CLARUS

DFARS Interim Rule Guide

What Businesses Working with the Government Need to Know

INTRODUCTION

DFARS Interim Rule:

Building upon the NIST SP 800-171 Framework

Many cybersecurity regulations in both the government andcommercial sectors havebeen implemented andare continuing to be rolled out due to the continued aggressive cyber-attacks.

If your company provides products or services for the Department of Defense (DoD), you will be required to meet new cybersecurity standards set by the Defense Federal Acquisition Regulation Supplement (DFARS).

DFARS provides a set of security controlsto safeguard information systems where contractor data resides. Currently,cybersecurity is based on the National Instituteof Standards and Technology (NIST),the NIST Special Publication 800-171 "Protecting Controlled Unclassified Information (CUI) in Non-Federal Information Systems and Organizations". Since 1997 the implementation of NIST SP 800-171 has been required for all contracts handling CUI and for these organizations to implement the security controls throughout all levels of their supply chain.Companies without full compliance are required to have a Plan of Action and Milestones (POAMs) mapping their progress toward compliance.

Over the past few years, the current method of self-assessments and cyber requirements used in DFARS standards has proved insufficient as the DoD supply chaincontinues to be subjected to cyber attacks,leading to the necessity of more immediate improvements to cybersecurity.

Effective since November 30, 2020, the DefenseAcquisition Regulation Systemreleased a new DFARS Interim Rule to supplement the current DFARS regulations as a procedure that helps bridge the gap between NIST SP 800-171 and CMMC, while CMMC is still being enacted. The DoD makes the case in the DFARS Interim Rule that contractors who were self attesting to compliance with DFARS were not actually making the necessary changesto their systemsand processes to meet the requirements.

As a result,the new DFARS 70 Series:7012, 7019, 7020, and 7021 are intendedto close the gap betweenDFARS and CMMC in order to address the need for better security.

Required in the DFARS InterimRule is a new Self-Assessment Scoring and Reporting requirement. DoD contractors who handle controlled unclassified information (CUI) are very familiar with the NIST SP 800-171 security requirements, which requirecontractors to self-assess their cybersecurity preparedness. The NIST SP 800-171DoD Assessment Scoring Methodology detailed in the Interim Rule will help contractors grade themselves with a standardized score that reflectsthe NIST SP 800-171 requirements they do not yet have in place.

The new requirement applies to all contractors subject to the DFARS 252.204-7012 clause based on handling of CUI and prime contractors must also require their subcontractors and suppliers meet this DFARS Interim Rule.

The Steps in this guide defines the actions your business needs to take to meet these DFARS compliance requirements.

Highlights of the DFARS Interim Rule:

- The DFARS Interim Rule is an expansion of DFARS NIST 800-171 requirements and is a procedure that helps bridge the gap between the two requirements while CMMC is still being enacted.

- Even if you have recently completed an assessment, contractors and subcontractors need to complete a new NIST 800-171 Self-Assessment based on the new scoring methodology and report on their scores in the Supplier Performance Risk System (SPRS) before a contract can be awarded.

- Along with your new Assessment Score, you must include the completion of your **System Security Plan (SSP)** and **Plan of Action and Milestones (POAMs)** describing the current state of your systems and networks and your outlined proposal to meet full compliance with the NIST 800-171 requirements.

- The DFARS Interim Rule applies to all contractors subject to the DFARS 252.204-7012/7019/7020 clauses based on their handling of Controlled Unclassified Information (CUI).

- The DFARS Interim Rule requirement applies to all contracts and sub-contracts that include any of these clauses, even if you are not actually accessing, processing, or storing Controlled Unclassified Information (CUI).

Step 1: Complete the New Assessment for NIST SP 800-171 Compliance

Requirement 3.12.1 of NIST 800-171 states that you “periodically assess the security controls in organizational systems to determine if the controls are effective in their application.”

