CyberNINES
COMPLIANCE WITHOUT COMPLEXITY®

Basic Assessment

CyberNINES utilizes the NIST SP 800-171 framework to complete our Basic Assessments. NIST SP 800-171 is a business-oriented cybersecurity standard that provides guidelines, technical specifications, recommendations, and annual reports to help keep your business information safe.

CyberNINES Basic Assessment Approach

01. DISCOVERY

- Policy and Procedure Review
- Business Process Review
- Employee Behavior Audit
- Network, Systems and Application Review

02. ANALYSIS

- Procedure vs Behavior
- Review domain settings and gather data
- Review endpoint antivirus, host firewall status, screen lock, etc.
- Findings Measured Against NIST SP 800-171

03. REPORT GENERATION

- System Security Plan (SSP)
- Plan of Actions and Milestones (POAM)
- Executive Summary Presentation with Results and Recommendations

04. REPORT PRESENTATION

- Presentation of Findings
- Schedule of Follow Up

CyberNINES®
COMPLIANCE WITHOUT COMPLEXITY®

Our audit will work to identify any and all gaps in existing behavior, policy, and infrastructure that are required to be filled for compliance.

We deploy experienced onsite auditors to develop a strong understanding of your business operations while investigating gaps in standard compliance to be addressed and mitigated. In-depth reports will be provided where the standards are detailed, and mitigation techniques are defined.

After completion of our Basic Assessment audit your business will be able to fully self-attest to DFARS 252.204-7008, 7012, 7019 and 7020.

01. SYSTEM SECURITY PLAN (SSP)

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.

02. PLAN OF ACTIONS AND MILESTONES (POAM)

Documents known gaps in compliance, or non-traditional mitigation techniques used for compliance, along with action plan to ensure compliance is met.

03. NIST SP 800-171 ASSESSMENT SCORE

Per the new interim final rule that went into effect all new contract awards after November 30, 2020 will need to submit their score from a basic assessment to the Supplier Performance Risk System (SPRS) at https://www.sprs.csd.disa.mil/

04. SUPPORT IN OBTAINING REQUIRED DIGITAL CERTIFICATE

In order to report cyber incidents in accordance with DFAR 7012, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/. The reporting requirement is 72 hours of an incident.

At CyberNINES®, we know what it takes to get ready to achieve CMMC certification & we want to help you on your compliance journey.