NIST 800-171 / DFARS 7012

Business Compliance Guide

CYBER MANAGEMENT SYSTEMS

People • Process • Technology

Business Compliance Guide

Overview

This guide will provide an in-depth overview of all you need to know about NIST SP 800-171 security requirements, the DFARS 252.204-7012 clause, the risks associated with non-compliance, and how to prepare for compliance.

The new NIST SP 800-171 security compliance requirements are already causing concern, if not panic, among many federal and defense contractors. The new standards are meant to prevent the theft of sensitive data, which have been targeted by hackers. In October 2017, U.S. officials acknowledged that hackers stole sensitive information about the F-35 Joint Strike Fighter from an Australian military supplier. According to ZDNet, the hackers faced few challenges in accessing the Australian defense contractor's system. The company was small, with a one-person IT department and lackluster security measures. The attacker reportedly had access to the company's network for at least three months.

The NIST SP 800-171 is a complex requirement. Consequently, very few large federal and defense contractors have met the associated mandatory requirements, and smaller contractors and subs are still learning how the compliance requirements impact their current and future contracts. As cybercrime escalates globally, compliance is a critical component in securing business systems and data from both domestic and foreign hackers. Cyber Management Systems has compiled this essential NIST SP 800-171 / DFARS Business Compliance Guide as an informative and compelling overview on the compliance requirements. We've mapped out the risks associated with non-compliance, and the recommended steps to meet the NIST SP 800-171 and DFARS 7012 requirements.

Business Compliance Guide

Contents

What is NIST SP 800-171

To comply with NIST SP 800-171, Non-Federal Organizations must meet the NIST SP 800-171 security standard.

The National Institute of Standards and Technology (NIST) has issued Special Publication (SP) 800-171 Revision 1 that establishes a minimum security standard for “protecting controlled unclassified information in Non-Federal information systems and organizations”. Revision 1 also added the requirement to create a detailed Plan of Action that describes how any unimplemented security requirements will be met and how any planned mitigations will be implemented.

To comply with this standard, contractors must document the state of their information system in a ‘system security plan’ and document how and when they will implement any ‘not yet implemented’ requirements in associated plans of action.

NIST SP 800-171 also mandates that federal contractors bring multifactor authentication into their organizations. In other words, you must have more than just a single password as your security controls.

To comply with this standard, organizations must fully understand what (and how) controlled unclassified information is stored, processed and/or transmitted while doing business with the federal government.

Business Compliance Guide

What is DFARS 252.204-7012

In October 2016, the Department of Defense (DoD) issued rule 252.204-7012 that changed the DFARS regarding Safeguarding Covered Defense Information and Cyber Incident Reporting. In essence, this provision required DoD contractors to provide adequate security to safeguard “covered defense information” (CDI) on its unclassified information systems that support the performance of work under a DoD contract.

In addition, upon contract award contractors have only 30 days to complete their DFARS CDI assessment and report their findings to the DoD Chief Information Officer. To demonstrate compliance, the contractor must produce a report detailing any gaps in control compliance for the information systems to be used in support of contract completion.

Contractors must also report cyber incidents that may affect their unclassified information systems and/or the covered defense information that may reside therein. These cyber incidents are defined in the regulations. In addition, the 252.204-7012 requirements do flow down. This means that prime contractors must incorporate this clause into their subcontracts, thereby mandating that the subcontractors also safeguard CDI according to the 252.204-7012 clause.

In essence, this provision requires DoD contractors to provide adequate security to safeguard “covered defense information” (CDI) on its unclassified information systems that support the performance of work under a DoD contract, and must had completed this process no later than December 31, 2017.

Business Compliance Guide

Failure To Comply

Contractors that fail to comply with the DFARS 252.204-7012 clause, which calls for the implementation of NIST SP 800-171, face many risks and potentially serious consequences, including some that could be crippling to their business.

