ncmbc
CONNECTING BUSINESS AND MILITARY

NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP #6

www.cybernc.us

17 February 2021

CyberChat Series Description

- Objective: To help defense contractors develop a cybersecurity quality management system [QMS] program that is compliant with [DFARS 252.204-7021] – the new CMMC regulation – and protects national security.
- Technical advice regarding cybersecurity tools and providers will not be given by the NCMBC. The focus will be on developing a compliance roadmap using tools and information provided on www.cybernc.us.
- CyberChats are not to be used to sell products or services. IT/Cyber companies can sign up as a resource for defense/federal contractors. Note: the NCMBC does not vet these companies. https://www.ncmbc.us/matrices-resources/

Agenda – CyberChat Workshop #5

- Mobilize IO CyberChat Community – Bob Burton
- Latest CMMC/cybersecurity updates
- CyberChat calendar
- Questions from previous workshops
- Scope review
- Gap assessment
- Homework

Mobilize CyberChat Community

WHY: To help companies in the North Carolina defense industrial base achieve compliance to cybersecurity regulations. Our goal is to “stack the deck” with companies that are compliant, so the DoD awards more contracts to North Carolina companies. The NCMBC will use the platform as an additional tool to keep you updated on cybersecurity events, activities, training, and resources.

WHAT: Mobilize is a private information sharing platform that allows members to collaborate, share knowledge; create teaming opportunities, and inform best practices. It’s easy to use and will take about 10 minutes to sign-up. There is more information inside the CyberChat Mobilize Community to help you navigate the community space.

Mobilize CyberChat Community

HOW: Use this link to sign up: https://nc-defense-technology-transition-office.mobilize.io/registrations/groups/45745

1. First, you may create a welcome post in the CyberChat Community. You may upload a picture and share some information about yourself and your company to connect with others. This is a PRIVATE community.

2. Create posts – articles, ask questions, answer questions, etc.

CMMC/Cyber Updates

- Delays in getting C3PAOs certified due in part to slow pace in getting POAMs closed
- Companies outside of the initial 15 pilot program supply chains may have the opportunity to get certified to CMMC by early summer
- Prime contractors take heed – per Katie Arrington, the DoD is not going to pay for unnecessary CMMC certifications.
- CMMC audit costs – for Levels 3 and below the costs should be rolled into your OH rates. For Levels 4 and 5, can be billed directly to the DoD.
- Reciprocity issue with FedRAMP is POAMs. FedRAMP allows POAMs, but CMMC does not.

CMMC/Cyber Updates

- DoD is asking companies not to advertise their certification level – can show adversaries your weaknesses.
- The Certified Professional (CP) role will most likely replace the Registered Practitioner (RP) role – per Ben Tchoubineh (CMMC-AB)
- DoD is suggesting that companies think ahead 5 years when determining compliance level requirements
- DoD suggested that "COTS-only" companies achieve CMMC Level 1 compliance
- **Cyberattacks and Cybersecurity Failure Top Risks of the Next Decade Says World Economic Forum**

CyberChats Calendar

Feb. 24th	How to use CMMC Level 1 in a Box tools; Assessment Control, Asset Management Domains
Mar. 3rd	Audit & Accountability, Awareness & Training, Configuration Management
Mar. 10th	Identification & Authentication, Incident Response, Maintenance
Mar. 17th	Media Protection, Personnel Security, Physical Protection
Mar. 24th	Recovery, Risk Management, Security Assessment
Mar. 31st	Situational Awareness, System & Communications Protection, System & Information Integrity

Scope

- Understanding audit scope is critical to minimizing costs and reducing the risk of data getting into the wrong hands
- Companies that don’t reduce their scope run the risk of having their entire network and all their employees considered in scope to the audit.
- Large scope = high risk = high costs
- How to determine scope:
    - Use your data-flow diagram to understand how CUI/FCI flows through and/or is stored on your network.
    - Use your network diagram and asset inventory to determine which IT assets are impacted by the flow of data
    - List the employees that have access to the CUI/FCI

Reducing Scope

- Understand your cybersecurity risks
- Identify the employees that must touch FCI/CUI in order to do their jobs
- Identify the IT assets that are necessary for the flow of FCI/CUI
- Segment the network so that only a portion of it is in scope
  - Examples of mechanisms that can be used for network segmentation – firewalls and routers

Remember – this is not just about passing an audit. The audit is a means to an end, with the end being protecting national security.

