Veltec Networks

Is Your Business Compliant with The New DFARS/NIST Requirements?

What DoD Contractors Need to Know About Controlled Unclassified Information (CUI) & Using a Technology Solutions Provider to Ensure Compliance with the DFARS and NIST.

Today, more than ever, the Department of Defense (DoD) relies on external contractors and suppliers to carry out a wide range of missions. Sensitive data is shared with these companies and must be protected. Inadequate safeguards for this sensitive data may threaten America's National Security and put our military members at risk.

In response to this threat, the DoD has implemented a basic set of cybersecurity controls through DoD policies and the Defense Federal Acquisition Regulation Supplement (DFARS). The DFARS rules and clauses apply to the safeguarding of contractor/supplier information systems that process, store or transmit Controlled Unclassified Information (CUI). These security controls must be implemented at both the contractor and subcontractor levels based on information security guidance developed by the National Institute of Standards and Technology (NIST) Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."

As a U.S. DoD contractor who collects, stores, or transmits Covered Defense Information (CDI) or Controlled Unclassified Information (CUI) you must comply with NIST (The National Institute of Standards and Technology) regulations 800-171 and DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012. Your subcontractors must comply as well and be able to maintain compliance. If you don't, you can't bid on DoD contracts, and you may lose the ones you have.

The Department of Defense enforces a specifically defined set of cybersecurity controls through the DFARS. The DFARS rules and clauses apply to the safeguarding of contractor/supplier information systems that process, store or transmit Controlled Unclassified Information (CUI). These security controls must be implemented by both you, the contractor, and your subcontractors according to levels based on information security guidance developed by the National Institute of Standards and Technology (NIST).

Finding everything you need to know about DFARS regulations and NIST cybersecurity guidance to ensure that your technology is compliant can be a daunting task. Using the services from a Technology Solutions Provider who has expertise in DFARS and NIST requirements is essential if you want to attain compliance and remain compliant.

Complying with DFARS and NIST requirements isn't easy. You and your subcontractors must meet DFARS cybersecurity standards and NIST Guidelines, or you can't apply for DoD contracts. To do this requires a complete scoping and readiness assessment to measure your compliance. You must then remediate any identified gaps in security.

To do this requires the support from a Technology Solutions Provider who specializes in providing compliance solutions. The right IT Provider will help you understand the risks of storing Controlled Unclassified Information in your IT system, and what you must do to comply. Your Provider should also be adept at conducting gap analyses services, vulnerability scans, and penetration testing to ensure your IT security.

Your Requirements as a DoD Contractor

Cyberattacks have reached epidemic proportions in the U.S. Even government agencies are at risk of breaches. This poses a real risk to National Security. It's imperative that you, your personnel and your subcontractors safeguard classified information and Controlled Unclassified Information. The security of the U.S. Government depends upon the measures you take as a contractor, as well as those in your supply chain. Unfortunately, many businesses don't have the right cybersecurity controls in place like firewalls, anti-virus and anti-malware, and identity-authentication processes. They also lack detection and response controls for IT exploits.

Until now, strict security processes, controls, and standards that applied to federal information systems weren't required for CUI. The DFARS 225.204-7012 and NIST SP 800-171 regulations were developed to cover unclassified federal information for nonfederal organizations. You must implement the security controls outlined in the NIST SP 800-171 to be compliant with DFARS.

The U.S. Government provided a disciplined and structured process for contractors to follow. If you want to comply and be accepted for DoD projects, you must leverage the following IT solutions.

- Security Information and Event Management
- Intrusion Prevention System
- Vulnerability and Threat Management
- Database Security Controls
- Log Management
- File Integrity Checking
- A Tested Incident Response Plan

The Right Technology Solutions Provider Will:

- ***Identify Information Security Gaps*** in your system design, architecture policies, and planning exercises.
- ***Utilize Advanced Security Engineering*** for remediation and enhancements so there are no interruptions in IT service.
- ***Deploy Cyber Operations Support*** with proven methods to maximize your operational security.
- ***Conduct Continuous Risk Management*** with a proactive rather than reactive approach.
- ***Use Advanced Cyber Security Testing*** to identify vulnerabilities in your IT assets that are at risk for cyber attacks.

What Specifically is Covered by the DFARS/NIST Regulations?

The DFARS 252.204-7012 | NIST SP 800-171 requirement for CUI includes any information related to a DoD performance contract, as well as anything that supports the contract. This is a very broad requirement and could have a dramatic impact on the number of systems that must be covered.

These systems are broken down into four categories:

1. **Controlled Technical Information:** Any and all technical information as defined by DoD, including those with space or military applications.

2. **Operations Security Information:** Any intentions, capabilities or activities that an attacker could use to guarantee failure or unacceptable consequences.

3. **Export-Controlled Information**, like biochemical or nuclear data.

4. **Any additional information** specified in the contract.

The new rule also applies to your subcontractors. They must meet the same applicability definitions described above.