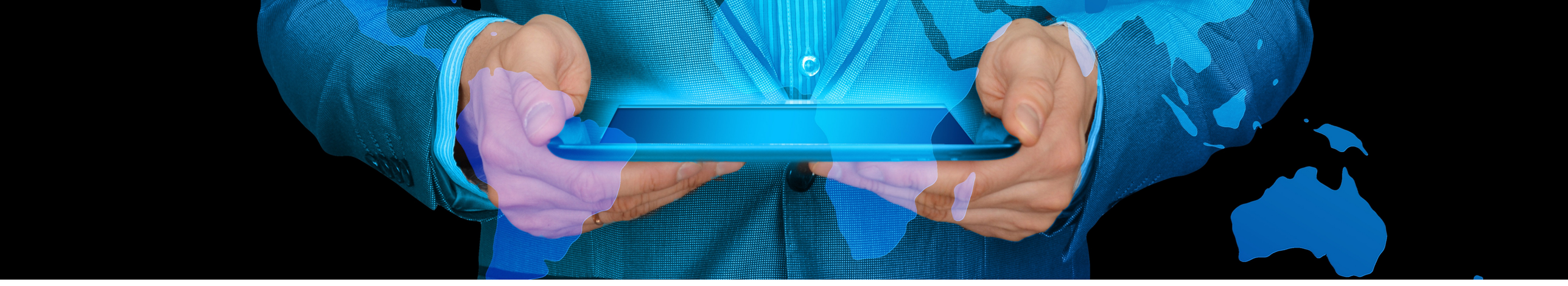
The new DFARS clause 7019 requires contractors to maintain a record of their NIST 800-171 compliance within the **Supplier Performance Risk System (SPRS)**. Even if you had a previous assessment completed, you will need to do a new assessment that incorporates the new scoring methodology and then record the score and other required information into the SPRS before contracts will be awarded. The new NIST 800-171 Self-Assessment is based on a Basic, Medium, and High scoring methodology.

- **Basic:** Similar to the self-assessment and self-attestations that have been previously required in the NIST 800-171 requirements.
- **Medium and High:** NIST 800-171 assessments run by the Defense Contract Management Agency (DCMA).

SPRS Reporting

If you do not have an account with SPRS, you will need to request access through the Procurement Integrated Enterprise Environment (PIEE). To submit your new assessment to SPRS, you must fill out:

- Your System Security Plan (SSP) name
- CAGE code associated with the SSP
- A brief description of the System Security Plan (SSP) architecture
- The date the assessment was completed
- Your total score
- The date that you can achieve a score of 110 security requirements



Step 2: Create and Maintain a System Security Plan (SSP)

Requirement 3.12.4 requires contractors to develop, document, and periodically update a System Security Plan (SSP) that describes your organization’s system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

The SSP information will also be entered into the Supplier Performance Risk System (SPRS). Your organization should describe in the SSP how the specified security requirements are met or how your organization plans to meet the requirements.

Your SSP should accurately reflect your actual implementation of the controls and will likely the first thing asked for in the event of an audit.

Step 3. Document Plan of Action & Milestones (POAMs)

Requirement 3.12.2 requires contractors to develop and implement a Plan of Action and Milestones (POAMs) designed to correct deficiencies and reduce or eliminate vulnerabilities in their organization’s systems.

Most organizations will not have met all 110 security requirements so the POAMs document describes the gaps and the mitigation plans.

The gaps should be identified during your assessment and POAMs should be documented. Also, the POAMs should contain plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented.

Organizations can document the System Security Plan and Plan of Action & Milestones as separate or combined documents.

Each company's POAMs is different because it includes information about weaknesses and gaps according to NIST 800-171 standards, as well as the risk postures for each respective gap and any mitigating steps your company intends to make. Not every company will decide to address every risk in the same way and are based on business decisions with operational and financial implications.

Step 4. Implement the Required Controls

The SSP and POAMs are critical inputs to an overall risk management strategy and documents how your organization processes, stores, and transmits CUI data.

You will need to execute your SSP and POAMs to meet compliance with NIST SP 800-171.

Document and implement your plans to leverage internal and external resources to maintain compliance. Compliance should be actively maintained daily and not as an annual activity on a check off list.

Key questions to ask within your organization:

- How will you detect, respond and report security breach incidents within the required 72 hour reporting window?
- What are your plans in managing your subcontractors and suppliers to meet compliance requirements?
- How will you update your SSP and POAMs as your business and IT infrastructure changes?

Maintaining compliance is an often overlooked aspect of achieving compliance. You will need to demonstrate compliance by automating and documenting your efforts for sustained success.

How Clarus Tech Partners Can Help

CLARUS

About Clarus Tech Partners

The Clarus Tech Partners team have extensive experience in cybersecurity, data compliance regulations, and government contracting.

Our team provides consulting, advisory and training solutions for businesses working across business sectors – government, financial services, technology, real estate, retail, ecommerce – to help your business navigate and achieve your industry-specific regulatory compliance mandates.

We provide affordable and customized NIST and DFARS Interim Rule solutions and support for your organization and provide the assessments, roadmap, documentation, policies & procedures, remediation steps, implementation, training, and on-going maintenance controls to prepare your business for government compliance.

We have expertise in technology, data protection, project & risk management, and privacy regulation to address your cybersecurity risks and data privacy compliance requirements in the U.S., Europe, and globally.

Contact us for an initial consultation and questions about meeting NIST 800-171 and DFARS Interim Rule compliance.

Clarus Tech Partners
Phone : 646-926-3850
Email: Info@ClarusTechPartners.com
Website: ClarusTechPartners.com