CMMC - DFARS NIST 800-171 Compliance Services

DFARS NIST 800-171 Assessment Services

Are you really DFARS 252.204.7012/NIST 800-171 compliant? All DoD contracts require compliance now!

Are you Prepared for CMMC? Do you have a Roadmap from DFARS to CMMC?

DoD leadership is profoundly concerned about contractor cybersecurity and protecting DoD supply chains from cyber-attack is a top priority.

DoD has stated that traditional measures of contractor performance cost, schedule and quality are insufficient to measure contractor cyber security. Limited adoption of NIST 800-171 self-certification standards prompted the DoD to seek third-party auditor verification that contractors adopt and maintain an appropriate level of cyber security.

By developing an auditable process, the Cybersecurity Maturity Model Certification (CMMC), DoD mandates measurable standards for third-party verified cyber security for all contractors.

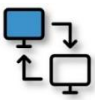
All DoD contractors must meet CMMC standards in order to hold a DoD contract starting in FY2021.

A leader in NIST 800-171 compliance support, LP3 offers a fixed price NIST 800-171 assessment to include a System Security Plan, POA&M, and a roadmap plan to get your company to CMMC compliance in time to continue to receive DoD contract awards.

CMMC – DFARS NIST-171 Assessment Deliverables

- Draft System Security Plans (**SSP**)
- Plan of Action & Milestone (**POA&M**) Report on gaps and remediation information
- Supplier Performance Risk System (**SPRS**) Registration and NIST 800-171 Compliance Score
- Draft policies cross-referenced to NIST SP 800-171 Controls and associated CMMC practices
- Draft CMMC Roadmap customized to achieve CMMC L3 compliance over the next 12 months

Over the past years, LP3 helped many businesses comply and can do the same for you. Our efficient process delivers inspection ready compliance documents quickly.



ASSESSMENT

COMPLIANCE

CONTINUOUS MONITORING

LP3 also delivers affordable military-grade remediation support and solutions. LP3's cybersecurity governance and compliance team brings more than 35 years of Cyber Security experience to secure your company.

Compliance Support Services

In order to maintain your current compliance status, there are several controls within the CMMC / NIST 800-171 Framework that need to be maintained on a Periodic basis. The following cost-effective services have been developed by LP3 for small and medium businesses to meet these requirements.

LP3 Continuous Monitoring (ConMon) Support Services
External Penetration and Internal Penetration Testing
Internal Credentialed Vulnerability Scanning
Staff Security Awareness Assessment/Training (Including Phishing, Vishing, testing)
Virtual CISO (V-CISO) Services
Monitor Client's Mandated Security Compliance Regulations and Advise on Updates
Handle Responses to Security Compliance Questions from Clients' Customers
Perform Ongoing System Security Plan (SSP) Review and advise on needed updates
Perform Ongoing Review of Client's Security Policies and advise on needed updates
Manage Plan of Action & Milestone (POA&M) for MSP or Local IT
Ensure that IT assets including operating systems, applications, databases, and network devices are compliant with policy and standards.
Perform Monthly/Quarterly Review of System and Network Audit reports and External/Penetration and Internal Vulnerability Scans and update POA&M.
Conduct Yearly Security Assessment & Compliance Review
Security Assessment (CA) Practices Supported by LP3 Services
Periodically assess controls in organizational systems to determine if the controls are effective. (**ID: 3.12.1, CA.2.158**)
Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. (**ID: 3.12.2, CA.3.159**)
Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. (**ID: 3.12.3, CA.3.161**)
Develop, document, and update system security plans that describe system boundaries system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.(**ID: 3.12.4, CA.2.157**)
System & Information Integrity (SI) Practices Supported by LP3 Services
Perform periodic scans of organizational system and real-time scans of files from external sources as files are downloaded, opened, or executed. (**ID: 3.14.5, SI.1.213**)
Audit & Accountability (AU) Practices Supported by LP3 Services
Provide audit reduction and report generation to support on-demand analysis and reporting Services (**ID: 3.3.6, AU.3.052**)
Awareness & Training (AT) Practices Supported by LP3 Services
Provide security awareness training on recognizing and reporting potential indicators of insider threat. (**ID: 3.2.3, AT.3.058**)

Compliance Less Complicated

Learn More Today!

CyberHELP@lp3.com

https://LP3.com

LP3 Headquarters

PO Box 710628
Oak Hill, VA 20171
Phone: 855-573-5625

LP3 Syracuse, New York
Phone: 315-992-5678

About LP3:
LP3 was formed in 2004 as a high-tech cyber security services firm supporting mission critical DoD systems. LP3 is a Service-Disabled Veteran Owned Business and proudly hires veterans as an equal opportunity employer.

Most employees hold TS/SCI clearances and are DoD 8570 certified professionals.

DUNS: 145055211
CAGE: 3SYQ8
NAICS: 541512, 541519, 541690, 541330, 541511, 541990

LP3 Brings Military-grade Cyber Security Solutions to Businesses