CMMC Update:
Mastering the Basics

Current As Of: October 2023

TODAY'S SPEAKERS

Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Scott Whitehouse

Director of Compliance Services

C3Integrated Solutions

Sponsored by:

C3 INTEGRATED SOLUTIONS

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **DRAFT NIST 800-171Rev3 released 10 May 23**
- **CMMC rule with OMB**

Timeline Summary

- **2 Processes moving the goal posts running simultaneously**
- **NIST 800-171 Rev3 Final – Anticipated Dec 23 – Jan 24 with Guidebook for Assessments**
- **CMMC: Interim Final Rule (IFR) vs Notice of Proposed Rulemaking (NoPRM)**
  - IFR: As early as Jan 24 3rd party assessment requirements may appear in contracts
  - NoPRM: Likely Q1 CY25 before assessment requirements hit

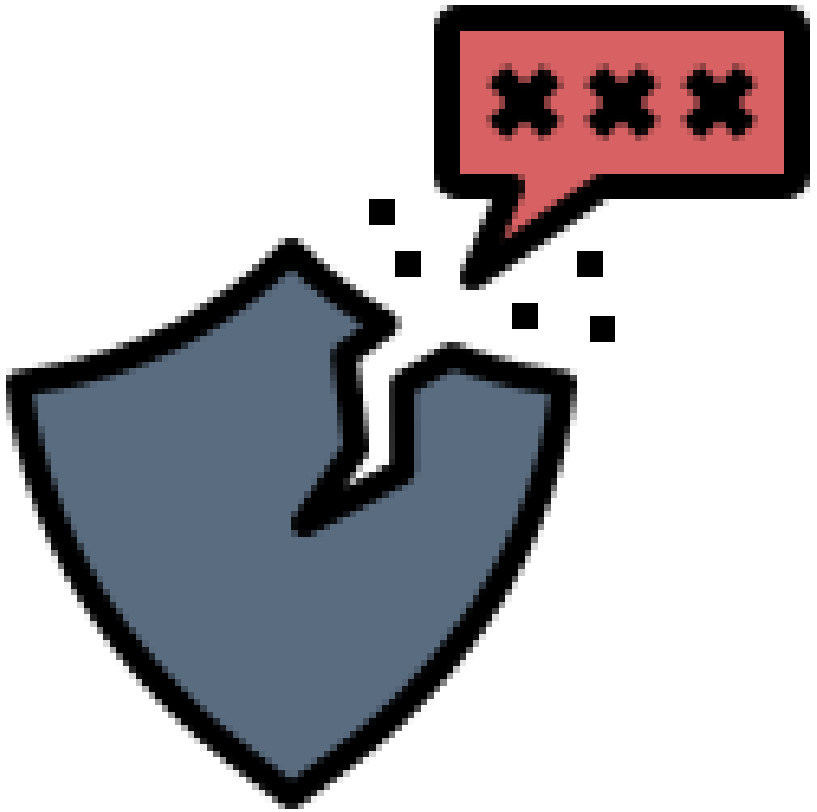
Start with Processes and Information

- **Define & Develop executable processes**
  - Build in regular reviews for updates
- **Where does your organization receive/process/store CUI?**
  - **Review your contracts & understand your obligations**
    - Is your company Prime?
      - What do you owe your subs?
    - Is your company a sub?
      - What should your prime provide?
    - Business Ops, Compliance personnel and IT / Cybersecurity personnel must collaborate
    - IT / Cybersecurity personnel generally lack awareness of “What” systems must receive/process/store

Processes and Information

- **Follow data throughout contract lifecycle**
- **Tracking data identifies where you must implement technical controls**
- **Where does information enter your organization's systems?**
- **What do you do with it on your systems?**
- **Does it transit certain systems and go to other systems?**
  - Technical specifications from a "main" system to a machine shop floor?
  - Information from a prime to a sub or from a sub to a prime?
- **Map the information and processes to understand cybersecurity requirements**

Basics of Vulnerability Management



All software has vulnerabilities.

