Hot Topics in Cybersecurity

June 9, 2023

Moderator:

Dan Nordquist, *Deputy Vice President for Research Operations, Office of Research Support, Washington State University*

Presenters (in order of presentations):

Kimberly Milford, *Chief Information Security Officer, University of Illinois*

Jarret Cummings, *Senior Advisor, Policy & Government Relations, Educause*

Follow COGR on LinkedIn!
linkedin.com/company/cogr

COGR

Cyber Summary (To get you up to speed again)

- The Serious
  - Since Oct. 2019, COGR - 20 times, maybe more…
- The Standard:
  - NIST Requirements - NIST 800-171
- The Standard being Implemented (at least for all of us):
  - FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems:
  - OSTP's NSPM-33 cybersecurity – "basic safeguarding protocols and procedures"
  - DOD's Cybersecurity Maturity Model Certification (CMMC).
- The Funny
  - CUI, CDI, DFARS 252.204-7012, NIST, 800-171, CMMC, DHS, FAR 52.204-21, OMB/OIRA, NDAA, and NSPM-33.

Cybersecurity Maturity Model Certification (CMMC) and Controlled Unclassified Information (CUI)

Kim Milford

CISO

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN

History of CMMC

- **2002** – Federal Information Security Management Act (FISMA) makes National Institute of Standards and Technology (NIST) responsible for developing controls for federal data
- **2011** – US Department of Defense (DoD) issues Defense Federal Acquisition Regulation Supplemental (DFARS) 252.204-7000 requiring protection of data
- **2014** – FISMA updated to account for Controlled Unclassified Information (CUI)
- **2016** – Pursuant to FISMA-2014, NIST issues Special Publication (SP) 800-171 with security controls for CUI
- **2017** – All Defense contractors required to self-attest to cybersecurity readiness
- **2019** – DoD works with a selection of contractors to develop the Cybersecurity Maturity Model Certification (CMMC)
- **2020** – General Services Administration (GSA) puts non-defense federal contractors on notice that they should prepare to comply with CMMC

History of CUI

- Historically every federal agency had its own requirements for unclassified data, resulting in different requirements between agencies for similar data

- **2004** – President Bush's *Commission on 9-11* recommends intelligence sharing between federal agencies

- **2009** – Presidential Task Force charged by President Obama with expanding the sharing recommendation to include all CUI under control of federal executive branch

- **2010** – Presidential Executive Order 13556 establishes the CUI program to standardize practices across over 100 federal agencies; state, local, and tribal agencies; private sector, academia, and industry entities

- **2016** – Office of Management and Budget (OMB) publishes final rule 32 CFR 2002 to cover Controlled Unclassified Information

https://www.archives.gov/cui/cui-history
https://www.law.cornell.edu/cfr/text/32/part-2002

Definitions: Unclassified Federal Data

Public

- Marked for public release

Federal Contract Information (FCI)

