NeoSystems®

Grow Ahead... We've Got Your Back Office.®

DFARS 7012 Survival Guide

This guide will provide an in-depth overview of all you need to know about the DFARS 252.204-7012 clause, the NIST SP 800-171 security standard, the risks associated with non-compliance, and how to prepare now for the December 31, 2017 (aka DFARS 2017) deadline.

The new Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012 clause is already causing concern, if not panic, among many defense contractors. With the December 31 deadline quickly approaching, contractors are scrambling to understand what to do and how to do it.

The DFARS 7012 is a complex regulation. Consequently, very few enterprise 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. NeoSystems, along with GBprotect, Citrix®, R&K Cyber Solutions and VMware® have compiled this essential DFARS Survival Guide as an informative and compelling overview on the compliance regulation. We've mapped out the risks associated with non-compliance, and the recommended steps for helping your organization meet the DFARS 7012 requirements.

NeoSystems®
Grow Ahead... We've Got Your Back Office.®

Contents

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 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 complete this process no later than December 31, 2017.

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 complete this process no later than December 31, 2017.

NeoSystems
Grow Ahead... We've Got Your Back Office.

What is NIST SP 800-171

To comply with DFARS 7012, defense contractors must also 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 nonfederal 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, organizations must fully understand what (and how) controlled unclassified information is stored, processed and/or transmitted while doing business with the federal government. In addition, organizations must provide adequate documentation regarding their technology solutions and processes, along with proof of their ability to detect and respond to incidents.

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.

What happens if you don't comply with these regulations?

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 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 DFARS 252.204-7012 can open a contractor up to allegations of violations of the False Claims Act.

NeoSystems
Grow Ahead... We've Got Your Back Office.

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, 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 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 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, DoD contractors have a fundamental choice on how to meet the 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 DFARS-compliant infrastructure, and availability of cash for capital expenditures.

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	Anomolies 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 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.

NeoSystems®
Grow Ahead... We've Got Your Back Office.®

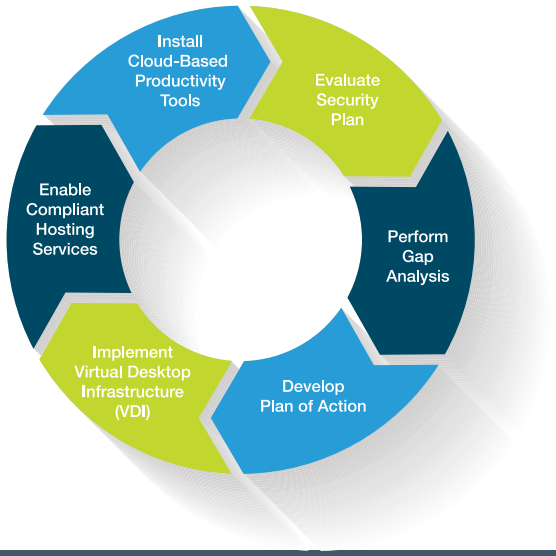
The NeoSystems DFARS Solution

NeoSystems offers a 360-degree NIST SP 800-171 R1 compliant solution that: satisfies the DFARS 252.204-7012 requirement to safeguard CDI, implements continuous monitoring and delivers cyber incident reporting. Many 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 cost. NeoSystems aligns our services and infrastructure with industry-leading partners such as GBprotect, Citrix®, R&K Cyber Solutions and VMware® to deliver compliant documentation materials, secure communications and productivity tools along with a seamless, protected data cloud for defense contractors.

Here's what you can expect:

1. Comprehensive gap analysis identifying vulnerabilities against NIST SP 800-171 R1
2. Formal Security Plan for submission to DoD Chief Information Officer
3. Documented Plan of Action to become DFARS 7012 compliant
4. Virtual desktop infrastructure (VDI) to safeguard data access
5. Compliant cloud-based hosting services to protect Controlled Unclassified Information (CUI) and Covered Defense Information (CDI)
6. Secure, cloud-based productivity and communications tools



GBprotect
Personalized Approach • Better Security

CITRIX®

R&K CYBER SOLUTIONS
YOUR GLOBAL SOLUTIONS EXPERT

vmware®

Defense contractors who take a proactive approach to DFARS compliance put themselves at a distinct competitive advantage. Make the move to a compliant, secure solution today!

Contact us at DFARS@neosystemscorp.com to schedule a complimentary DFARS 7012 consultation.

Our Partners

GBprotect

Who They Are

GBprotect is a comprehensive Managed Security Services Provider. They have managed security events for thousands of devices internationally and have the bandwidth of 24-hour staff and industry-leading Security Operations Centers.

Solution Value

GBprotect's Security Control Assessment services are designed to identify gaps in control compliance and to present the identified gaps alongside actionable remediation guidance.

Citrix

Who They Are

Citrix technology makes the world's apps and data secure and easy to access, empowering people to work anywhere and at any time. Citrix provides a complete and integrated portfolio of Workspace-as-a-Service, application delivery, virtualization, mobility, network delivery and file sharing solutions that enables IT to ensure critical systems are securely available to users via the cloud or on-premise and across any device or platform.

Solution Value

Citrix XenApp is an application virtualization solution that helps you optimize productivity with universal access to virtual apps, desktops, and data from any device. Citrix XenDesktop carries all the same functionality as XenApp, plus the option to implement a scalable VDI solution.

R&K Cyber Solutions

Who They Are

R&K Cyber Solutions LLC (R&K) is a leading, ISO 27001:2013 certified award-winning provider of Computer Network Defense (CND) Services in the Government and Commercial market. As a 2017 award recipient of the Top 10 Vulnerability Management Solution Providers from Enterprise Security Magazine, R&K a Cyber proactive defense platform to mitigate the risks of malware exposure and breaches.

Solution Value

R&K is a trusted partner throughout the entire incident handling life cycle both on-site and remotely as a Managed Security Service Provider (MSSP). R&K CND procedures are driven by industry best practices, such as DoD CJCSM 6510.01b and NIST Special Publications, and provide custom security for sensitive data. All R&K CND services ensure compliance with DFAR Clause 252.204-7012 and NIST 800-171.

VMware

Who They Are

VMware is a global leader in cloud infrastructure and digital workspace technology. With VMware solutions, organizations are improving business agility by modernizing data centers and integrating public clouds, driving innovation with modern apps, creating exceptional experiences by empowering the digital workspace, and safeguarding customer trust by transforming security.

Solution Value

VMware Horizon 7 is the leading platform for virtual desktops and applications. Horizon 7 provides a streamlined approach to delivering, protecting and managing virtual desktops (VDI) and apps while containing costs and ensuring that end uses can work anytime, anywhere, across any device.

NeoSystems
Grow Ahead... We've Got Your Back Office.

Grow Ahead with NeoSystems!

Contact NeoSystems Corp
for your free consultation!

(888) 676-6367

DFARS@neosystemscorp.com

About NeoSystems

NeoSystems delivers strategic back office services and solutions - Accounting & Finance, Contract Management, Human Capital, Information Technology, and Hosting (SSAE 16 SOC 1/SOC 2) – for high-compliance organizations, including government, government contractors, non-profit, and commercial organizations. Leveraging best-of-breed technology and in-depth expertise, our team enables companies to improve vital operations, reduce their overhead costs, and stay compliant with complex requirements.