Scoping Tool

- The best scoping guide to use is the Compliance Forge NIST 800-171 & CMMC Scoping Guide for FCI/CUI
    - https://www.complianceforge.com/free-guides/free-nist-800-171-cybersecurity-compliance-scoping-guide.html - download the guide. I will post it on my blog and on Mobilize IO

Gap Assessment - CUI

- ***For defense contractors that touch CUI***; DFARS 252.204-7019 will apply sometime during the next 3 years (part of DFARS Interim Rule)
  - Must perform a gap assessment to the 110 controls in NIST 800-171 using DoD Assessment Methodology (DoD AM)
  - Your score, along with date a score of 110 will be achieved must be uploaded into the Supplier Performance Risk System (SPRS)
  - Scores are not made public – only contracting officers and other DoD personnel see the scores
  - Assessment valid for 3 years

Gap Assessment – DoD AM

DoD Assessment Methodology

- Provides a standard methodology for contractors to do a self-assessment (Basic Assessment) to the 110 controls in NIST SP 800-171 – assigns a numerical value to each control
- *“**The requirement for the Basic Assessment would be imposed through incorporation of the new solicitation provision and the contract clause in new contracts and orders. As such, the requirement to have completed a Basic Assessment is expected to phase-in over a three-year period…” Reference – DFARS Interim Rule***

Gap Assessment – DoD AM

Assessments

Basic Assessment

- Self-assessment to 110 NIST controls
- Pre-award assessment
- Uploaded to SPRS prior to award
- Valid for 3 years
- Confidence level - low

Medium Assessment

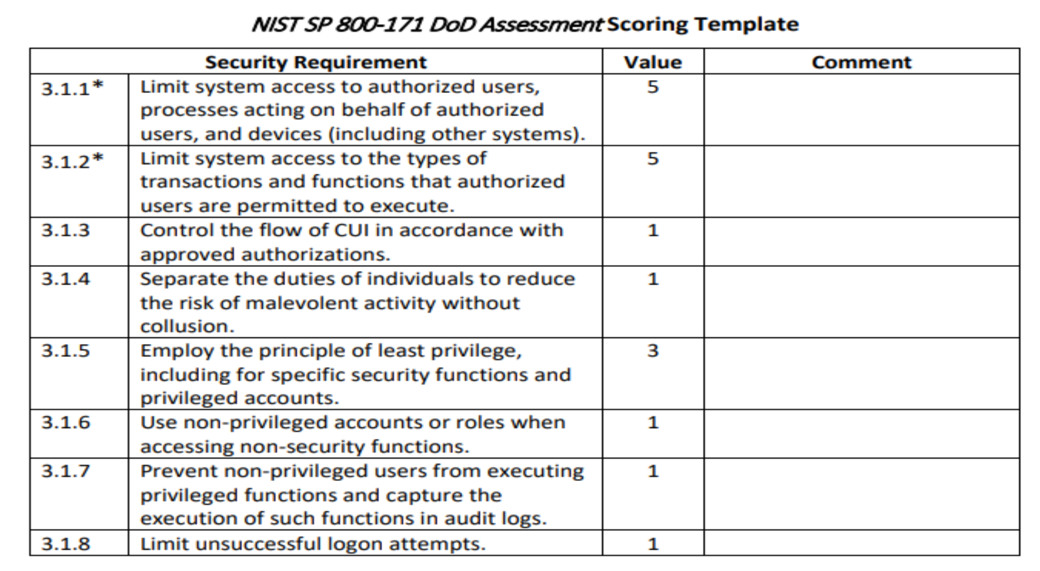
- Performed by DCMA
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- Confidence level – medium
- DoD uploads results to SPRS

High Assessment

- Performed by DCMA
- Based on criticality of program and sensitivity of data
- Post-award assessment
- Valid for 3 years
- Confidence level – high
- DoD uploads results to SPRS

Gap Assessment – DoD AM Scoring

- How to Score the Self-Assessment – a perfect score is 110, meaning the contractor has all 110 NIST controls in place.
- For every control that is not in place, subtract its value from 110 – see below