Here are just a few implications of non-compliance:

- **Termination for Default**

A government agency may well be within their rights to terminate a contract for failure to comply with mandated cyber security and IT requirements. This is no surprise when you consider the inherent danger cyber attacks and data breaches, not to mention the potential loss of confidential data, can cause to a contracting organization.

- **Breach of Contract**

Because the NIST 800-171 and/or DFARS clause is a specified requirement of the funding agency's contract, failure to comply with the clause's security requirements can be considered a breach of the contract. If noncompliance is caused by the subcontractor, the prime contractor will be held responsible and will then look to the subcontractor to resolve the situation.

- **Liquidated Damages**

If there is sensitive personal information involved, government agencies may add provisions into the contract around liquidated damages. Liquidated damages can range from $35 to $5,000 per affected individual in the agency's contracts. Also, it's not uncommon for prime contractors to flow down provisions on liquidated damages to their subcontractors.

- **False Claims Act**

Both prime and subcontractors can be held liable under the False Claims Act if they submit any false information, including invoices or security documentation. Failure to comply with NIST SP 800-171 and/or DFARS 252.204-7012 can open a contractor up to allegations of violations of the False Claims Act.

Business Compliance Guide

What steps do I take to become compliant?

NIST SP 800-171 R1 specifies 14 separate categories that a government contractor must comply with to satisfy the DFARS 252.204-7012 clause:

- **Access Control**
- **Awareness and Training**
- **Audit and Accountability**
- **Configuration Management**
- **Identification and Authentication**
- **Incident Response**
- **Maintenance**
- **Media Protection**
- **Personnel Security**
- **Physical Protection**
- **Risk Assessment**
- **Security Assessment**
- **System and Communications**
- **Protection**
- **System and Information Integrity**

To address these areas, NIST 800-171 and DFARS 7012 compliance requires a combination of documented procedures and technology controls. Overall, 110 controls exist across these 14 security control families.

Following are the specific steps federal contractors and defense contractors must take to become compliant:

1. Conduct a gap analysis against NIST SP 800-171 R1.
2. Create a Security Plan according to NIST SP 800-18.
3. Develop a Plan of Action to address security gaps.
4. Report gap analysis and Plan of Action to Contracting Officers and/or the DoD CIO within 30 days of award.
5. Prepare to meet rapid reporting requirements within 72 hours of incident discovery.
6. Flow down the requirements to covered subcontractors.

While there can be multiple methods of completing the steps above, including minimizing the scope of covered data and systems, Federal contractors and DoD contractors have a fundamental choice on how to meet the NIST 800-171 and DFARS requirement. As a contractor approaches its strategy for compliance, it needs to consider many factors, including company size, workforce stability, expected growth, use of subcontractors, IT expertise in building and operating a NIST 800-171 / DFARS-compliant infrastructure, and availability of cash for capital expenditures.

Business Compliance Guide
What steps do I take to become compliant?

❖ Option 1

Upgrade and continually manage an on-premise IT system based on the NIST cyber security framework. This framework is organized as follows:

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

The on-premise choice may provide advantages for large companies with a very stable workforce, especially if they do not use a lot of subcontractors. While this choice does require a greater upfront capital investment and an extensive IT staff, it can provide for greater customization of the IT infrastructure.

❖ Option 2

Outsource IT systems that store or process controlled unclassified information to a hosting vendor that specializes in supporting government contractors with NIST, DFARS, FAR, and ITAR requirements.

By outsourcing, instead of shouldering all the compliance risk yourself, you can share and shift some of the compliance risk to a third party and enable your company to focus resources on meeting your customers' mission requirements. This choice offers a lower upfront capital cost and reduces or eliminates the need to hire additional IT personnel. Also, when you build an on-premise IT system, you commit to an infrastructure and size that meets your existing and anticipated needs. When you outsource, you get greater flexibility to staff up and staff down during the natural progression of contract lifecycles.