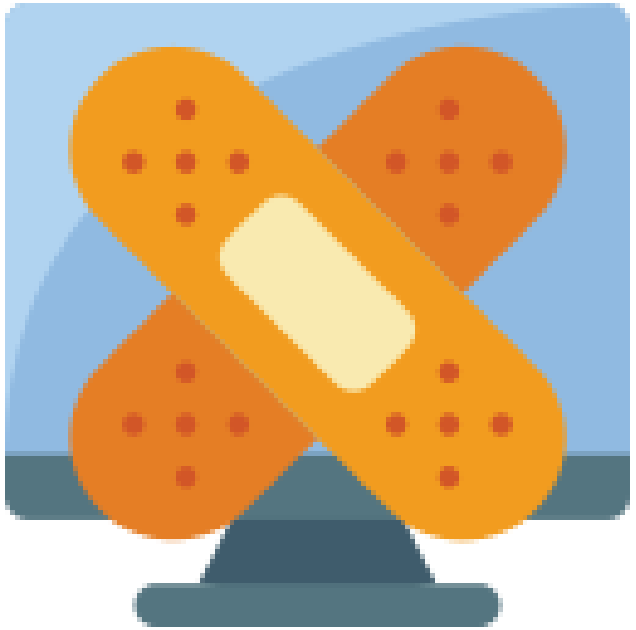
All hardware has vulnerabilities.

All firmware has vulnerabilities.

All devices have vulnerabilities.

Which vulnerabilities are in YOUR systems?

Basics of Patch Management



Patching cannot be a human API

Should be considered when building the software catalog

Not just Operating System and applications

Set it and forget it is insufficient

Not sure where to start? See NIST 800-40 r4

Basics of Asset Management – Part 1

Classic assets

- Computers – Active and Inactive
- Servers
- Software
- Network equipment
- Printers / MFD’s

Don’t forget

- IOT devices
- Removable Storage
- OT

Scoping Basics

- **“Out of Scope Assets”**

- **Cannot store, process, or transmit CUI**
  - Because of effective boundaries
  - Technical: firewalls, Data Loss Prevention, walls/locks
  - Administrative: “don’t email CUI to your personal email”

- **No security required**

Scoping Basics

- **“CUI Assets”**
- **Stores, processes, or transmits CUI**
- **Expected to be protected by all 800-171 requirements**

Laptops
File Servers
Switches
Printers
Paper docs

Scoping Basics

- **“Specialized Assets (SA)”**
- **Meets one of 5 specialized asset definitions**
  1. Government Property
  2. Internet of Things / Industrial Internet of Things
  3. Operational Technology
  4. Restricted Information Systems
  5. Test Equipment
- **Security risks expected to be addressed as much as possible, but SA not directly assessed**

GFE for a contract
Prototypes
Simulators
Dev systems
Machinery
Cameras

Scoping Basics

- **“Contractor Risk Managed Assets (CRMA)”**
- **Can, but is not intended to, process / store / transmit CUI**
- **Security risks expected to be addressed as much as possible, but CRMA are not directly assessed**

Laptops that aren’t used to handle CUI

Servers that don’t provide security or hold CUI

Endpoints used to access VDI Enclave

Scoping Basics

- **“Security Protection Assets”**
- **Provides security function to any in-scope asset**
- **Future? All security requirements apply / assessed**
- **Future? CMMC Level 2 Cert for any external SPA**
- **Future? “Security Protection Data” to be protected with same security as CUI - network diagrams, SSP, endpoint configurations, logs**

Firewalls
Patch servers
Antivirus servers
IT Databases
Log Server

External Service Providers

- **Prepare for worst-case rulemaking**
  - Public release is only a few weeks away, don't make costly changes until you see the exact text
- **Cloud provider where you store CUI or security data:**
  - Requires FedRAMP (performing all controls in 800-53 moderate baseline)
- **Non-Cloud provider where you store CUI or security data:**
  - Requires CMMC Level 2 certification (110 requirements in 800-171)
- **Provider who performs security function(s) for you**
  - Evaluated as a Security Protection Asset (all 110 requirements in 800-171) assessed. What about security for the security?
  - Also need to show that they do the security function

Google Drive
AWS
Microsoft 365
Dropbox

MSP / MSSP

Facilities security

Challenges and Mistakes

- **Unfamiliarity with scoping concepts – read the CMMC Scoping Guide for Level 2!**

- **Not realizing that editing or manipulating documents on endpoints (laptops, workstations etc.) means they need to be very secure**

Indicators of success

- **Onboard or get training from a CMMC specialist**
  - CMMC Certified Assessor/Professional
  - IT Services with clients that have PASSED an assessment before
  - Use that knowledgeable person to perform a high-quality assessment
  - You'll find out you are doing worse than you thought
  - **But** you will be prepared for the real assessment

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **DRAFT NIST 800-171Rev3 released 10 May 23**
- **CMMC rule with OMB**
- **DRAFTS of updated CMMC model & Assessment Guides posted last week**
- **Communicate with your MSPs/MSSPs/ESPs**
  - Be ready for implementation of the final rule

Questions?

Sponsored by:

C3 INTEGRATED SOLUTIONS