DEFENSE CONTRACT MANAGEMENT AGENCY

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Overview

Presented By:

Ashley Johnson

Information Technology Cybersecurity Specialist, Security Assessor, DIBCAC (TDXBE)

20240813

Agenda

- Overview
- Assessments
- DoD & DCMA Impacts
- International Partnering
- Q&A Session

Overview - Who is DIBCAC?

- DIBCAC is a young DCMA organization that focuses on supporting the warfighter via security assessments to verify the protection of contractor managed systems storing, processing, and/or transmitting DoD Controlled Unclassified Information (CUI) data
- Established in 2019, DIBCAC only had 42 employees at that time
- In 2021, DIBCAC received additional funding to expand our capabilities for assessments, and the team began to grow
- We now have ~135 personnel including assessors, team chiefs, group chiefs, business operations divisions, training teams, and more

Overview – DoD Cybersecurity Timeline

- Why are security assessments necessary?
  - Contracts have thousands of Federal Acquisition Regulations (FAR) and Defense FAR Supplement (DFARS) requirements, with very few that addressed cybersecurity
  - In 2024, cybersecurity is now considered an essential part of any organization and is required
  - DoD Cybersecurity Timeline:
    - 2016 June: FAR clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*. It had 15 requirements for protecting data
    - 2016: 32 CFR 236, *DoD DIB Cybersecurity Activities,* required all DoD contractors to rapidly report cyber incidents that involved covered defense information on their contractor information systems, as well as any cyber incidents affecting their ability to provide operationally critical support to the DoD
    - 2017: DoDI 5000.02, *Operation of the Adaptive Acquisition Framework,* established cybersecurity as a requirement for all DoD programs and implemented in all aspects of acquisition
    - 2017 December 31: DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting,* mandated compliance with incident reporting requirements
    - November 30, 2020: DFARS 252.204-7019 and 7020 required cyber assessments to prove compliance

Overview - DFARS 252.204-7012, 7019, and 7020

- DFARSS 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*, gives the Government the authority to conduct the assessments. The DCMA DIBCAC conducts assessments on behalf of the DoD.
- A specifically states that “adequate security” should be provided on all covered information systems
- DFARS 252-204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements,* provides requirements prior to contract award, including a self-score in the Supplier Performance Risk Management System (SPRS) before a High assessment can be completed

NOTE: As of May 2024, the Department of Defense issues a Class Deviation to DFARS 252.204-7012 in which it effectually paused the requirement for contractors to comply with at NIST 800-171r2. This deviation is in effect until rescinded by DoD.

NIST SP 800-171

- NIST SP 800-171 rev. 2 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- “This publication provides agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations;”
- There are 110 security requirements, with 320 objectives covering 14 control families
- NIST SP 800-171 rev. 3 released in May 2024, however DoD issues a Class Deviation (CD) that pauses implementation of that new revision and requires revision 2 until the CD is rescinded.

NIST SP 800-171a

- NIST SP 800-171a – Assessing Security Requirements for Controlled Unclassified Information
- “This publication provides federal and nonfederal organizations with assessment procedures and a methodology that can be employed to conduct assessments of the CUI security requirements in NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.”
- This document gives both federal employees and contractors specific insight to how each control will be addressed and even examples are of what is being looked for per requirement

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].

Assessment Types - NIST SP 800-171

Assessing Contractor Implementation of DFARS clause 252.204-7012

There are 3 levels of DoD assessment methodology, each resulting in a different level of confidence:

Trust

Basic

System Security Plan Review

NIST SP 800-171 Contractor Self-Assessment

Trust & Examine

Medium

Plans of Action Review (If Req'd)

System Security Plan Review

NIST SP 800-171 DoD + Contractor Assessment

Trust & Verify

High (includes virtual/on-site)

On-site Discussions/Interviews

Documentation Review

Plans of Action Review (If Req'd)

System Security Plan Review

NIST SP 800-171 DoD + Contractor Assessment

DIBCAC performs the Medium and High Assessments

Assessment Types – NIST SP 800-171

- NIST SP 800-171 Basic Assessment
  - The contractor will do a “self” or Basic assessment
  - This score will be logged in the Supplier Risk Management System (SPRS)
  - Pre-award requirement
- NIST SP 800-171 Medium Assessment
  - A documentation only review
  - Only utilizes the 800-171
  - No on-site visit, DIBCAC will review the documentation, make a determination on if the provided artifacts have enough information to say that a requirement is implemented
  - Medium score is logged in SPRS
  - Post contract award
- NIST SP 800-171 High Assessment
  - Utilizes the SP 800-171 and the 800-171a
  - All documents will need to provided, such as a System Security Plan (SSP), network diagram, and any other policies or procedures relevant to the system
  - On-site visits required to assess physical security requirements
  - “Over the shoulder” methodology – DIBCAC assessors will want to see in real-time how each security requirement is implemented
  - High confidence score will be put into SPRS
  - Post contract award

