CyberNINES®
COMPLIANCE WITHOUT COMPLEXITY®

CYBERNINES NIST SP 800-171 READINESS ASSESSMENT: YOUR PATH TO CMMC COMPLIANCE AND BEST PRACTICE

In today's ever-evolving cybersecurity landscape, protecting sensitive information is paramount, especially for those operating in the Defense Industrial Base (DIB). As cyberattacks continue to rise, it's critical for organizations to fortify their defenses and safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) shared within the DIB.

NIST SP 800-171 is the framework that the Department of Defense (DoD) requires all DIB contractors to meet today. Whether you are a prime contractor or a subcontractor, if you handle DoD CUI, you need to be compliant. And it is just as good for securing all the critical data in your business, not only the DoD's data. Today, this is an acquisition requirement flowed down through DFARS 252.204-7012.

WHAT ABOUT CMMC?

That's where the DoD's Cybersecurity Maturity Model Certification (CMMC) program comes into play. It's a program developed by the DoD to enhance the security measures of the DIB. CMMC goes beyond the self-attestation approach of DFARS 252.204-7012 by introducing a comprehensive third-party independent verification component. CyberNINES is the twenty-sixth company in the U.S. to have undergone the rigorous CMMC assessment to become a Certified Third-Party Assessor Organization (C3PAO).

Estimates suggest that approximately 80,000 out of 300,000 DIB companies will need to comply with CMMC Level 2. Once the CMMC rule-making process is complete and the CMMC DFARS is implemented, if your company handles DoD CUI that is considered Controlled Technical Information (CTI) and you seek to provide goods and services to the DoD, you must obtain CMMC certification before being eligible for contract awards. The phased rollout is expected to include CMMC regulations in DoD solicitations starting in late 2024, with all DIB Level 2 companies required to achieve CMMC certification by Fiscal Year 2026.

To help your organization navigate this transformative journey toward CMMC Level 2, we introduce the CyberNINES NIST SP 800-171 Readiness Assessment, a comprehensive pre-assessment that determines your readiness for the CMMC Voluntary Assessment or CMMC Level 2 Assessment, ensuring you're fully prepared to meet the stringent requirements set forth by the DoD.

By leveraging the expertise of CyberNINES, you gain a strategic advantage in securing your data and bolstering your cybersecurity posture. Our evaluation gives you invaluable insights into your organization's strengths and weaknesses, empowering you to make informed decisions and implement needed controls.

Don't wait until it's too late. Stay one step ahead of cyber threats, and position your organization for success in the defense industry. Partner with CyberNINES and embark on your NIST SP 800-171/CMMC journey today. Achieve the highest level of confidence and credibility with CMMC certification, setting the stage for growth, trust, and continued collaboration with the DoD.

CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

2200 Pennslyvania Ave.
Madison, WI 53704

CyberNINES LLC | CyberNINES.com | (608) 512-1010

Visit cyberAB.org to validate

CyberNINES®
COMPLIANCE WITHOUT COMPLEXITY®

NIST SP 800-171 READINESS ASSESSMENT

YOUR READINESS JOURNEY - READINESS ASSESSMENT MADE SEAMLESS

Achieving CMMC certification may seem daunting, but with CyberNINES as your trusted partner, it becomes a seamless and efficient process. Preparing for CMMC Level 2 Assessment requires meticulous attention to detail and a streamlined approach, which is why our RA mirrors the format of an actual CMMC Level 2 Assessment.

Step 1: Discovery

We start by providing you with intuitive intake forms, which allow us to gather essential information and documentation to ensure a tailored, accurate assessment.

Step 2: Scoping Call

Our experienced lead assessor engages with you in a comprehensive discussion regarding artifact gathering, interview approach, and test approach. We work closely with you to create a customized plan that aligns with your organization's requirements and goals.

Step 3: Determining Your Preparedness to Proceed

We now provide you with an insightful determination of your preparedness to proceed with the RA. If we find that you're not quite prepared, don't worry. You can still choose to continue with the RA, or you can request a CyberNINES Gap Analysis, which clearly explains each failed practice and recommends remediation steps. It's a valuable opportunity for you to bridge any gaps and strengthen your cybersecurity measures.

Step 4: Point of Contact

To ensure a seamless experience, we recommend you designate an Organization Seeking Certification Point of Contact to work with our lead assessor. This individual serves as your liaison with us, facilitating communication and coordination throughout the assessment process.

Step 5: Onsite Review

We might recommend an onsite evaluation of specific practices, particularly physical access control and monitoring, personnel control during system maintenance, secure digital and physical storage of CUI, and proper identification of media containing CUI.

Step 6: Assessing Your Readiness

We use a variety of methods—examination of your specifications, procedures, and activities; interviews with the responsible individuals; and tests comparing actual with expected behavior—to determine your readiness for formal assessment.

Step 7: Report/Presentation

Our comprehensive report provides a clear breakdown of each practice, indicating whether it is "Met," "Not Met," or "Not Applicable." This helps you easily gauge your organization's compliance status and identify areas for needed improvement.

Step 8 (optional): Remediation Recommendations

At your request, we provide a detailed assessment for each practice that has fallen short. Our report outlines why a particular practice failed and recommends remediations. We empower you with actionable insights, equipping you to make informed decisions and implement effective measures.

AN IMPORTANT NOTE ON CONSULTING SERVICES

If you choose to consult with CyberNINES as part of the RA (i.e., gap analysis or remediation recommendations), we cannot perform a future Voluntary Assessment or CMMC C3PAO Assessment. You will need to obtain that service from another C3PAO. This separation guarantees an unbiased evaluation, setting the stage for a fair and rigorous assessment process in the future.

ABOUT CYBERNINES

CyberNINES is a Service-Disabled Veteran-Owned Small Business (SDVOSB) focused on cybersecurity services that provide high-value and affordable CMMC & NIST SP 800-171 assessments, audits, and compliance management to small and medium-sized businesses within the DoD Supply Chain. Our solutions include Government Cloud solutions for Controlled Unclassified Information (ITAR and 600 Series) to meet DFARS 252.204-7012, 7019, and 7020 regulations and virtual CISO services to limit the cybersecurity risk posture of suppliers and primes. CyberNINES is a CMMC Registered Provider Organization (RPO) and a CMMC Third-Party Assessment Organization (C3PAO). Schedule a free consultation by sending us an email at inquiry@cybernines.com.

CYBER AB
CMMC CERTIFICATION
AUTHORIZED C3PAO

Visit cyberAB.org to validate

2200 Pennslyvania Ave.
Madison, WI 53704

CyberNINES LLC | CyberNINES.com | (608) 512-1010