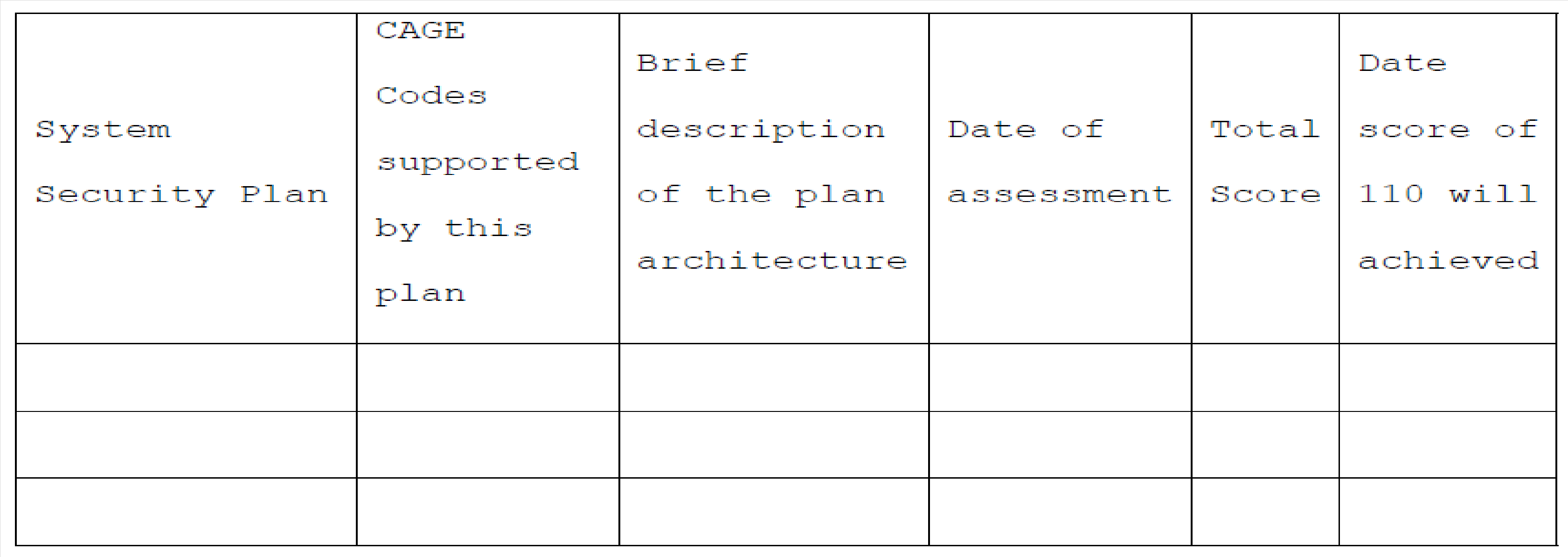
***NIST SP 800-171 DoD Assessment* Scoring Template**

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	

Example: If my company is not compliant with controls 3.1.1 and 3.1.5, subtract 8 points from 110.

DFARS Interim Rule –
DoD Assessment Methodology - Results

- The information below must be posted to SPRS - https://www.sprs.csd.disa.mil/



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

Gap Analysis - System Security Plan

- Purpose of the system security plan (SSP) is to provide an overview of the security requirements of the system and describe the controls in place or planned, responsibilities of all individuals who access the system
- List of controls in NIST SP 800-171 and status: implemented, plan to be implemented, or not applicable.
- Controls that are deemed not applicable need to be approved by your contracting officer
- Can use NIST template on cyberNC.us OR the CMMC Level 1 Guide
- My suggestion: do the gap analysis first

Gap Assessment - POAMs

- If any of the 110 controls are not in place, a Plan of Action and Milestones (POAM) must be developed to show how you plan to implement the control and when the control will be in place. Template available on cyberNC.us, OR use the CMMC Level 1 Guide
- The date that a score of 110 will be achieved (uploaded to SPRS) should be the latest date on your POAMS.
- There has been no guidance on how long POAMS can be open.
- Companies should upload a new score each time a POAM is closed, and the score improved.
- Compliance does **NOT** mean you must have a score of 110. Compliance means that you have performed a self-assessment, have POAMs in place, and have uploaded your score to SPRS.

Gap Assessment

Tools

- **Project Spectrum** – https://www.projectspectrum.io/#!/
  - ✓ Gap assessment for NIST 800-171/CMMC Levels 1 - 3
  - ✓ Not mapped to standard designation
  - ✓ No mapping between NIST and CMMC
- **CSET - https://github.com/cisagov/cset**
  - ✓ Gap analysis tool for NIST/CMMC as well as industry standards such as: chemical/oil/natural gas, electrical, financial, health care, nuclear, transportation, etc.
  - ✓ Mapped to standard designation
  - ✓ No mapping between NIST and CMMC

Gap Assessment

Tools Continued

- CMMC Center of Awesomeness - https://www.cmmc-coa.com/cmmc-awesomeness
  - ✓ Gap analysis for NIST and CMMC
  - ✓ Maps to standard designations
  - ✓ Maps NIST to CMMC

Homework – CyberChat #6

1. Begin working on your gap analysis

Remember to document your work!

ncmbc
CONNECTING BUSINESS AND MILITARY

NORTH CAROLINA MILITARY BUSINESS CENTER CYBERCHAT SERIES – WORKSHOP #6

www.cybernc.us

17 February 2021