As a DoD Contractor, you must know what CUI you store, process, or transmit in the course of performing your duties. You and your subcontractors must be prepared to apply NIST SP 800-171 security controls to your information systems. You must create and sustain an environment for the proper storing, processing, or transmitting of CUI. This includes ensuring your employees or any individuals involved in the contract practice security and privacy when it comes to information systems.

As you can see, this broad scope of requirements demands the expertise of a Technology Solutions Provider who can develop, deploy and enhance a secure and compliant environment for your CUI processing needs. You need one who can engage with stakeholders to identify the key security objectives and critical requirements to develop a prioritized IT roadmap, information security architecture, security controls and operations that comply with the DFARS 225.204-7012 and NIST SP 800-171 Guidelines.

Minimum cybersecurity standards are described in NIST Special Publication 800-171 and broken down into fourteen areas:

1. Access Control - You must limit system access to authorized users.
2. Awareness & Training - You are required to promote awareness of the security risks associated with users' activities, train them on applicable policies, standards and procedures, and ensure they are trained to carry out their duties.

3. Audit & Accountability - You must create, protect, retain and review all system logs.

4. Configuration Management - You are required to create baseline configurations and utilize change management processes.

5. Identification & Authentication - You must authenticate information systems, users, and devices.

6. Incident Response - You're required to develop operations to prepare for, detect, analyze, contain, recover from, and respond to incidents.

7. Maintenance - You must perform timely maintenance on your information systems.

8. Media Protection - You must protect, sanitize and destroy media containing CUI.

9. Personnel Security - You're required to screen individuals before authorizing their access to information systems, and ensure these systems remain secure upon the termination or transfer of individuals.

10. Physical Protection - You must limit physical access to and protect and monitor your physical facility and support infrastructure that houses your information systems.

11. Risk Assessment - You are required to assess the operational risk associated with processing, storage, and transmission of CUI.

12. Security Assessment - You must periodically assess, monitor and correct deficiencies and reduce or eliminate vulnerabilities in your organizational information systems.

13. System & Communications Protections - You must monitor, control and protect data at the boundaries of your system, employ architectural designs, software development techniques and system engineering principles that promote effective information security.

14. Protection System & Information Integrity - You're required to identify, report and correct information and any flaws in your information in a timely manner. You must also protect your information systems from malicious code at appropriate locations, and monitor information security alerts and advisories so you can take appropriate actions.

Plus, there are specific security requirements comprising 110 individual controls that you and your subcontractors must implement in each of these areas.

Large enterprises probably have these security systems in place. Smaller businesses probably don't–And this is a big undertaking. With the right experience in CUI requirements, your TSP can help by handling these responsibilities for you. They can:

- Periodically assess the security controls in your company's systems to determine if the controls are effective in their application.
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in systems.

- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
- Develop, document, and periodically 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.

As a DoD contractor, you and your authorized employees must fully understand what Covered Defense Information you store, process, or transmit in the course of doing business with the Department of Defense. You must also be ready to provide adequate security using controls outlined in the NIST SP 800-171, Security and Privacy Controls for Non-Federal Information Systems.

Your Technology Solutions Provider must be adept at integrating methodologies for incorporating security and privacy into business solutions. They should leverage the following services:

- **Compliance Services** that include security awareness training, information technology security training, computer-based training classes, IT oversight, system registration and categorization, and continuous monitoring planning.
- **Risk Management Services** via successful risk management programs and concise, actionable risk assessments.
- **A 24/7 Virtual Network and Security Operations Center** (VNSOC) with a team of highly trained, certified and experienced network and security analysts that monitor your network and systems around the clock with log management.

- **Security Assessments** that utilize the latest trends in data protection, technology advancements, and legislative changes, and that test the security posture of your information systems.
- **Security Controls** that determine how to implement NIST SP 800-171 R1 security requirements.
- **Identity, Credential & Access Management** (ICAM) to simplify the identification, credentialing and assessment of your IT infrastructures to ensure privacy, security, privacy, compliance, and efficiencies.
- **Cyber Incident Reporting** to plan, develop and execute testing of a cyber-incident plan.
- **Response and Recovery Service** if a cyber event is confirmed. Your TSP should support and advise you during the Incident Response lifecycle. Your TSP should immediately preserve and protect all evidence and capture as much information about the incident as possible. They should review your networks to identify compromised computers, services, data, and user accounts and identify specific covered defense information that may have been lost or compromised. You must always be helpful and transparent with the DoD and cooperate with them to respond to any security incidents.

Meeting the SP 800-171 is not a one-time fix – Rather it's a continuous assessment, monitoring and improvement process.

Your TSP should periodically assess the security controls in your company's systems to determine if the controls are effective in their application. They should develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in systems.

They must monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls that are in place. And, they should develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with connections to other systems.

If the Department of Defense determines that other measures are required to provide adequate protections and security, you and your subcontractors may also be required to implement additional precautions.

It's essential that you stay up to date on these requirements if you want to keep your standing with the DoD or to bid on future contracts. Again, your Technology Solutions Provider is your best friend where this is concerned.

Veltec Networks

For more information, contact Veltec Networks at (408) 849-4441 or info@veltecnetworks.com.