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
- FAR 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 252.204-7019/20 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)

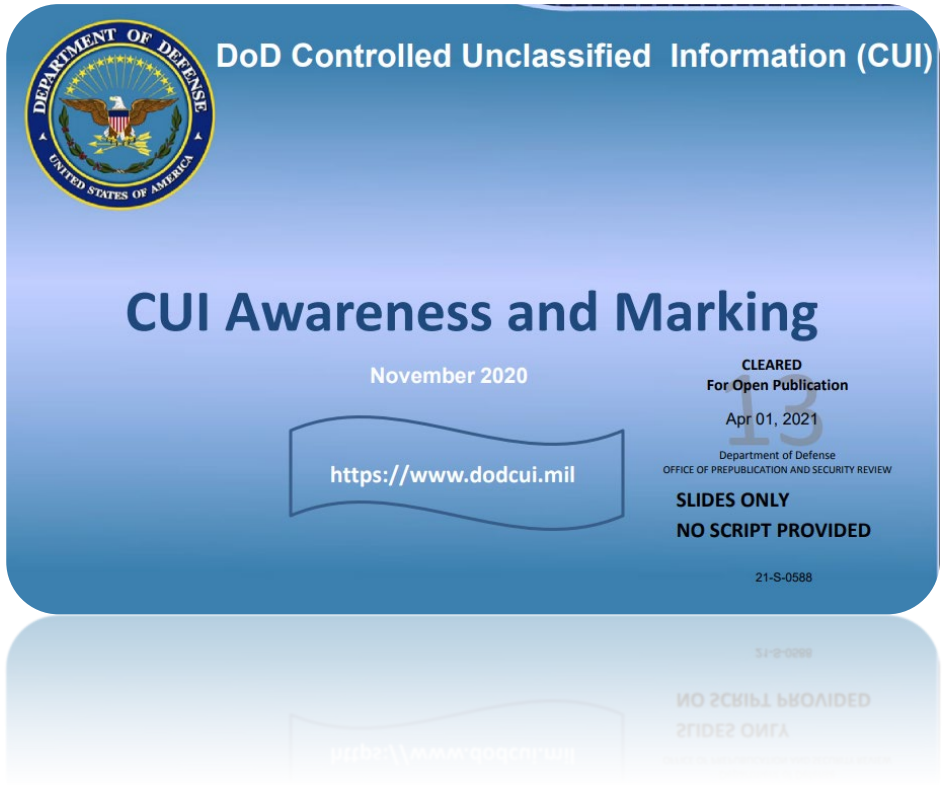
To safeguard covered defense information contractors/subcontractors **must implement NIST SP 800-171**, Protecting CUI in Nonfederal Information Systems and Organizations

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



Safeguard CDI: What is CTI?

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.

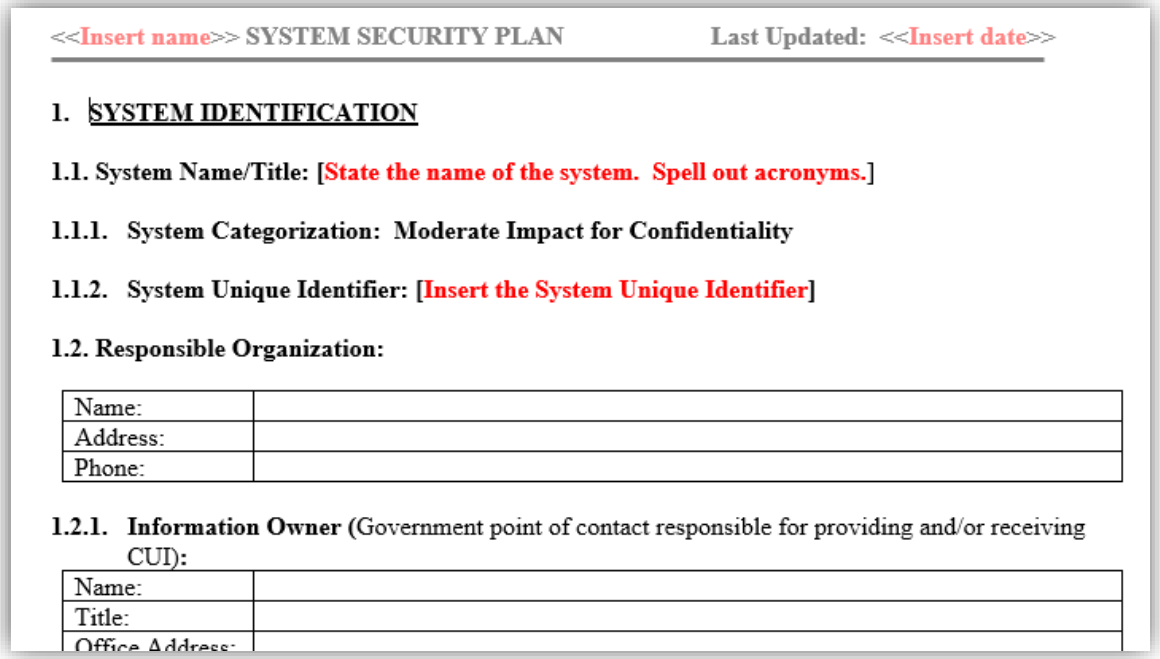
Controlled technical information is to be marked.

