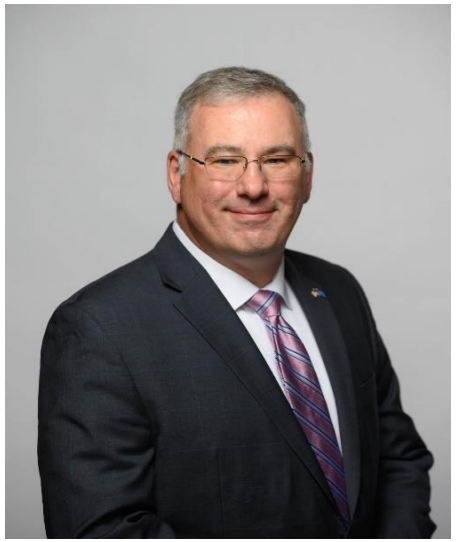
CMMC Update:
Implementation Timeline and Impact

Current As Of: August 2023

TODAY'S SPEAKERS

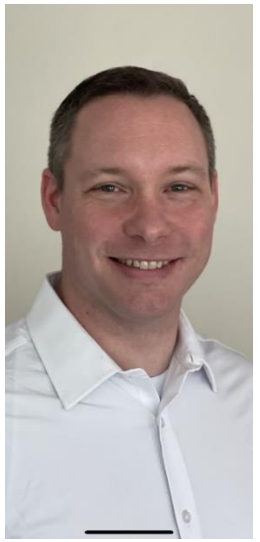


Vince Scott

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**
- **DRAFTS of updated CMMC model & Assessment Guides posted last week**

Sponsored by:

C3 INTEGRATED SOLUTIONS

But First, Timeline for Implementation…

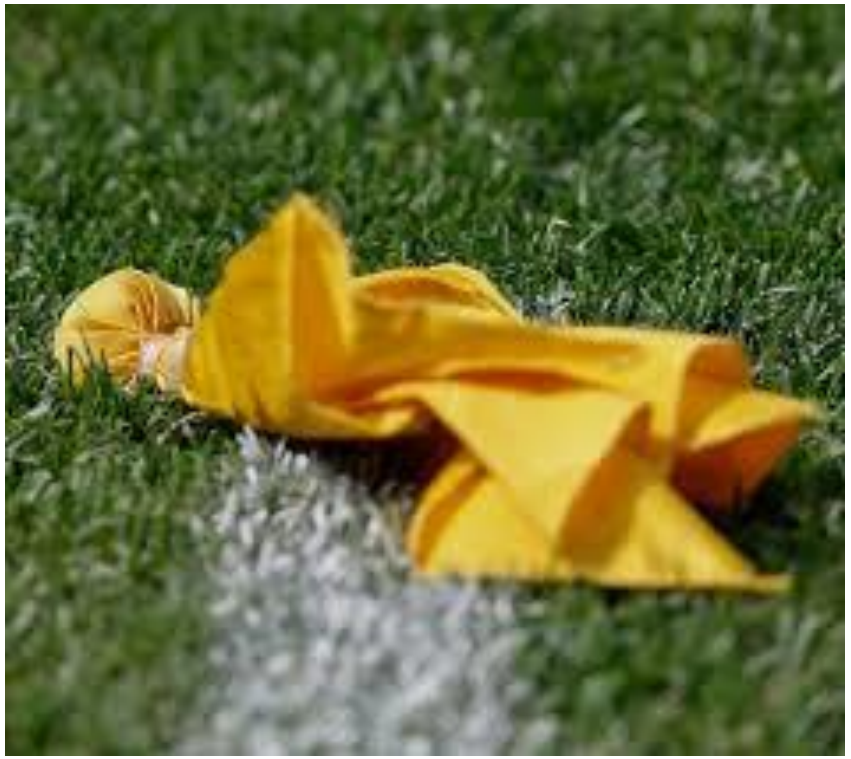
- **Jacob Horne**
  - **Sum IT Up: Major CMMC Rulemaking Updates: https://www.youtube.com/watch?v=z_4dW8U3QYQ**
  - **CMMC AB podcast: https://cyberab.org/News-Events/Town-Halls/Details/july-2023-town-hall**
  - **~3:45 Jacob begins his overview**
  - **Outlines the process**
  - **Researched previous OMB Regulatory Review**
  - **Analyzed and Estimated: Final Rule Publication Q1 CY25 / Q2 FY25**
  - **Added to contracts via "Phased roll-out"**
  - **Politically: After Inauguration**

Updated CMMC Model & Assessment Guides

- Posted on Office of Management and Budget (OMB) Office of Information and Regulatory Affairs (OIRA) website
- DRAFTS marked for Distribution A, Public Release
- Highlighted by user in Sweden
- Removed within hours

False Start

- Assessment guides levels 1-3
- Scoping documents levels 1-3
- Hashing guideline



False start – What we learned

DOD RELIES HEAVILY ON SMALL BUSINESS

THERE IS A [SMALL] CHANCE OF A LEVEL 2 SELF-ASSESSMENT

LEVEL 3 ASSESSMENTS ARE PERFORMED BY DIBCAC

NIST 800-171 REV 2 IS EXPLICITLY REFERENCED

Sponsored by:

C3 INTEGRATED SOLUTIONS

Level 2 Scoping Guide – External Service Providers (ESPs)