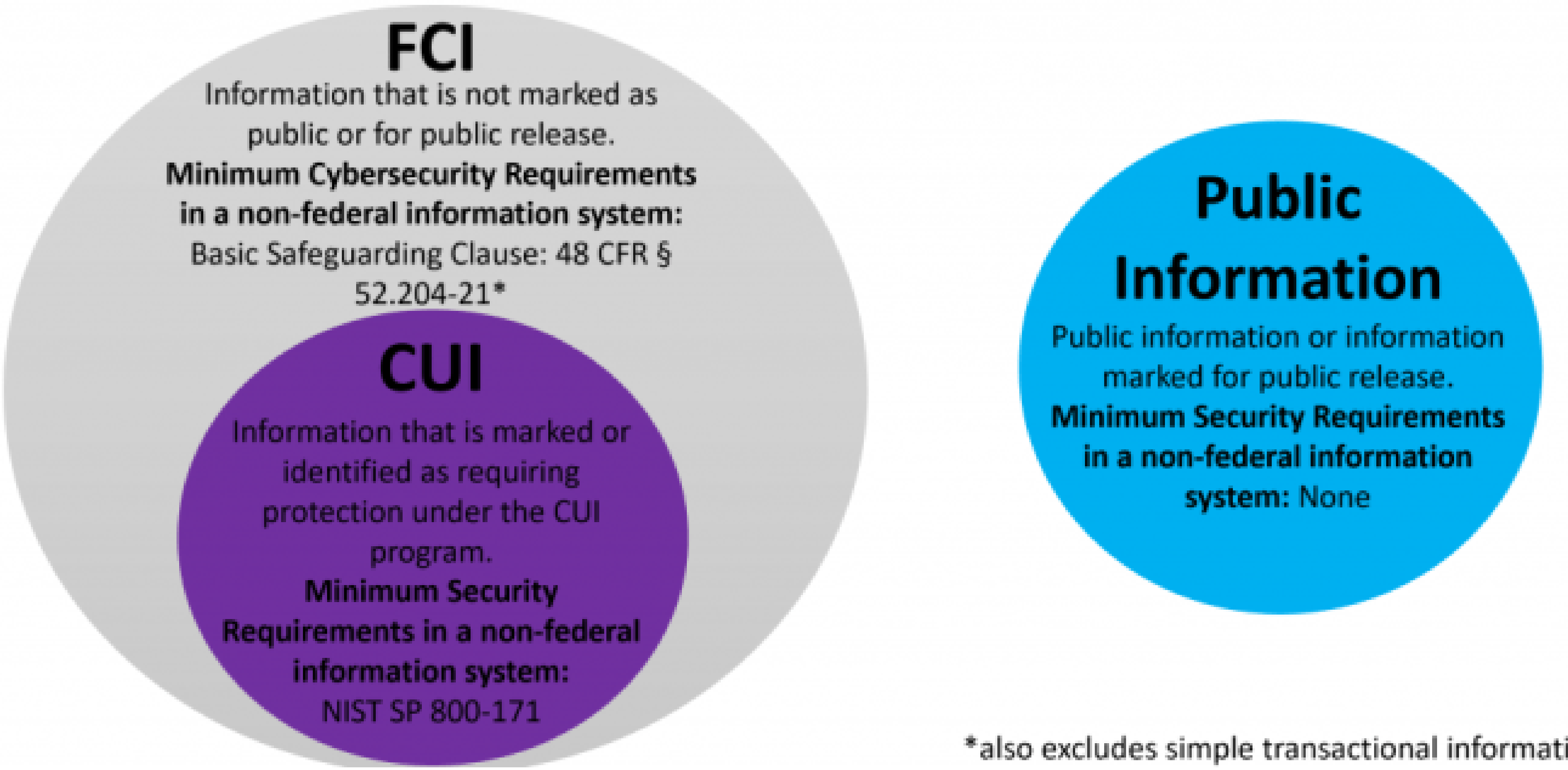
- Information not intended for public release
- Requires some basic security – minimum controls specified in Federal Acquisition Regulation (FAR) 52.204-21
- Covered by CMMC

Controlled Unclassified Information (CUI)

- Information does not meet threshold for "classified" (national security or atomic energy information)
- Requires some level of protection from unauthorized access and release
- Security requirements more stringent than basic FCI requirements, specified in NIST SP 800-171
- Protection may be required for privacy reasons or other law, regulation or federal policy
- Applies only to information held by executive branch agencies
- Covered by CMMC

All CUI is FCI, but not all FCI is CUI

Information that is collected, created, or received pursuant to a government contract



FCI

Information that is not marked as public or for public release.

Minimum Cybersecurity Requirements in a non-federal information system: Basic Safeguarding Clause: 48 CFR § 52.204-21*

CUI

Information that is marked or identified as requiring protection under the CUI program.

Minimum Security Requirements in a non-federal information system: NIST SP 800-171

Public Information

Public information or information marked for public release.

Minimum Security Requirements in a non-federal information system: None

*also excludes simple transactional information.

