American Technology Services
a WWTS Company

ATS Webinar Series

February 3, 2021

First in a series presented by
American Technology Services and **OCD**TECH

"NIST 800-171 Self-Assessment and the CMMC"

Leslie Weinstein
CMMC Practice Lead,
OCD Tech

OCDTECH

in

Leslie Weinstein is an Army veteran and management consultant with 14 years of experience in intelligence and cyber operations, and strategy and policy consulting. She has eight years of experience in a joint environment, and four years of experience at the OSD level. Five years of active duty, complementing eight years as a federal civilian and consultant, provides a diverse and unique skill set that she has successfully leveraged to solve some of the most complex issues facing the Department of Defense.

Agenda

- DFARS Interim Rule
- NIST 800-171 Self Assessment
- CMMC Update Jan 2021

DFARS Interim Rule

- Defense Federal Acquisition Regulation Supplement (DFARS) Case 2019-D041
  - Effective December 1, 2020
  - Introduces the DoD Assessment Methodology
  - -7019 Clause
    - NIST 800-171 self-assessment (Basic assessment)
    - Supplier Performance Risk System (SPRS) score reporting
  - -7020 Clause
    - Government access to facilities, systems, and personnel
  - -7021 Clause
    - CMMC requirement

DFARS Interim Rule

-7019	Perform self-assessment using NIST 800-171A (Basic Assessment)
	Score self-assessment using DoD Assessment Methodology
	Report raw score and estimated completion date into SPRS
-7020	DoD may conduct a “higher” level assessment (Medium or High Assessment)
	Medium Assessment: DCMA review of contractor System Security Plan (SSP)
	High Assessment: Assessment by DoD personnel at a contractor's location and leverages the full NIST 800-171A assessment methodology

NIST 800-171 Self Assessment

- Leverage NIST 800-171A
- DoD Self-Assessment Methodology
  - Start with perfect score (110)
  - Subtract points for requirements not met

***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	

NIST SP 800-171 (Revision 2)

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

- 110 prescriptive controls
- Allows POA&Ms for gaps

3.1.1 **Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.

NIST SP 800-171A

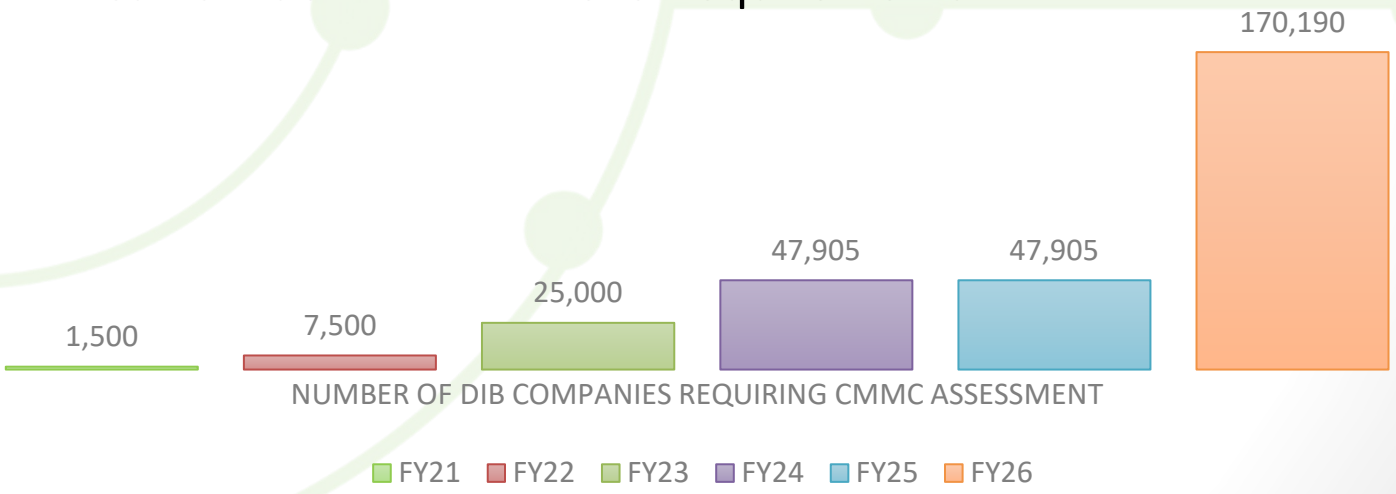
Assessing Security Requirements for Controlled Unclassified Information

- Catalogue of assessment objectives
- Potential assessment methods

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.1[a] *authorized users are identified.*
	3.1.1[b] *processes acting on behalf of authorized users are identified.*
	3.1.1[c] *devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d] *system access is limited to authorized users.*
	3.1.1[e] *system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f] *system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC Update

- CMMC pilot program until October 1, 2025
- 53 C3PAOs
  - 100 Provisional Assessors
  - None authorized to conduct CMMC assessments
- Default CMMC ML3 for pilot program
  - Primes flow down CMMC level requirements



Q & A

If you haven't already, please submit your questions in the Q&A Zoom window (access it by clicking "Q&A" icon)

Thank you for attending

We look forward to you joining us on ***March 3, 2021*** *in this continuing webinar series on CMMC / NIST 800-181.*

We will be reviewing ***"What is CUI and How Do I know if I have it?"*** *next!*

If you need to reach us or have topic suggestions for future sessions, please send us an email to:

webinars@networkats.com