Regulated Data and Associated Cybersecurity Frameworks: The Quest to secure CUI, FCI, and other Sensitive Data

31-March-2022

ALLEN BAXTER, CISSP

ASSISTANT DIRECTOR, RESEARCH DATA SECURITY AND COMPLIANCE

Why should you care about Data Security/Cybersecurity Compliance?

- MSU has grants and contracts with the Department of Defense – the most immediate driver of these new requirements.
- Cybersecurity compliance requirements are rapidly evolving.
- These requirements, while admittedly burdensome, can actually help to secure your data-whether research or administrative– and improve the security posture of the University.
- Will allow MSU to remain competitive and continue valuable relationships with federal partner agencies as well as those from the private sector.

Cybersecurity Compliance: A Rapidly Regulatory Evolving Environment

Evolving Federal Data Security/Cybersecurity Requirements

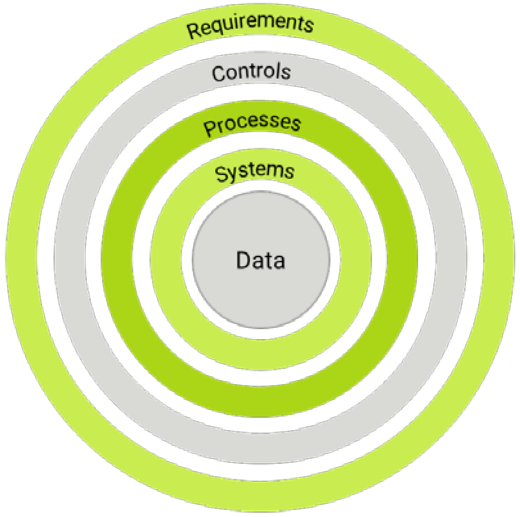
- Executive Orders/Memos
  - Obama
    - EO 13636: Improving Critical Infrastructure Cybersecurity
    - EO 13556: Controlled Unclassified Information (CUI)
  - Trump
    - **NSPM-33: Safeguards the Security and Integrity of Federally Funded R&D**
    - EO 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
  - Biden
    - EO 14028: Improving the Nation's Cybersecurity

- Regulations/Frameworks/Laws
  - Obama
    - FAR 52.204-21: Basic Safeguarding of Contractor Information Systems
    - DFARS 252.204-7012: Safeguarding CDI and Cyber Incident Reporting
    - 32 CFR 2002: Controlled Unclassified Information
  - Trump
    - DFARS 252.204-7019/20: NIST SP 800-171 DoD Assessments
    - DFARS 252.204-7021 (Rescinded by Biden Admin due to CMMC 2.0)
    - CMMC 1.0
  - Biden
    - **CMMC 2.0**, new CUI FAR rule
    - Strengthening American Cybersecurity Act
      - Mandatory cyber incident reporting for covered critical infrastructure entities

The Data

MSU Compliance Requirement

- An increasing number of compliance requirements that apply/will apply to MSU:
  - DOD CUI which primarily falls under CMMC and **existing** DFARS clauses
  - DOD FCI which primarily falls under CMMC and **existing** FAR clauses
  - CUI from the rest of the federal government
  - FCI from the rest of the federal government



Data – Do I have CUI, FCI, Proprietary info….?
Systems – What all systems do I need or intend to use? Academic Dept., Research Center, Cloud…?
Processes – How do I have to handle/protect this data? Specialized Training, policies, removeable media, disposal, process monitoring, governance….
Controls – What controls are required? NIST SP 800-171, CMMC, Basic Controls, CIS 20, ISO 27001….
Requirements – What are the requirements? FAR/DFARS, NSPM 33, HIPPA, GLBA, FERPA, Contractual Requirements….

