with the Department maintain a baseline level of cybersecurity commensurate with their risk to the DoD mission. It was designed with distinct levels of maturity, allowing for less stringent cybersecurity criteria for non-mission critical tasks, while demanding elevated cybersecurity standards for more sensitive undertakings.

CMMC Impact on the DIB

The CMMC framework provides a model for contractors in the DIB to protect CUI on non-federal systems and measures compliance against 110 Security controls in NIST SP 800-171. For more complex and sensitive engagements, the framework will also measure a subset of requirements from NIST SP 800-172.

CMMC encompasses fourteen (14) functional domains and offers three (3) levels of compliance. The expectations for a company increase significantly with each level and range from basic cyber hygiene and the execution of essential processes (Level 1) to the full complement of optimized processes with advanced/proactive cybersecurity capabilities in place (Level 3). Depending on the sensitivity of data handled and the level of compliance required, companies may either self-assert compliance or submit to an independent audit from the Third-Party Assessment Organization (3PAO) or the federal government. Whether self-asserting compliance at the foundational Level 1 or working with a third-party assessor for higher certifications, all companies, regardless of size or service, are required to have a CMMC assessment in place to work with the DoD and renew it every three years.

CMMC Model 2.0

	Model	Assessment
Level 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
Level 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information: Annual self-assessment for select programs
Level 1 Functional	**17** practices	Annual self-assessment

Armis' Role in Supporting CMMC Compliance

Armis Centrix™, the Armis Cyber Exposure Management Platform, helps DIB members maintain compliance with DFARS 7012, 7019, and 7020. Our platform's flexible deployment means there is little impact on the existing IT teams and time-to-value in minutes. Reports can be produced and used for self-accreditation or by third-party auditors for a higher level accreditation. Armis Centrix™ will also detect DFAR 889 assets in near real-time. For instance, when an "Alexa" or Chinese manufactured Huawei device connects to a corporate network, Armis Centrix™ detects it within seconds and issues an alert.

Armis Centrix™ plays a vital role in assessing CMMC compliance and implementing the required controls. It offers a comprehensive solution that automatically identifies all physical and virtual assets - from the ground to the cloud, associated vulnerabilities, and generates a detailed report to assist DIB members in achieving and upholding their CMMC certification. The platform is unique in its ability to provide customers unparalleled visibility into the assets on the network and the risks associated with each and every device, directly addressing the core requirements of CMMC.

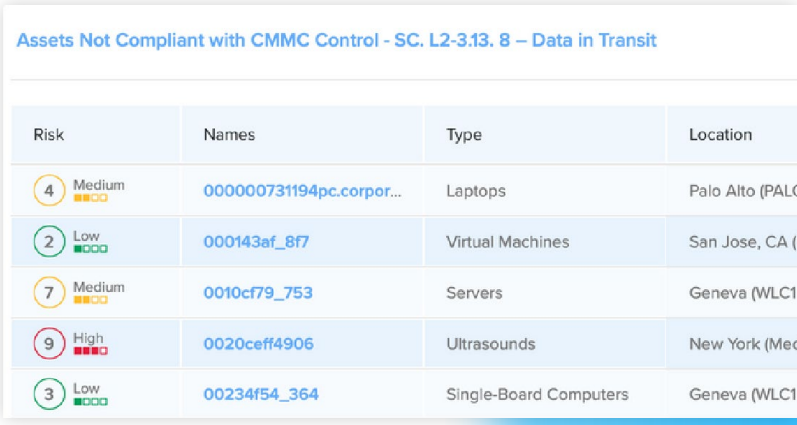
Armis Centrix™ detects and characterizes every device connected to the network. It monitors all network traffic for known threat activities and abnormal device behavior. This encompassing approach involves conducting a risk assessment for each device, to identify all known Common Vulnerabilities and Exposures (CVEs) associated with a device and the software it operates. Armis Centrix™ utilizes a large set of out of the box integrations with leading cybersecurity systems. The platform harnesses these integrations to draw data from external systems and consolidate the information into a unified and comprehensive view of all assets. Additionally, Armis Centrix™ duplicates and refines the data. Through integrations, you can pull additional device information from a contractor's configuration management database, identity management system, end point security solutions, additional vulnerability tools, patch management systems, and cloud infrastructures. The platform incorporates this information into each device's profile, granting the contractor the ability to examine, organize, refine, and establish policies for the entirety of a customer's technology environment.

Through other integrations, Armis Centrix™ provides policy driven actions, including alerts sent to the contractor's SIEM and the creation of tickets in the contractor's ITSM system. It can also initiate enforcement actions with the contractor's firewalls, IDS systems, and wireless LAN controllers. This represents a complete and mature deployment of the platform into a contractor's environment and provides the baseline set of capabilities for CMMC.

Armis Centrix™ also possesses the capability to identify compliance with Section 889 of the National Defense Authorization Act and can further provide insights into network assets, including manufacturer details, operating system versions, and any associated CVEs. Moreover, it empowers security teams to stop attacks before they happen. By combining early warnings of the vulnerabilities that matter based on what threat actors are doing with the context of all critical security findings and asset context, teams can focus resources on the highest-priority risks and reduce the exposure window for what may impact the business most.

The Easy Button

Armis Centrix™ is FedRAMP and IL Authorized, and flexible, making it extremely easy to deploy. Traditionally, most CMMC audit requirements were manually gathered and tracked in spreadsheets, a laborious and time-intensive task repeated on a regular schedule. More critically, this manual process led to an inaccurate understanding of network assets at any given moment, wasting valuable time and resources on data quality rather than focusing on reducing vulnerabilities and improving compliance.
With Armis, customers start receiving valuable compliance insights on day one.



Summary

Armis Centrix™ and the CMMC program have the same objectives: to see, protect and manage risks associated within a specific network environment. With Armis Centrix™, a DoD DIB member can easily collect the required data for self-certification or 3PAO certification in near real-time.

Armis Centrix™ pulls data from a contractor's existing cybersecurity solutions and integrates this data with Armis sensor data, cleaning up and de-duplicating the information for easier analysis. With the Armis platform, DoD contractors can detect all devices physical and virtual - from the ground to the cloud. It then assesses the risk and behavior ofthe devices on the network and enforces established policies and alerts based on abnormal behavior or compliance violations.

The DoD published the final CMMC 2.0 rule in October 2024, and the new cybersecurity standards for contractors are expected to be in place by mid-2025. It is inevitable that prime contract holders will inquire about the compliance status of their subcontractors, and rightly so as the protection of CUI data is mission critical when working with the Department of Defense. Our platform is uniquely positioned to arm DIB members with a clear compliance picture of the required data and evidence needed for CMMC compliance. Contact us today to start your journey towards compliance and helping to protect our nation's sensitive defense information.

ARMIS FEDERAL

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

armisfederal.com

888.452.4011

in

Armis Centrix™ is a FedRAMP and IL authorized solution for the U.S. federal government.