CMMC Version 2.0

Level	Description	Controls	Assessment	Data Type Protected
1	Foundational	17 basic cybersecurity practices from NIST 800-171	Annual Self-Assessment plus annual affirmation by leadership	Federal Contract Information (FCI)
2	Advanced	110 controls (All of NIST 800-171)	Non-Prioritized Acquisitions Annual Self-Assessment plus annual affirmation by leadership Prioritized Acquisitions (contract will specify) External Third-Party Assessment required every three years	Controlled Unclassified Information (CUI)
3	Expert	All Level 2 controls, plus 35 controls (All of NIST 800-172)	Government-led assessments every three years	Controlled Unclassified Information (CUI) deemed to be a target of Advanced Persistent Threats (APT) APT generally refers to attacks from unfriendly nation-states

CMMC Version 2.0 Updates

- Three levels instead of five
- All CMMC-unique controls and all maturity processes removed from all levels
- No external assessment required for Level 1 and certain Level 2
- DoD has suspended CMMC requirements in contracts until CMMC 2.0 final rulemaking complete
- Proposed rulemaking for Title 32 (DoD implementing CMMC 2.0) and Title 48 (Pentagon implementing controls and assessment requirements into contracts) is expected by the end of June 2023
- Allowing one year for public comment and finalization of the rules, CMMC requirements should not start showing up in contracts until federal fiscal year 2025, which begins Oct 1, 2024

EDUCAUSE

Research Cybersecurity Comment Processes

Quick (If Not The Greatest) Hits

Jarret Cummings, Senior Advisor, Policy and Govt. Relations, June 9, 2023

Poll Everywhere **Pollev.com/cogrstaff949** ***Ask a question from your seat!***

About EDUCAUSE

- Association for IT leaders/professionals in higher ed.
- Cybersecurity community = major component
- Higher Ed. Information Security Council (HEISC) = member guidance for our Cybersecurity and Privacy Program
  - HEISC 800-171 Compliance Community Grp: Research focused, main source for current comment processes
  - 800-171 group overlaps w/ Regulated Research Community of Practice (RRCoP) (NSF project)

Current Processes

- OSTP Research Security Programs Standard Requirement (Cybersecurity Protocols) (June 5th)
- NIST
    - Research Cybersecurity Resources for Higher Ed. (June 30th)
    - Draft SP 800-171, Rev. 3 (July 14th)
- NSF Research Security and Integrity Information Sharing and Analysis Organization (RSI-ISAO) (June 30)

OSTP Standard Requirement (Cybersecurity)

- SR cybersecurity “protocols” = Fed. Contract Info. requirements = sub-optimal checklist approach
- OSTP = set objectives, institutions = identify solutions
- Recommend shift to risk assessment/management model
- If not, SR should explicitly recognize need for:
  - Institutional discretion to interpret/apply via institutional policy
  - Discretion to use alt. measures/controls as appropriate

Standard Requirement (Cybersecurity) (cont’d)

Examples of other problems

- Overall lack of compliance metrics (so need discretion)
- Protocol 1 (access authorization): Drop OMB M-21-31; activity logging, not authorization; scope/cost concerns
- Protocol 3 (control external sys. access):
  - Implies only institutionally controlled devices = infeasible (cost)
  - May limit inter-institutional collaboration, use of cloud services
- Protocol 6 (authentication): Not all research equip. can…

Other Processes

- NIST 171_R3: Working group assessing
- NIST research cybersec. resources—preliminary feedback
  - Curate existing orgs./resources (e.g., Trusted CI, national labs)
  - Develop awareness/guidance resources for *researchers*
  - Produce resources to help grow research cybersec. profession
  - Collaborate w/ community on research cybersec. framework
  - Create/maintain effective practices guide for research contexts

Other Processes (cont'd)

- NSF RSI-ISAO
  - Really supposed to be an ISAO?
  - Focus on standardizing cybersec. frameworks/practices (no new)
  - Collaborate w/ relevant ISACs (e.g., REN-ISAC, MSI-ISAC)
  - Provide common tools/resources
    - Vulnerability mgt., incident mgt. in research contexts
    - Cybersec. awareness, compliance (see frameworks)

COGR Point of Contact

Robert Hardy, Research Security & Intellectual Property Director
rhardy@cogr.edu