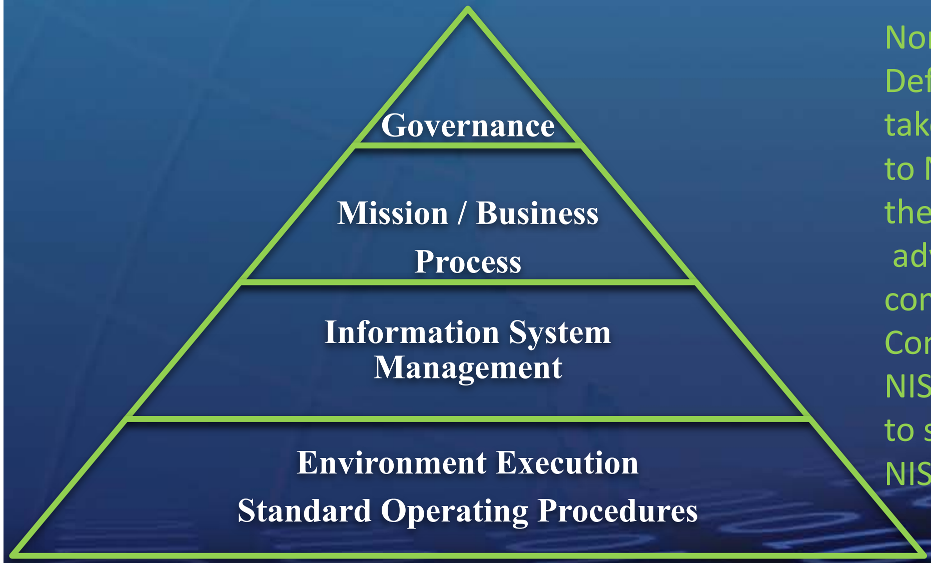
Business Compliance Guide
The Cyber Management Systems Solution

Cyber Management Systems offers a multi-tier NIST SP 800-171 compliant solution that: satisfies the NIST 800-171 and DFARS 252.204-7012 requirement to safeguard CUI, CTI and CDI, implements continuous monitoring and delivers cyber incident reporting. Many non-federal organization and defense contractors are realizing that developing their own internal cyber security and incident reporting initiative puts the security of all their systems, equipment and data at risk while also incurring significant upfront costs.

Our solution incorporates all the essential end-to-end steps, services, deliverables and technology for a single, reasonable monthly/annual cost. Cyber Management Systems aligns our services and infrastructure with industry-leading partners to deliver compliant documentation materials, secure communications and productivity tools along with a seamless, protected data cloud for non-federal organizations and defense contractors.

Here’s what you can expect:

1. Comprehensive gap analysis identifying vulnerabilities against NIST SP 800-171 R1.
2. Identification of information systems that process, store, or transmit CUI, CDI, or CTI.
3. Professionally Written Information Security Program (WISP) on day 1.
4. Formal System Security Plan(s) for submission to Contracting Officers and/or the DoD Chief Information Officer.
5. Documented Plan of Action to become NIST 800-171 / DFARS 7012 compliant.


Governance
Mission / Business Process
Information System Management
Environment Execution Standard Operating Procedures

Non-Federal Organizations and Defense contractors who take a proactive approach to NIST SP 800-171 compliance put themselves at a distinct competitive advantage. Make the move to a compliant, secure solution today! Contact us at NIST-800-171@cybermss.com to schedule a complimentary NIST 800-171/DFARS consultation.

About Cyber Management Systems

Cyber Management Systems, based in the Washington, DC region is a SDVOSB Information Technology consulting firm offering customized solutions to federal, state, local governments and private/public businesses.

Our main areas of focus are Enterprise IT Systems Monitoring, Cyber Security Management & Consulting, and IT Consulting.

Cyber Management Systems has the focus, energy, commitment, and discipline required to implement the right solution to meet all of our customer requirements. We are right sized to provide the agility and flexibility to adjust to customer priorities, and changes in day-to-day operational needs resulting from real life situations.

Let Cyber Management Systems help you manage your People, Processes, and Technologies!

Contact Cyber Management Systems for your free consultation!

NIST-800-171@cybermss.com

(301) 613-3717