



SECURITY DUE DILIGENCE CHECKLIST

The merger of IT and OT networks raises the importance of protecting all sensitive data — especially if one carries the Controlled Unclassified Information (CUI) within its network. To ensure cybersecurity readiness and compliance with government regulations, it is important to implement basic, critical actions against common cyberattacks. Based on the NIST SP 800-171 framework, this checklist provides few best practices to develop your security due diligence program.

Are you getting ready to sell your company or evaluating potential acquisition targets? Bring CyberNINES in to make sure you are complying with current DoD cybersecurity regulations. In post acquisitions, CyberNINES can help you meet compliance with DFARS 7012, 7019 and 7020 and support integration efforts.

- ☐ Review and define CUI in organization's systems
- ☐ Develop and enforce organization's cybersecurity policies
- ☐ Implement an employee training program on cybersecurity best practices and awareness
- ☐ Enable multi-factor authentication (MFA)
- ☐ Ensure the use of unique and complex passwords
- ☐ Provide and maintain inventory of network connections, including connected devices and applications
- ☐ Review company's network access and permissions
- ☐ Establish automated data backup
- ☐ Install firewall and anti-virus software, and leverage malware protection
- ☐ Ensure end-to-end encryption of data storage
- ☐ Develop Incident Response & Disaster Recovery policies

NIST SP 800-171 CONTROL FAMILIES

Access Control

Audit & Accountability

Identification & Authentication

Media Protection

Physical Protection

Security Assessment

Systems & Communications
Protection

Awareness & Training

Configuration Management

Incident Response

Maintenance

Personnel Security

Risk Assessment

System & Information Integrity



SECURITY DUE DILIGENCE

ABOUT CYBERNINES


CyberNINES is a Service-Disabled Veteran-Owned Small Business (SDVOSB) focused on cybersecurity services that provides high value and affordable CMMC Pre-Assessment Readiness Review & NIST SP 800-171 assessments, audits and compliance management to small and medium size business within the DOD Supply Chain. Our solutions include Government Cloud solutions for Controlled Unclassified Information to meet DFAR regulations and virtual CISO services to limit the security risk posture of suppliers and primes.

OUR SERVICES INCLUDE

- PCI DSS, HIPAA, NIST SP 800-171 & CMMC Pre-Assessment Readiness Reviews for Level 1 and Level 3
- DFARS 252.204-7012, 7019 and 7020 compliance assessments
- Plan of Actions and Milestones (POAM) – Creation and on-going management
- Managed Security & Compliance Services – Protecting companies by providing management and support services with annual audits and security-focused services
- Help posting your NIST assessment score into the Supplier Performance Risk System (SPRS)

**Let us help you work,
secure and prosper.**

Contact Us:

 608.512.1010

 Inquiry@CyberNINES.com

OUR SECURITY PARTNERS

CyberNINES uses a variety of tools to provide enterprise-level cybersecurity services to our clients. We have partnered with industry leading providers and organizations bringing you the best practices in cybersecurity and compliance methodology to help small and medium-sized manufacturers meet NIST SP 800-171 and CMMC framework requirements.