CMMC Update

Current As Of: 14 November 2022

TODAY'S SPEAKERS

Col (Ret) Rachel McCaffrey, USAF

Senior Vice President of Membership & Chapters, NDIA

Executive Director, Women In Defense

Vince Scott

CEO

Defense Cybersecurity Group

INFRAGARD National SME Cyberwarfare

Alex Major

Attorney, McCarter and English

https://www.mccarter.com/

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your contracts/Know your data**
  - FAR 52.204-21; DFARS 252.204-7012/-7019/-7020
- **NIST SP 800-171 Released Jun ‘15 / Updated Aug ‘16: 110 controls**
  - Revision 3 draft planned for release in Spring of ’23
  - Expect 110 number to increase
  - NIST SP 800-172, Enhanced Security Requirements for Protecting CUI
- **CMMC announced Jul ’19 to independently assess implementation of controls outlined in NIST**
  - CMMC 2.0 announced Nov ’21
  - Interim rule expected March 2023
  - 60 days after Interim Rule published, CMMC requirements could appear in DoD solicitations/contracts

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Be working on these controls now!**
  - Reported/reportable under SPRS
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- **Prioritize!**
  - Some controls provide larger impact
  - 100% implementation extremely difficult

Three Big Questions

- **What are we trying to protect? And why?**
  - We cannot protect information/data if we don't understand why something should be "Controlled"
  - We cannot protect CUI if it is not properly marked
- **From whom are we trying to protect it?**
  - Assume all US persons have access?
  - Is "Need to Know" a component of access?
  - What about friends, partners and Allies?
- **Can NDIA encourage the government to begin by:**
  - Focusing on most critical data/information
  - Providing some guidelines on releasability

Costs – Getting Compliant / Staying Compliant

- **For small businesses, <200 employees**
- **Likely a 6-figure expense annually**
  - Cost for 5-person company roughly = to 25-person company
- **Starting from 0, technical implementation:**
  - $80 - $150K if outsourcing
  - Higher if in-sourcing
- **Sustainment Budget: ~$3500 - $4000 / user / per year**
  - 5-person to 25-person company: $87,500 - $100,000
  - IT spend related to compliance, not all IT spend
- **Economies of scale: ~100+ employees**

Costs – Getting Compliant / Staying Compliant

- **Non-technical implementation:**
  - 1 year to prepare a reasonable estimate
  - ROM: ½ internal FTE = $30 - $52K ***minimum***
  - Developing/Organizing 250-300 pages of documentation
- **Sustainment likely similar in order to maintain the programs that are required under the regulation**
  - Configuration Management, Vulnerability Management, Documentation updates, evidence gathering, annual Basic Self Assessment
- **“Getting Compliant” is not an end state**
  - This is NOT one and done. Requires ongoing security operations in order to stay compliant

Costs – Getting Compliant / Staying Compliant

- Government Estimate (800-172):

Estimated costs for 25-50 end-point systems:

- Process and IT configuration changes: $15K
- Network Isolation:
  - $10K to isolate existing network or existing network segment
  - $250K-500K to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $75K (if not already met).

Estimated costs for 50-100 end point systems:

- Process and IT configuration changes: $50K
- Network Isolation:
  - $100K to isolate existing network or existing network segment
  - $500K-2.5M to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $75K-150K (if not already met).

Estimated costs for 750-1500 end point systems:

- Process and IT configuration changes: $100K
- Network Isolation:
  - $250K to isolate existing network or existing network segment
  - $20M to create new isolated network (depending on network complexity)
- Security Operations Center/Threat related costs: $150K-1M (if not already met). Large companies are assumed to have generally implemented the SOC-related costs.

Costs – 3rd Party Assessment Costs

- **Limited data, and dependent on final CMMC rule and CAP**
- **Paying for assessment team's time**
  - Costs will vary based on company size and preparation
  - Best Practices: Document scope; gather/organize objective evidence
- **Well-prepared companies with great documentation may have shorter assessments and potentially lower costs**
  - Much depends on assessor pricing, which could be Firm Fixed Price
- **$30K likely low end**
  - Could increase by $20K+ if not well-prepared
  - Triennial cost
- **Cost of failure outweighs preparation costs for any company with significant DoD revenue**
  - Companies with low DoD revenue may "opt out"

CUI – Continuing the Discussion

- **Company A operates in CUI Basic**
  - Critical Infrastructure category: environmental engineering, remediation
  - Pricing options between GCC and GCC High
    - GCC High double the cost
    - Export control & Reporting obligations
  - Unknown what upcoming FAR CUI clause / FAR part 40 will include
    - Potential for overmarking
  - What is likelihood Company A will have CUI Specified info?
    - Can they request KO for a "downgrade" to CUI Basic?
    - Can they remain Prime without being GCC High?

