Omada

SOLUTION BRIEF

5 Ways to Prepare for U.S. Department of Defense's CMMC 2.0 with Omada Identity Cloud

The transition to Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) represents a crucial milestone for organizations working with the Department of Defense (DoD). Achieving compliance with these updated requirements ensures the protection of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI), which are key to retaining eligibility for DoD contracts. With its focus on streamlining compliance, the CMMC 2.0 places a strong emphasis on adhering to NIST SP 800-171 standards and implementing robust identity and access controls. Omada Identity Cloud simplifies the challenges of meeting these requirements, enabling a streamlined approach to compliance while strengthening overall cybersecurity posture.

1 Align with the Core Requirements of NIST SP 800-171

NIST SP 800-171 provides the foundation for CMMC 2.0 compliance. Start by conducting a comprehensive gap analysis to identify security control deficiencies. Then, implement policies and technical safeguards to protect Controlled Unclassified Information (CUI). Refer to authoritative sources, such as the NIST publication, to verify that your measures align with recognized best practices.

2 Strengthen Identity Governance and Administration (IGA)

CMMC 2.0 emphasizes controlling access to sensitive data. Omada Identity Cloud supports this by enforcing the principle of least privilege, ensuring users only have access to the resources they need to perform their roles. A well-structured IGA program provides continuous visibility, life-cycle management, and automated access reviews. This helps eliminate excessive entitlements and prevent unauthorized access, thus reducing risk and aligning with CMMC's requirements for secure identity management.

3 Implement Zero-Trust Access Controls

A zero-trust model is central to the security requirements of CMMC 2.0. This approach requires continuously verifying every identity and device before granting access, ensuring sensitive information is only accessible to authenticated, vetted users. Omada Identity Cloud enables seamless enforcement of role-based access, control (RBAC), aids in enforcing multi-factor authentication (MFA), and provides continuous risk assessments—helping to ensure your organization maintains a security posture that is fully aligned with evolving CMMC standards and the zero-trust model.

4 Automate Evidence Collection and Reporting

Being audit-ready is essential. With CMMC 2.0's shift towards auditable evidence, automation can simplify data collection, tracking, and reporting. Omada Identity Cloud automates the collection, tracking, and reporting of compliance evidence, reducing the complexity and manual effort typically associated with audits. You can efficiently manage the required documentation, ensuring that assessments and audits are conducted smoothly, and compliance is easily demonstrated.

5 Strengthen Identity Governance and Administration (IGA)

CMMC 2.0 mandates consistent security controls across all environments, whether on-premises or in the cloud. Omada Identity Cloud provides unified governance across hybrid infrastructures, enabling secure collaboration and mitigating risk across both on-premises and multi-cloud environments. With real-time insights, policy-driven provisioning, and advanced analytics, you can improve visibility, reduce blind spots and ensure compliance.

Positioned for Success Under CMMC 2.0

By aligning with NIST SP 800-171, implementing robust IGA practices, adopting zero-trust principles, automating reporting, and providing unified oversight across your entire IT environment, organizations can successfully navigate the complexities of CMMC 2.0. Access official guidance from the DoD's CMMC website and integrate these strategies with Omada Identity Cloud to achieve readiness, strengthen security, and maintain a competitive edge in the Defense Industrial Base.

V022124

Omada

Omada simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences—without the complexities traditionally associated with identity governance.

© 2025 Omada A/S