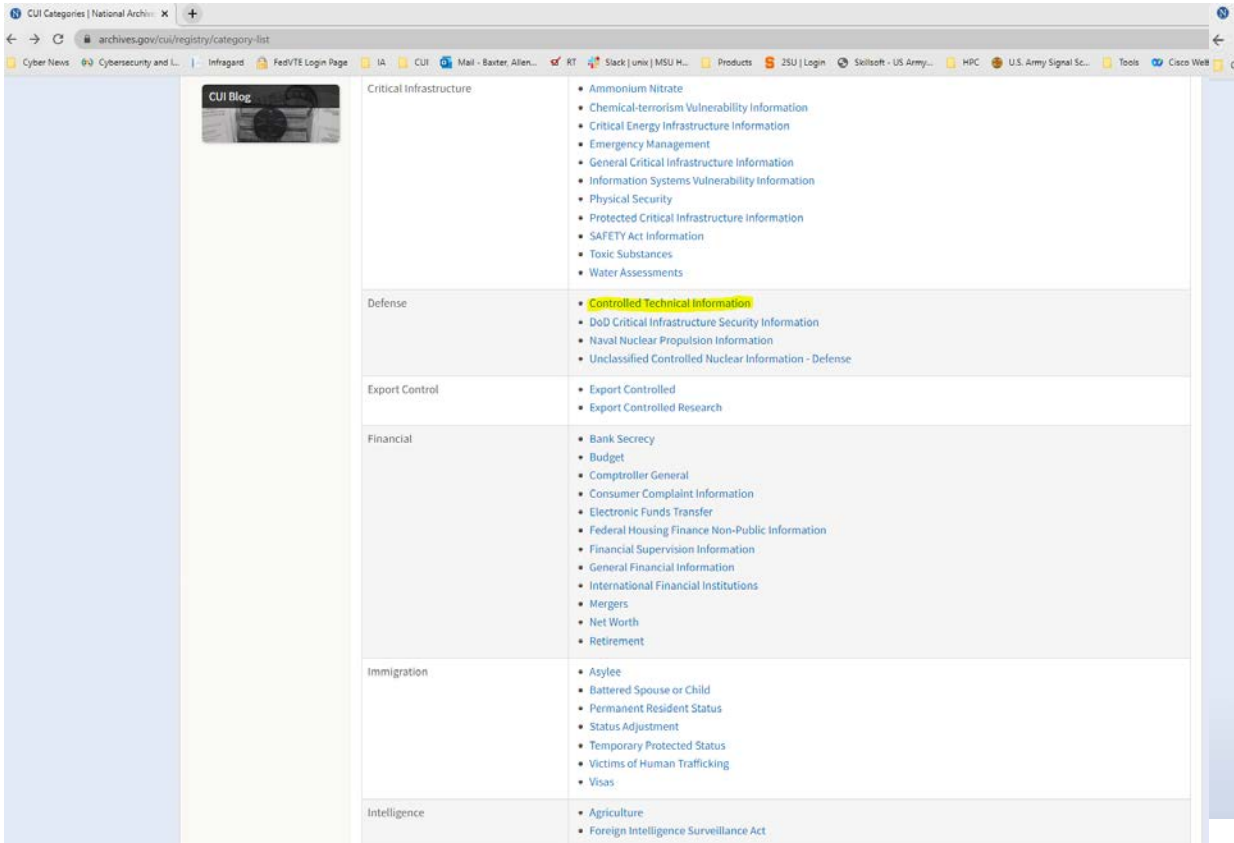
*This graphic provided by Baker Tilly

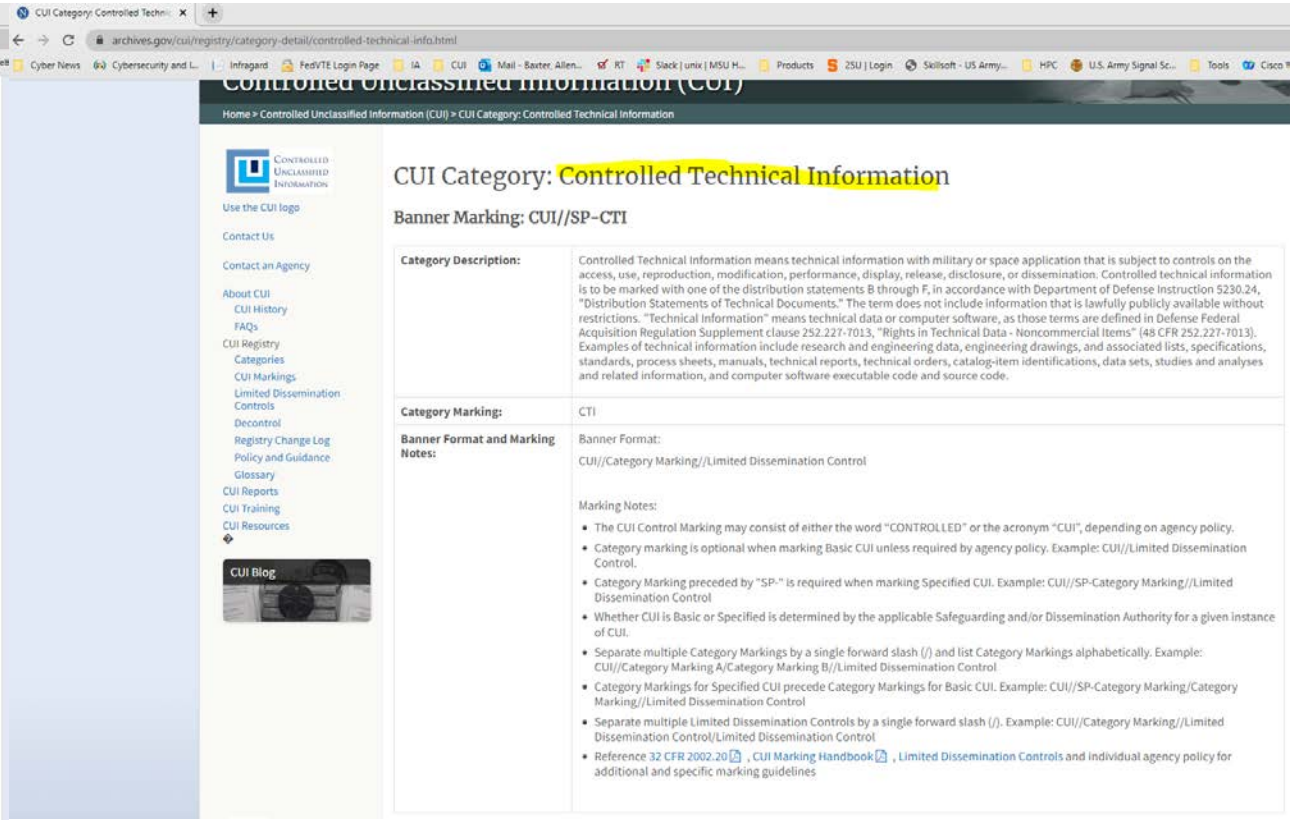
What is CUI?

- **Controlled Unclassified Information (CUI)** as defined in 32 CFR Part 2002 is information the [Federal] Government creates or possesses, or that an entity creates or possesses for or on behalf of the [Federal] Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
- CUI Program is managed by the National Archives (NARA) Information Security Oversight Office (ISOO)
- It is **Federal Government data only** but could be provided by or generated in support of a sub-contract.
  - This **does not** include classified national security information.
  - This **does not** include proprietary information.
- Covers a wide range of categories.
- Is generally protected using **NIST SP 800-171.**
  - Consists of 110 Security Controls

NARA CUI Registry

https://www.archives.gov/cui/registry/category-list



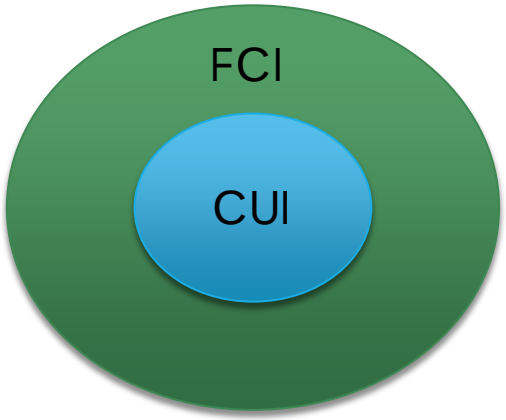


What is CDI?

- **Covered Defense Information (CDI) –** a term, specific to the Department of Defense, defined in DFARS clause 252.204-7012 as unclassified **controlled technical information** or other information, as defined in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is:
  - 1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
  - 2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
- **Basically**, **CDI is a term used by the Department of Defense (DoD)** to let the contractor know that DoD wants their CUI **protected in a more specific way than the rest of the federal government**.
  - Currently protected using DFARS 252.204-7012
  - In 9 to 24 months it will be protected via a new **DFARS rule and CMMC Level 2**

What is FCI?

- " **Federal contract information (FCI)** means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments." –FAR 52.204-21
- "All CUI in possession of a Government contractor is FCI, but not all FCI is CUI." – NARA
- For non-DoD Federal entities security requirements are contractually implemented via FAR 52.204-21.
  - **Consists of 15 Basic Cybersecurity and Physical Security Measures**
- **This is NOT specific to DoD or CMMC**