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)



<<Insert name>> SYSTEM SECURITY PLAN Last Updated: <<Insert date>>

1. SYSTEM IDENTIFICATION

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

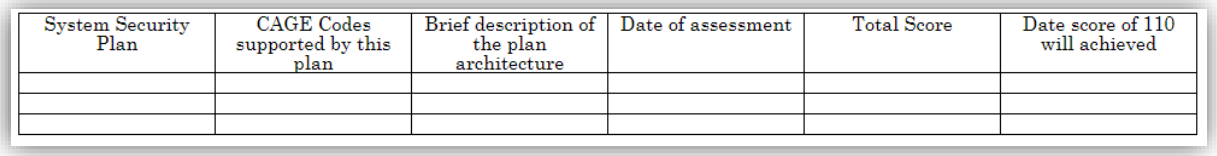
1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI):

Name:	
Title:	
Office Address:	

Optional Template available on NIST.Gov



System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

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

NIST SP 800-171 DoD Assessment Methodology

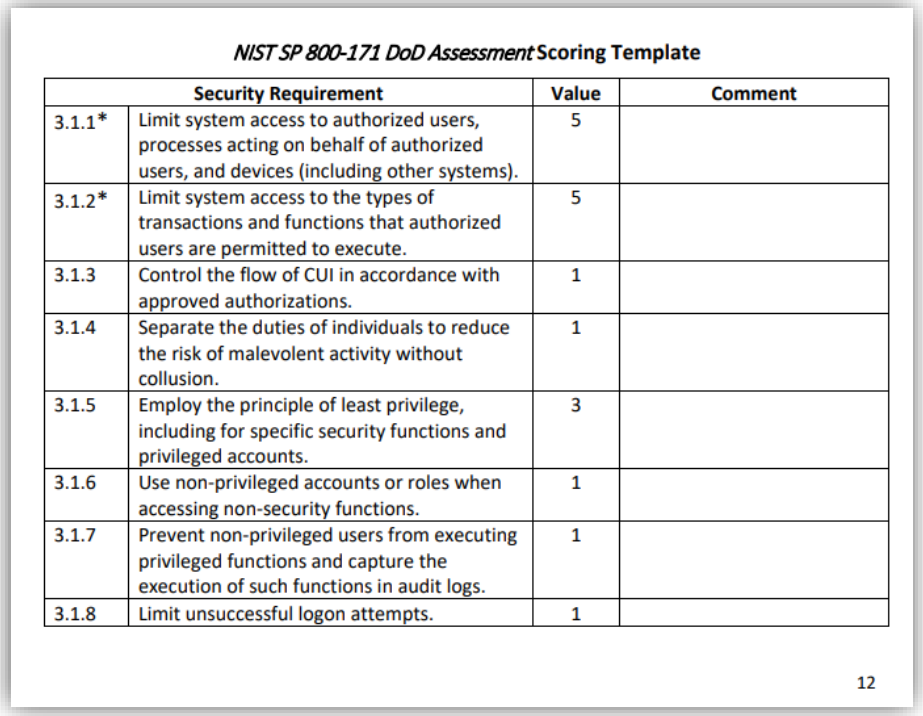
For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110.