External Service Provider Considerations

An External Service Provider (ESP) can be within the scope CMMC requirements if it meets CUI Asset and/or Security Protection Asset criteria. **To be considered an ESP, data (specifically CUI or Security Protection Data, e.g., log data, configuration data) must reside on the ESP assets** as set forth in 32 CFR § 170.19(d). Special considerations in 32 CFR § 170.19(c)(2) for an OSA/OSC using an ESP include the following:

- Defines (yes/no questions) organizations that qualify as ESP
- Good hygiene practices can limit “ESP scope”
- Only systems that process, handle or store CI or Security Protection data / affect confidentiality of CUI

Level 2 Scoping Guide - ESPs

- If the OSA utilizes an ESP other than a CSP, the ESP must have a CMMC Level 2 Certification as set forth in 32 CFR § 170.19(b)(2).

- **Introduces requirement for CMMC Level 2 certification of EXTERNAL SERVICE PROVIDERS**
- **Solves assessment issue where multiple independent information systems are reviewed during OSA's assessment**
- **Assessors simply check certification status of ESPs**

Level 2 Scoping Guide – Security Protection Assets (SPAs)

> Security Protection Assets provide security functions or capabilities within the OSA's CMMC Assessment Scope
>
> Security Protection Assets are part of the CMMC Assessment Scope and are assessed against all CMMC requirements. For example, an External Service Provider (ESP, defined in 32 CFR

- Clarifies DoD expects full security for Security Protection Assets (SPAs)
- **Conflicts with existing precedent / has not been tested during past DIBCAC assessments of 800-171 compliance**
- Expands burden of proof 3x or more compared to prior 800-171 assessments (which verified security was performed for CUI)
- In many cases, the security of security systems irrelevant to CUI protection
  - For example, CUI cannot be directly compromised if an NTP or MFA server is insecure – only performance of one security requirement is affected
  - Requirements designed to be redundant
- DoD should amend / clarify
  - CMMC requirements only assessed against SPAs when compromise of CUI could occur if SPA compromised

Updated CMMC Model & Assessment Guides Initial Assessments

- **All Assets that process, handle, store CUI OR provide security for those assets must:**
  - Be in-house and on-premises
  - Or use a FEDRAMP-certified Cloud Service Provider (CSP)
    - Could be “equivalent” but currently there is no equivalent
  - Includes SIEMs, Badge Logs, any security related data, ticketing systems, spam filters etc.
  - If leveraging an External Service Provider (ESP) it must be CMMC certified at the level of the company/client requires
    - This includes all Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs)

Updated CMMC Model & Assessment Guides Some Impacts

- **No company pursuing early certification can use outside help (MSP/MSSP)**
  - Because no MSPs/MSSPs are certified by a 3rd party assessor
  - Will there be sufficient assessors to assess all MSPs/MSSPs needed to support DIB companies?
  - Will sufficient MSPs, MSSPs offer capabilities including SOCs and Penetration Testing teams? Will they accept the costs of pursuing CMMC certification?
- **Two big impacts**
  - Under the proposed guidelines, no company using an MSP/MSSP can become certified until **their** MSP/MSSP is certified
  - **Cost**: Certification requirement likely drives large increases for consuming those services & large numbers of small cost efficient MSPs may struggle to afford certification

Updated CMMC Model & Assessment Guides Some Impacts

- **Cost—Companies might have to "rip and replace"**
- **Examples: One Small Business (400 people) exclusively serving Federal customers**
  - Okta: Provides security for passwords & single sign on -- Keep?
  - Carbon Black: Shift to FedRAMP? Drop?
  - Firewall Cloud Console: Security and FW synchronization -- Eliminate?
  - CloudFlare: DNS protection -- Shift to NSA offering? Is it certified?
  - Badge System: Cloud based and many badge systems controlled by building landlord
  - DUO - Move to FedRAMP?
  - Ticketing System – Cloud based, used to meet controls
    - Move to FedRAMP? Bring on prem? Use hard copy log for CMMC?
  - Email protection/Spam filtering: In Cloud -- Eliminate?
- **In the end this will reduce rather than enhance security**

Lots of churn; Focus on the basics!

1. **Have a Program with executable processes**
   - Good Programs will endure
   - Cybersecurity is not one and done
2. **This is *not* easy, moderate, just the basics etc.**
   - 1-year implementation timeline possible but 2-year timeline better
   - Assessments in spring of ‘25… ***start now!***
3. **Best place to begin: “where do I receive/process/store CUI?”**
   - Review your contracts
   - Follow data throughout contract lifecycle
   - Tracking data identifies where you must implement technical controls
   - **NOT** IT challenge; data makes this an operational challenge
   - Companies who expect IT to “fix this” **will fail** certification / assessment

Lots of churn; Focus on the basics!

4. **Follow Assessment Objectives**
   - No single point causes more problems during mock assessment
   - Objectives located in Assessment Guides & NIST SP 800-171**A**
     - **A =** Assessment Guide version
   - **Objectives ADD requirements**
     - **Failure to track will lead to assessment failure**
5. **Role of Prime Contractors**
   - Tremendous shift in Prime supply chain approach
   - Examine your T's & C's
     - Many "changing" "under the radar"
   - Large Primes: please consider helping your subs
   - **Help Educate** as you flow cybersecurity obligations down to your critical suppliers

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