Other Data Security Requirements and Considerations

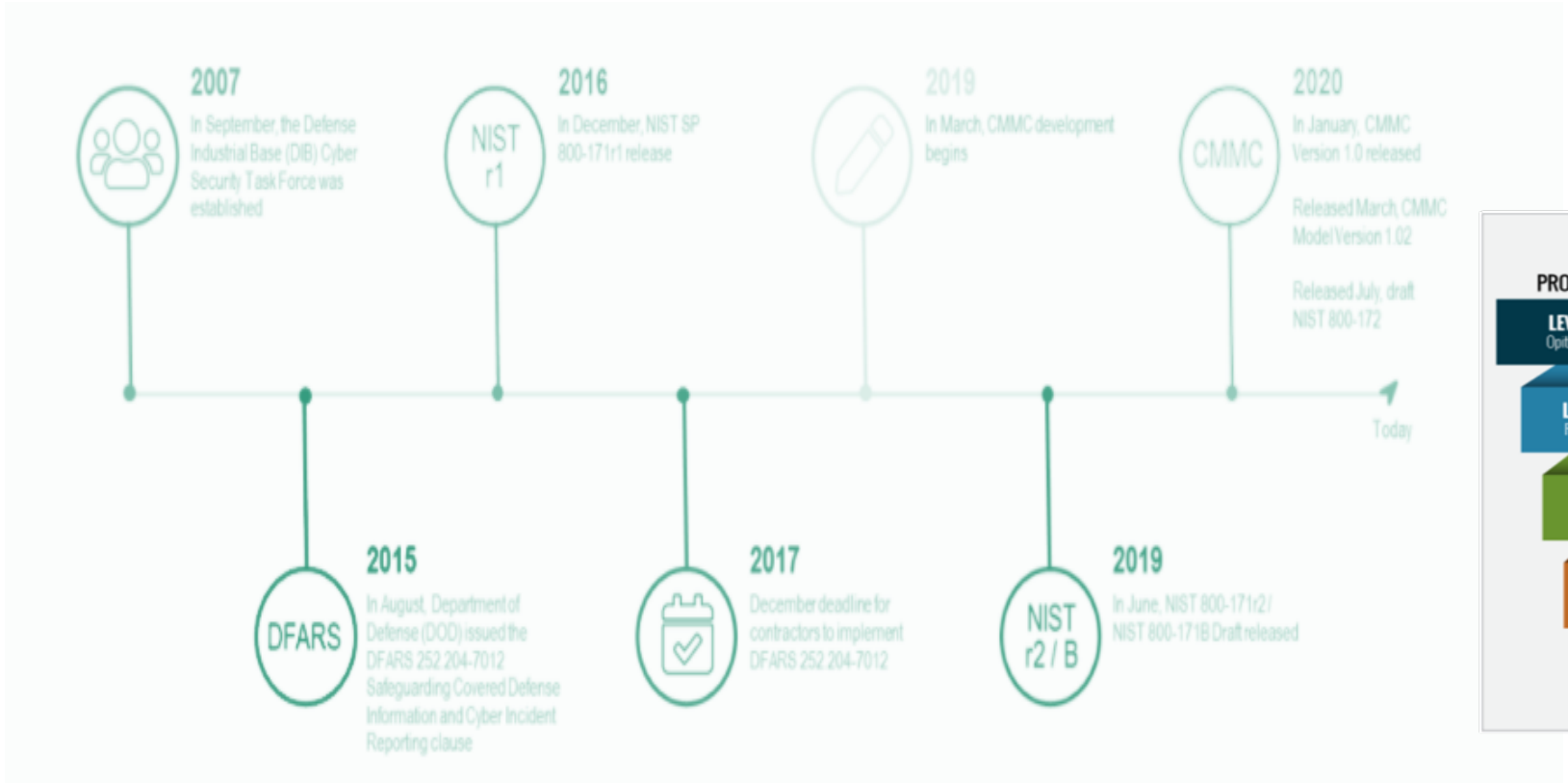
- PI and Administrators should be aware that are many different cybersecurity frameworks that can be incorporated in grants and contracts (i.e. ISO 27001, CIS 20, etc..) or associated with specific data sets.
- You should contact the MSU Office of Research Security and Compliance (ORC&S) or ITS if you have questions about how or if you can comply with these requirements.
- If the determination is made that there is no capacity for compliance, then you should discuss these concerns with your sponsor.
  - Any exceptions should be clarified in writing by the contracting officer.

