AN OFFERING IN THE BLUE CYBER SERIES:

Can I give my contractor CUI? You need to ask.

Compliance with NIST SP 800 - 171

Version 14 March 2022

#4 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 252.204-7020 NIST SP 800-171 DoD Assessment Requirements.
- DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement

DFARS 252.204-7012
Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting

- The contractor creates a System Security Plan which addresses how each of the 110 NIST SP 800-171 has been implemented. Also, A Plan of Action and Milestone Date (POAM) is created for any incomplete NIST SP 800-171 security requirements.
- This DFARS calls out safeguarding CDI which is the data which is collected/developed/received/transmitted/used/ stored by the contractor in performance of contract.

DFARS 7012 “Adequate Security” quote red added for emphasis

… (b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor **shall implement, at a minimum, the following information security protections:**

…

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, 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,** “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor **shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.** …

DFARS 252.204-7008 Compliance with safeguarding covered defense information controls

This DFARS calls for the contractor to identify **an alternative but equally effective**, security measure to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

- For any POAM item, you need an alternative, but equally effective security measure

DFARS 252.204-7019/20
DoD Assessment Requirements

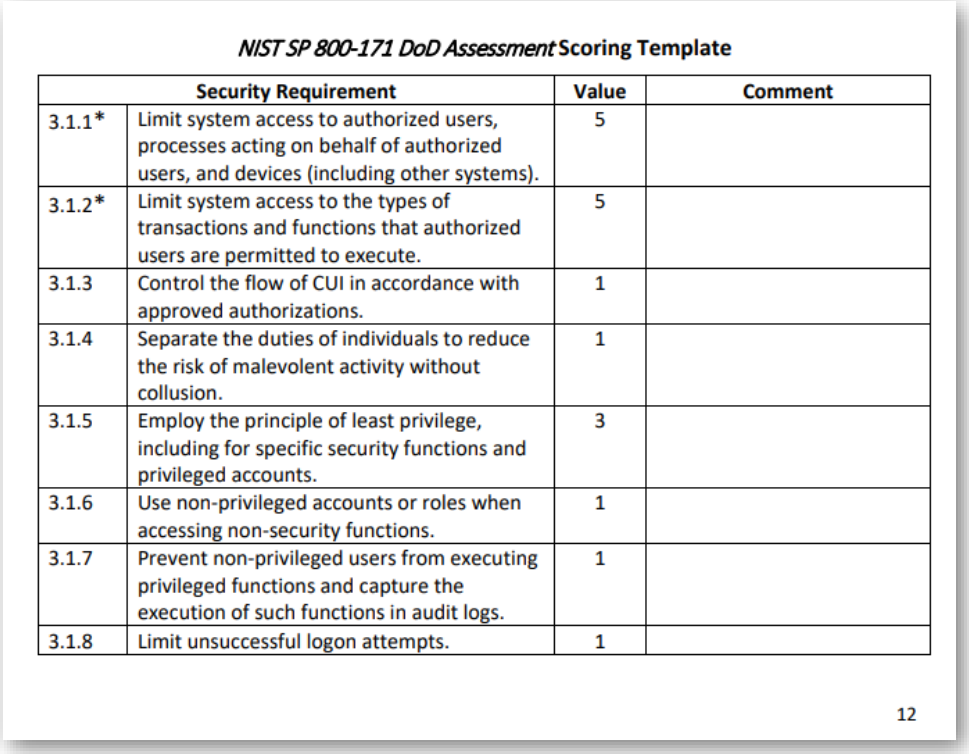
- This DFARS calls for the contractor conduct a self-assessment of NIST SP 800-171 using the **DOD NIST SP 800-171 Assessment Methodology** and the contractor System Security Plan and POAM; the result is an overall score.
- The contractor documents this self-assessment score in the SPRS system.

Not all of the NIST SP 800-171 security requirements are equal

The NIST SP 800-171 DoD Assessment Methodology identifies **42 security requirements** that, if not implemented, could lead to **significant exploitation of the network, or exfiltration of DoD CUI.**

These high-risk security requirements are worth 5 points in the DoD scoring rubric.

- **For example**, Failure to limit system access to authorized users (Requirement 3.1.1) **renders all the other Access Control requirements ineffective, allowing easy exploitation of the network**
- **For example**, Failure to control the use of removable media on system components (Requirement 3.8.7) **could result in massive exfiltration of CUI and introduction of malware.**



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

Answer today:
Can I give my contractor CUI? You need to ask.

- The decision to share CUI is a risk-based decision based upon a conversation with the contractor regarding if they are ready to provide **adequate security** to DoD CUI.
- There is not a cut and dried answer rubric.
- CUI protection is a shared responsibility between the DoD and industry.

If you need help with this decision, please contact your Program or Wing cybersecurity office. Also, Kelley Kiernan from the DAF CISO Office is available to talk with you. Keep your contracting officer informed of your activities.

This question is being studied across the DOD – check back for an updated answer

Discuss with the contractor their readiness to provide adequate protection for DOD CUI

Risk-Based Decision Questions

- Review the contractor's System Security Plan and associated POAM
  - Are all 42, 5-point weighted security requirements implemented with no POAM?
  - Are all 14, 3-point weighted security requirements implemented with no POAM?
- Is the CUI that the DAF is considering sharing with the contractor in a sensitive category such as these categories? NOFORN, FED ONLY, NOCON, DL ONLY, REL TO [USA, LIST], DISPLAY ONLY, Attorney-Client, Attorney-WP or otherwise sensitive?
- Is the CUI that the DAF is considering sharing with the contractor mission-essential?
- Is the CUI the DAF is considering sharing with the contractor appropriate for research?
- Have you rejected the use of synthetic data in this contract?
- Apply these questions to contractor-created CUI and the government-provided CUI

DOD SAFE creates potential exposure

DOD Safe will let a CAC-holder send CUI to any email address. You must ask contractors if they are ready to provide adequate protection to any CUI sent via DOD SAFE and be satisfied with the answer you receive.

- Contractors who are not ready to protect CUI should not accept CUI

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 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.