Assessment Types - CMMC

- Proposed rule - Cybersecurity Maturity Model Certification (CMMC) Assessments that will be added to Title 32 of the Code of Federal Regulations (not the DFARS)
  - Based off the NIST SP 800-171 rev. 2
  - CMMC Program managed by the DoD CIO
  - The Cyber Accreditation Body (AB) contracts with the government to manage the ecosystem.
  - The assessments are then managed by the CMMC Certified 3rd Party Assessment Organizations (C3PAOs).
  - C3PAO assessors will conduct the L2 assessments
  - Tiered model – L1, L2, & L3 – Dependent on the type and sensitivity of the information
  - Once CMMC is fully implemented, certain contractors will be required to have a specific level of CMMC certification as a condition of being awarded a contract
  - Pre-contract award

After the Assessment

- What happens when the assessments are done?
  - For 171 assessments, the results will be uploaded into SPRS, as mentioned above
  - Depending on the overall score, a Corrective Action Report (CAR) could be submitted, due to contractual non-compliance
  - DIBCAC will work with the assigned Administrative Contracting Officer (ACO) on any follow up actions
  - Contractor has a “reclama period” where they can write their plans of action (POAs), which will then be uploaded as part of their final assessment package
  - If the contractor has a perfect score – woo! – we will then upload the scores and start the final reports process that will make its way back to the contractor

Future of Assessments

- NIST SP 800-172
  - This is an enhanced security requirement guide that will be assessed in addition to the “basics” required in the 171
  - Will be required depending on the type of information that each information system processes and based on DoD guidance to Contracting Officers (CO)
  - Must be amended to the contract as a requirement
- CMMC Rulemaking
  - Proposed rule published November 2023 with final rule expected FY25
  - After publication, CMMC requirements will phased in over a period of time
  - CMMC assessments are a pre-award requirement
- NIST SP 800-171 rev. 3
  - 97 requirements with 507 objectives across 14 families versus 171 rev. 2 with 110 requirements and 320 objectives across 20 families
  - Adds new control families such as Planning, Program Management, PII Processing, and Supply Chain Risk Management
  - Aims to align even more closely with NIST SP 800-53 rev. 5
  - Not being enforced yet, but could be soon

International Partnering

- DIBCAC provides direct support to DoD CIO's engagements with Foreign Partners for DIB cyber standards and assessment alignment efforts
- DIBCAC partners with other organizations (government and industry) to conduct cyber assessments
  - Met with 7 foreign partners to discuss training and joint assessment opportunities
  - Trained ~ 40 foreign partners' cyber assessors
  - Completed the first 6 international NIST SP 800-171 High Assessments
  - Performed joint assessments with officials from 3 foreign partners
  - Conducted 5 assessments with other US government organizations
  - Conducted ~100 assessments with non-government organizations under DCMA's joint surveillance authority
  - Conducted 1 assessment of a NATO program's enterprise system
  - Training events and assessments scheduled for FY24-25 with multiple foreign partners

How does this impact DoD and DCMA?

- Overall, the goal is to support the warfighter lethality by assessing the DIB in the protection of CUI data to ensure that the lethality is not reduced via loss of data
- Once DIBCAC enters the assessment results into SPRS, specifically for the 171 medium or High assessments, the acquisition workforce can see those scores as well as the DFARS compliance status
- DIBCAC also wants to ensure that DoD acquisition decision-makers have the information they need to make educated and data-driven decisions
- Supports DoD organizations with assessment results and technical guidance during ongoing investigations

What does a SPRS Score Mean?

- High
- Low
- The same score could be different requirements...

References

- NIST SP 800-171 rev. 2
- NIST SP 800-171 rev. 3
- NIST SP 800-171a rev. 2
- NIST SP 800-171a rev. 3
- DoD CIO DFARS Clause Memo
- DFARS Clause
- CMMC Information
- DIBCAC Public Site
- SPRS

Questions and Answers Session