# CMMC Update:
# Timelines & NIST 800-171 Rev3

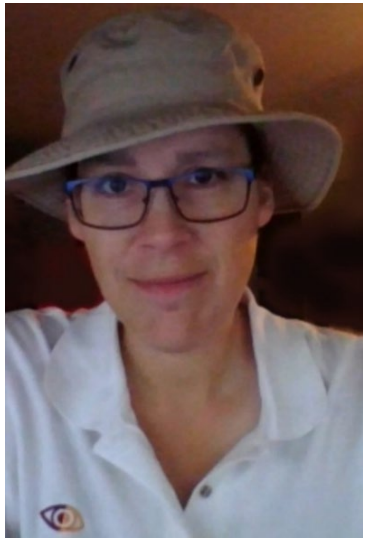
## Current As Of: September 2023



Sponsored by:

C3 INTEGRATED SOLUTIONS

# 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:**

# 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**

Sponsored by:

C3 INTEGRATED SOLUTIONS

# Timelines

- **2 Processes moving the goal posts running simultaneously**
  - NIST Revision and CMMC rulemaking = complicated
- **NIST 800-171 Rev3**
  - **Draft 1 – Delivered; NIST Adjudicating comments**
  - **Final – Anticipated Dec 23 – Jan 24**
- **171A – Guidebook for Assessments**
  - **Draft due in October**
  - **NIST will publish with Final 171Rev3**

# Timelines

- CMMC: Interim Final Rule (IFR) vs Notice of Proposed Rulemaking (NoPRM)
  - IFR: rule goes into effect 60 days after publication & can begin to appear in contracts
  - NoPRM: After comment period DoD must:
    - Adjudicate comments
    - Adjust rule if they deem appropriate
    - Publish final rule & include reasoning and approach to comments
  - Impact on implementation
    - IFR: Then as early as Jan 24, 3rd party assessments requirements may appear in contracts
    - NoPRM: Then likely Q1 CY25 before assessment requirements hit
    - Overall, 5-7 year phased implementation planned
    - Previous full implementation date 1 Oct 25 (beginning of FY26) – as outlined in DFARS 204.7503, likely to adjust for phased roll out

# Will CMMC use Rev2 or Rev3?

- **The case for Rev2**
  1) IF OMB publishes an Interim Final Rule late in CY23, it will be based on Rev2
  2) Assessment Guides do not automatically change with NIST update
  3) Give Contractors time to adjust…and matches what is in their contracts?
- **The case for Rev3**
  1) CMMC certification only required for new (or rebid) contracts
  2) Rev3 in solicitations and contracts
  3) Allows contractors to price bid to include compliance costs
  4) DFARS 252.204-7012 automatically increments to Rev3 for new / rebid contracts

# Other Important Questions

- When will DIB Cybersecurity Assessment Center (DIBCAC) update the DoD Assessment Manual (DoDAM)?
- When will DoD expect SPRS scores to reflect updated DoDAM?
- Will DoD grant a variance or waiver to phase in Rev3 on a reasonable timeline based on rulemaking timeline?
- Will contractors be able to choose which version is assessed by a C3PAO?

# Rev3 Significant comments (ODPs)

"The use of [Organizationally Defined Parameters] ODPs… ultimately renders the 171r3 neither a standard nor scalable… The ODP construct means that a contractor with 1,000 contracts may have 1,000 different implementations they are required to meet simultaneously, many on the same enterprise network… Recommend replacing all ODPs with a standard wording." – DoD CIO

"Eliminate ODPs and provide specific baseline variables in the security requirements." – Carnegie Mellon

# Rev3 Significant comments (Scope)

“”The security requirements in this publication are only applicable to **components** of nonfederal systems that process, store, or transmit CUI or that provide protection for such components” has been (in 800-171r2) purposefully misinterpreted to mean that the requirements only apply to components that actually process store or transmit CUI and the other components (e.g. servers, workstations) that do not process CUI do not meet the requirements.”

“Rephrase applicability statement to read “The security requirements in this publication are only applicable to **nonfederal systems** that process, store, or transmit CUI and the components within that are capable of processing, storing or transmitting CUI or that provide protection for such components…”

- DoD CIO

# Rev3 Significant comments (Cryptography)

"Assign ODP as "**FIPS-validated** or **NSA-approved**"…" - DoD CIO

"Adjust definition to verified by [Cryptographic Module Validation Program] CNVP (sic) to meet requirements of FIPS 140-2 or **FIPS 140-3"  - Carnegie Mellon**

# Rev3 Significant comments (Self-Assessment)

"This requirement needs to be removed… We believe this excludes anyone internal to the [Non-Federal Organization, aka contractor] NFO from being the "independent" assessor because they always have some level of COI… Minimally you have doubled the cost of a CMMC Level 2 assessment…" - DoD CIO

# Rev3 Significant comments (Plan of Action)

"Rewrite to allow for an org not to have a POAM…
… set POAM limit of 180 days" - DoD CIO

# Rev3 Significant comments (Marking CUI)

"… the company cannot be held accountable for CUI not marked by the govt." - DoD CIO

# Rev3 Summary of key comments

- **Only large government agency providing comments = DoD**
  - Other agencies not paying attention
- **Everyone hates Organizationally Defined Parameters**
- **DoD wants NIST standards to apply to larger scope (information-system wide, rather than individual components)**
  - All security for security
- **FIPS not going away**

# 3.8.9 – Protecting backups

REMEMBER 800-171 IS LIMITED TO CONFIDENTIALITY (BACKUP YOUR SYSTEMS ANYWAYS)

THE SOURCE CONTROL IS 800-57 CP-9(8)

CRYPTOGRAPHIC PROTECTION IS REQUIRED ON BACKUPS

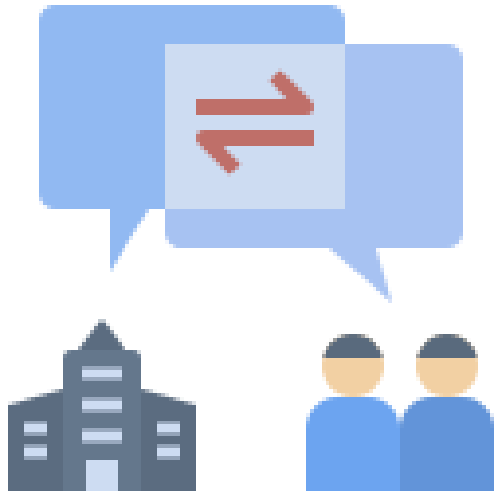
# 3.4.12 – High Risk Areas

**Prerequisites – Define information locations and what defines low or high risk**

**Do we have a travel policy, and what is the frequency of review?**

**The source control is 800-53 CM-2(7), but review MP-5 assessment procedure for guidance**

# Information Exchange – 3.12.6



ASSUMPTION IS EXTERNAL INFORMATION EXCHANGE – B2B, B2G, ESP

MAJOR FOCUS FOR CHINA

CONTRACTS VS TECHNICAL IMPLEMENTATION

Sponsored by:

C3 INTEGRATED SOLUTIONS

# 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 just an IT challenge**; data makes this a **Business 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 assessments
   - 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