Cybersecurity Maturity Model Certification (CMMC)

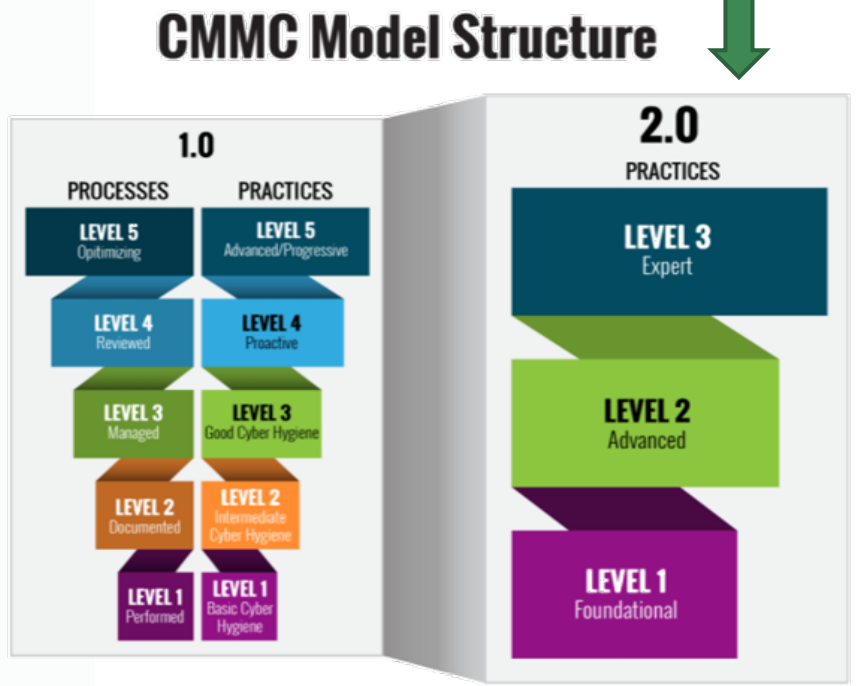
What is CMMC?

- **Cybersecurity Maturity Model Certification (CMMC)** is a Department of Defense program that aims to address cybersecurity risks to every level of the DoD supply chain.
- CMMC is an evolution of the DFARS 252.204-7012 which mandated compliance with NIST SP 800-171 (among other requirements).
- The entire CMMC model and associated requirements **changed in November 2021 from CMMC 1.0 to CMMC 2.0**. The general impact of these changes is that it reduced the number of security controls that we have to implement, reduced third party certification requirements for Level 1, and condensed our implementation timeline:
  - Security Controls reduced from 130 to 110 for CMMC L2.
  - Third-Party Certification is no longer required for Level 1.
  - An Executive University Official will have to make an annual attestation of compliance with these requirements IF we are not required to receive third-party certification (i.e. the years between 3rd party certs).
  - Implementation Timeline reduced from 4 years to "9 to 24 months."

DoD, NIST 800-171, DFARS, and the evolution of CMMC



Today we are here!



DFARS, FAR, NIST SP 800-171, CMMC: How does MSU get these requirements?

- Contractual Channels
- Non-Disclosure Agreements (NDA)
- Interconnection Security Agreements (ISA)
- In other words, and generally speaking, via a document that someone at the University signs.

Considerations in Negotiating Contracts with Restricted Research Data

- Validate that any security requirements defined in the contract actually needs to be there.
- Ask the contracting officer from the sponsor agency to clarify what CUI, FCI, etc.. is being provided or will be generated in support of the contract.
- Ensure that you can actually comply with the security requirements outlined in the contract.
- Some requirements are required to “flow down.” Thus some security requirements may be present in a sub-contract but no actual sensitive or restricted data is being provided or generated.

General Data Security Considerations – Regulated Data

- CUI/FCI should generally not be stored, processed, or transmitted on cloud-based systems not specifically designated for this type of data.
- CUI should be properly marked (see NARA ISOO CUI Website).
- Procedures for alternate worksites and media control should be developed with the assistance of ORC&S or ITS for projects involving CUI.
- Physical Security Considerations.
- Proper Destruction.

Current and Future Capabilities to Support Compliance: What is MSU doing?

- Currently **MSU HPC2 is the only entity** on campus with the ability to store, process, or transmit CUI or FCI.
- Developed a comprehensive scoping strategy to address CMMC Level's 1 and 2.
  - Validating strategy and reviewing processes with outside firm.
- PreVeil for File Transfer, Storage, Compliant Email
- Level 1 Enclaves
- Updating Policies, Procedures, and Training

Resources to Help

- Allen Baxter, ITS
- Office of Research Compliance and Security
- https://www.archives.gov/cui
- https://cmmcab.org/
- https://www.acq.osd.mil/cmmc/
- MSU Information Security Program
  - https://www.infosecurity.msstate.edu/

Questions?