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 Scoring Template

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

12

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

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

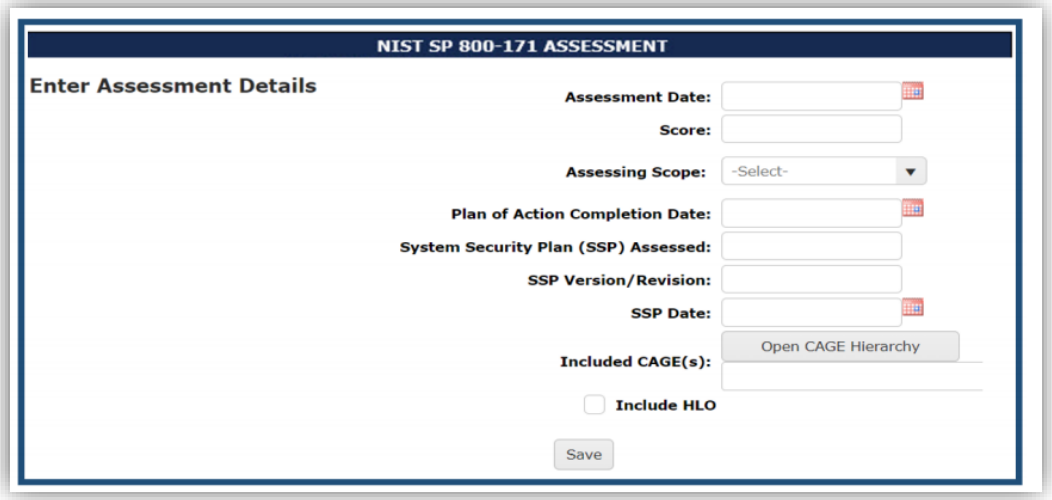
1. **A system security plan** (NIST SP 800-171 item 3.12.4) supporting the performance of a DoD contract—)

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

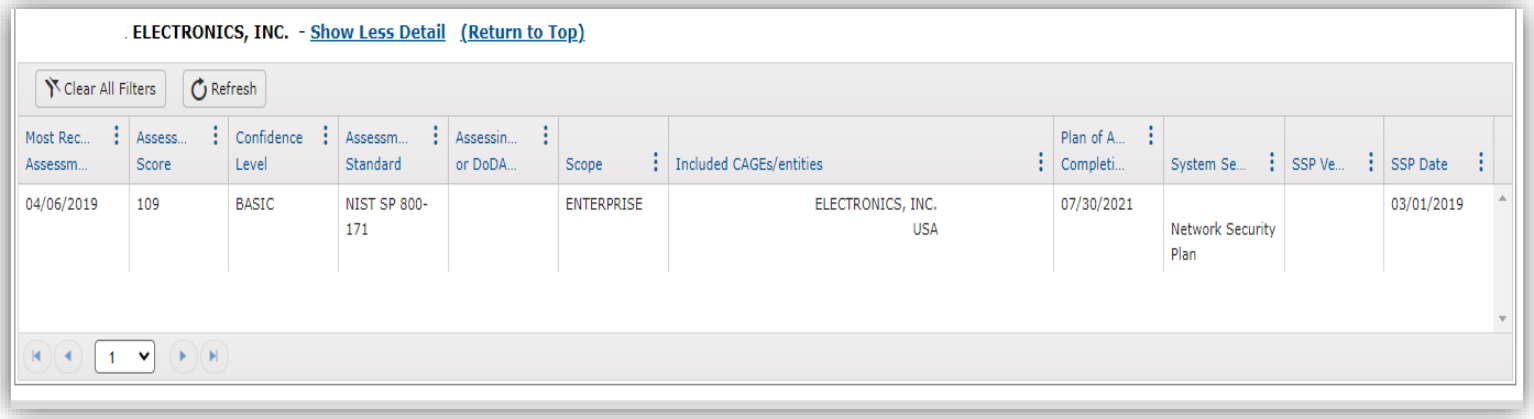
3. **Date that all requirements are expected to be implemented** (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171

