AN OFFERING IN THE BLUE CYBER SERIES:

Get Your SPRS On!
Implementing and Documenting Compliance with NIST SP 800-171

Version 14 March 2022
#3 in the Blue Cyber Education Series
Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contains many FARS and DFARS, some are listed some are referenced and you have to look them up. These are not all, but some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (DFARS) contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public.

DFARS Clause 252.239-7010, Cloud Computing Services

DFARS Clause 252.204-21, Basic Safeguarding of Covered Contractor Information Systems

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS Clause 252.204-7008, Compliance with safeguarding covered defense information controls

DFARS Clause 252.204-7009/20 NIST SP 800-171 DoD Assessment Requirements.

DFARS Clause 252.204-7021, Cybersecurity Maturity Model Certification Requirement

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information
Safeguard Covered Defense Information (CDI)

To safeguard covered defense information contractors/subcontractors must implement NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations

The covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171

- The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.
- The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO
Safeguard CDI: What is CUI?

The DOD CUI Registry and detailed training on what constitutes CUI is available from the DOD at this link: https://www.dodcui.mil
Controlled Technical Information (CTI) means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled technical information is to be marked.

The term does not include information that is lawfully publicly available without restrictions.

"Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items"

Examples of technical information include: research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
NIST SP 800-171 System Security Plan (SSP)

Optional Template available on NIST.Gov

Optional Template to record the Plan of Action on NIST.gov

For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110.

For example, failure to limit system access to authorized users (Basic Security Requirement 3.1.1) renders all the other Access Control requirements ineffective, allowing easy exploitation of the network.

- 23 Basic Security Requirements have a value of 5 points

For example, failure to control the use of removable media on system components (Derived Security Requirement 3.8.7) could result in massive exfiltration of CUI and introduction of malware.

- 19 Derived Security Requirements have a value of 5 points
NIST SP 800-171 DoD Assessment Requirements

This clause applies to covered contractor information systems that are required to comply with the NIST SP 800-171, in accordance with DFARS clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

Supplier Performance Risk System (SPRS) is a sophisticated website is ready to record your Self-Assessment and SSP information. Link [https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf](https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf)

The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment.
The Requirement in DFARS Clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements

In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment for each covered contractor information system that is relevant to the contract.

A Basic Assessment, which is a self-assessment, assigned a low confidence level (because it is self-generated) is:

- Based on the Contractor’s review of their system security plan(s) associated with covered contractor information system(s)
- Conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology
How to enter a Basic Assessment Data into SPRS

Post or email your business’ summary level scores of a current NIST SP 800-171 DoD Assessment to SPRS for all covered contractor information systems relevant to the contract.

Your entry consists of

1. A system security plan (NIST SP 800-171 item 3.12.4) supporting the performance of a DoD contract—

2. Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement) using the NIST SP 800-171 DoD Assessment Methodology

3. Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171

The SPRS website offers numerous training videos which will help you get an account and make your entry
How to enter a Basic Assessment Data into SPRS

SPRS Basic Assessment data entry fields

Example output of SPRS Basic Assessment

You Have Help with the NIST MEP Handbook

NIST Manufacturing Extension Partnership (MEP) Handbook will walk you through all 110 requirements and provide a list of process and policy documents you would create to have a robust CUI protection program.
You Have Help with NIST SP 800-171A, Assessing Security Requirements for CUI

- The NIST SP 800-171A provides nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements.

- The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments.
Why NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations?

The NIST SP 800-171 was written using performance-based security requirements to enable contractors to use systems and practices they already have in place to process, store, or transmit CUI.

- It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection.
- Though most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, some require security-related software or additional hardware.
Will the DoD monitor contractors to ensure implementation of the required security requirements?

The DFARS rule does not add any unique/additional requirements for the DoD to monitor contractor implementation. ...

- **By signing the contract**, the contractor agrees to comply with the terms of the contract.
- The contractor’s system security plan (SSP) – required by NIST SP 800-171 - documents how the organization meets, or plans to meet, the NIST SP 800-171 requirements.
  - When requested by the requiring activity, the SSP (or elements of the SSP) may be used to demonstrate implementation of NIST SP 800-171 or to inform a discussion of risk between the contractor and requiring activity.
- If a subcontractor does not agree to comply with the clause, CDI should not be on that subcontractor’s information system.
References

- Supplier Performance Risk System (SPRS) ([https://www.sprs.csd.disa.mil/](https://www.sprs.csd.disa.mil/))
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil

➤ Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!

Every Tuesday, 1pm Eastern, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVvE0Qg