CUI – Continuing the Discussion

- **DoD implementing directive on CUI 5200.48 states:**
  - 3.4(g). During DoD's initial phased implementation of CUI Program, no required distinction that must be made between Basic and Specified CUI
  - Contractors will protect all DoD information IAW requirements under Basic level of safeguards and dissemination
  - Unless specifically identified otherwise in a law, regulation, or government-wide policy
  - Forthcoming guidance will address distinction between two levels of CUI:
    - Including list of which categories are Basic or Specified
    - What makes the category one or the other
    - Unique requirements, to include markings, for each

Contractor Responsibility to Mark CUI
Arguing Both Sides

- **Companies should not unilaterally mark information CUI when it is not Federal contract information (FCI)**
  - If company proprietary, mark: “Acme Proprietary Info”
  - If you mark it CUI, you indicate you believe the info to **BE** FCI
  - Could potentially give government claim to your proprietary info

Contractor Responsibility to Mark CUI Arguing Both Sides

- **Companies do not have a responsibility to identify and mark information CUI**
  - Identification and marking inherently governmental function
  - Lack of clear definition and marking guidelines make this responsibility fraught with peril
    - Contractors likely to drift toward “mark everything when unsure”
- **Note: Government asked for contractor assistance**
  - Government personnel busy
  - Without partnership, collaboration, incentives for Government to “mark everything” increase

Contractor Responsibility to Mark CUI Arguing Both Sides

- **Companies do have a responsibility to identify and mark information CUI**
  - 3 Criteria
  1. Data in NARA Categories including / especially:
     - Controlled Technical Information (CUI//SP-CTI)
     - DoD Critical Infrastructure Security Information (CUI//DCRIT)
     - Naval Nuclear Propulsion Information (CUI//SP-NNPI) or (CUI//NNPI)
     - Unclassified Controlled Nuclear Information – Defense (CUI//SP-DCNI) or (CUI//DCNI)
  2. Owned by the government
  3. Created by the contractor for the Government
- **Cannot make CUI easy; FCI is anything created as part of a Federal Contract**

CMMC Challenges – Cloud Implementations

- **Technically Cloud "addressed" in contracts/CMMC**
  - Addressed under 7012(b)(2)(D)
  - Addressed in CMMC Scoping and Assessment Guides
  - Addressed in the draft CAP
- **The way the government addresses it is increasingly problematic**
- **Mandating all Cloud provided services even those not handling CUI must be FedRAMP Moderate**
  - Likely unexecutable
  - Cyber incident reporting requirements may also be problematic/costly
- **Enforcement likely results in less security**
  - **Trade small risk**: back plane attack on a CSP that might somehow then lead to a breach through the back door
  - **For much larger risk**: not using good security tools, &/or reverting to ineffective but compliant manual processes resulting in a breach through the front door

NDIA Concerns

- **NDIA Iowa Illinois Chapter Annual Midwestern Contracting Symposium**
- **World's Largest 3-D printer briefing**
  - Cursory Google search with and without "US Government"
- **At least one slide was marked CUI…but what kind?**
- **Was the presentation computer cleared for CUI?**
- **What is the government protecting on that slide?**
  - Specific technical capabilities?
  - If I don't know, how do I know what I can share?
  - Did I have a need to know? Did I need a need to know?
  - Default is to say almost nothing
- **From whom is the government protecting the information?**
  - Was everyone in the room a US person? Did they need to be?

NDIA Concerns – Failure Rate

- **Can DoD organizations meet the standard with their current IT infrastructure and processes?**
  - GAO* determined internal organizations complying with ~70-78% of requirements
- **Can other <u>Executive</u>** Branch organizations meet standards?
  - OMB?
- **Can the <u>Legislative</u>** Branch meet standards?
  - Hill oversight of MDAPs?

NDIA Recommendations

- **Current plan as NDIA understands it will result in significant failure rates across the DIB (and government)**
- **2 potential options**

1. **DoD CIO include industry in their assessment plan**
   - Without correction, 1st year assessments could carry 75%+ failure rate
   - Likely to drive industry opt outs
   - Likely to drive anger and additional congressional oversight
2. **Adjust implementation plan**
   - 80% of 110 controls = PASS
   - Max 10% of controls auto-fails
   - Consider further adjustments for small business

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Know your contracts/Know your data**
  - FAR 52.204-21; DFARS 252.204-7012/-7019/-7020
- **Be working on these controls now!**
  - 18-24 months a reasonable, serious timeline; lower costs
  - 7 months a crash program with heavy investment
  - 7 days / 7 weeks un-executable at any cost
- **Prioritize!**
  - Some controls provide larger impact
  - 100% implementation extremely difficult

Questions?

Sponsored by: CALFIRE FEDERAL