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



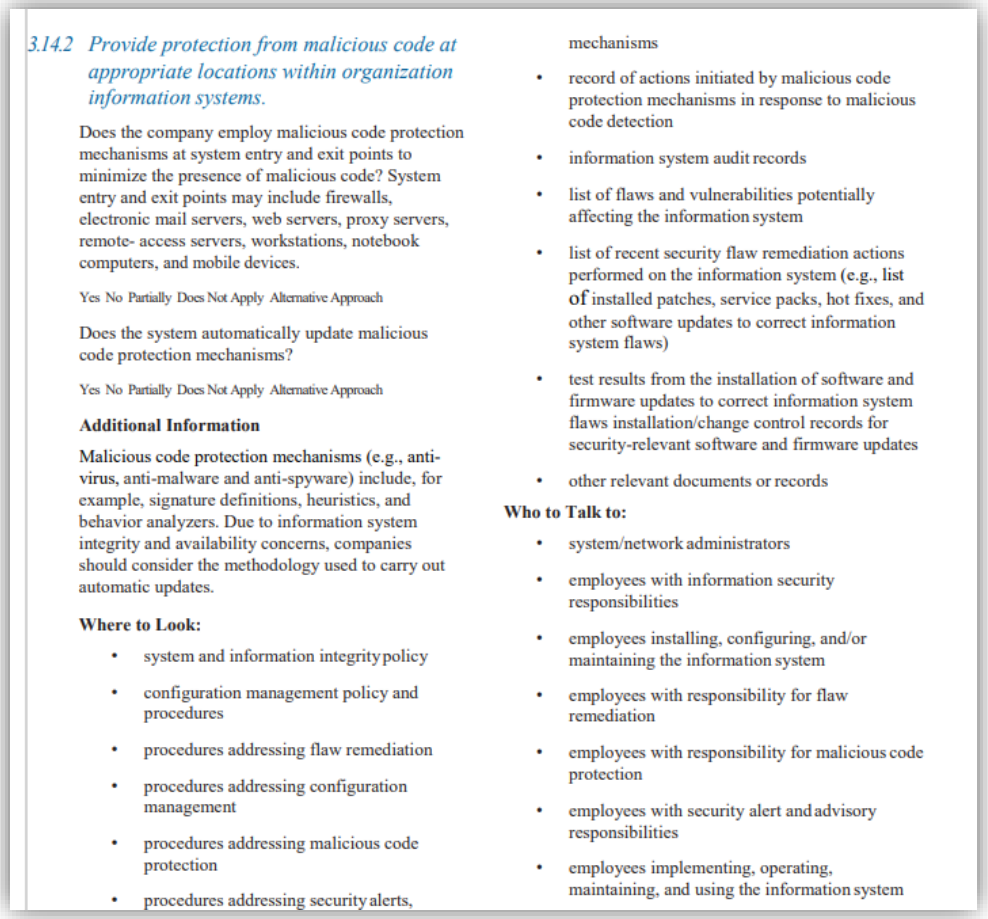
SPRS Basic Assessment data entry fields



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



3.14.2 Provide protection from malicious code at appropriate locations within organization information systems.

Does the company employ malicious code protection mechanisms at system entry and exit points to minimize the presence of malicious code? System entry and exit points may include firewalls, electronic mail servers, web servers, proxy servers, remote- access servers, workstations, notebook computers, and mobile devices.

Yes No Partially Does Not Apply Alternative Approach

Does the system automatically update malicious code protection mechanisms?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

Malicious code protection mechanisms (e.g., anti-virus, anti-malware and anti-spyware) include, for example, signature definitions, heuristics, and behavior analyzers. Due to information system integrity and availability concerns, companies should consider the methodology used to carry out automatic updates.

Where to Look:

- system and information integrity policy
- configuration management policy and procedures
- procedures addressing flaw remediation
- procedures addressing configuration management
- procedures addressing malicious code protection
- procedures addressing security alerts, mechanisms
- record of actions initiated by malicious code protection mechanisms in response to malicious code detection
- information system audit records
- list of flaws and vulnerabilities potentially affecting the information system
- list of recent security flaw remediation actions performed on the information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct information system flaws)
- test results from the installation of software and firmware updates to correct information system flaws installation/change control records for security-relevant software and firmware updates
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- employees installing, configuring, and/or maintaining the information system
- employees with responsibility for flaw remediation
- employees with responsibility for malicious code protection
- employees with security alert and advisory responsibilities
- employees implementing, operating, maintaining, and using the information system

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.

3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.2[a]	*designated locations for malicious code protection are identified.*
	3.14.2[b]	*protection from malicious code at designated locations is provided.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine:** [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records]. **Interview:** [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for malicious code protection; personnel with configuration management responsibility]. **Test:** [*SELECT FROM:* Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing employing, updating, and configuring malicious code protection mechanisms; mechanisms supporting or implementing malicious code scanning and subsequent actions].	

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.

AFWERX SBIR ★ STTR

References

- NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf
- NIST MEP Cybersecurity Self-Assessment Handbook https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf
- SPRS NIST SP 800-171 Quick Entry Guide https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
- NIST CUI SSP Template https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-1/final/documents/CUI-SSP-Template-final.docx
- NIST CUI Plan of Action Template https://csrc.nist.gov/CSRC/media//Publications/sp/800-171/rev-1/final/documents/CUI-Plan-of-Action-Template-final.docx
- Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/)
- NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information (the Assessment Standard) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf
- DOD CMMC Scoping Guidance and Assessment Guides
  (The Assessment Guides incorporate NIST SP 800-171, 171A and the MEP 162 Handbook – they are fantastic)
  at https://dodcio.defense.gov/CMMC/

AFWERX SBIR ★ STTR

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 at https://www.safcn.af.mil/Contact-Us/
  - 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.