What's Hot in Cybersecurity & Implications for Institutions

February 26, 2025

Speakers:

#COGRFeb25

Melissa Bianchi, Partner, Hogan Lovells

Laura Raderman, Policy and Compliance Coordinator, Carnegie Mellon University

Moderator:

Kevin Wozniak, Director, Research Security & Intellectual Property

COGR

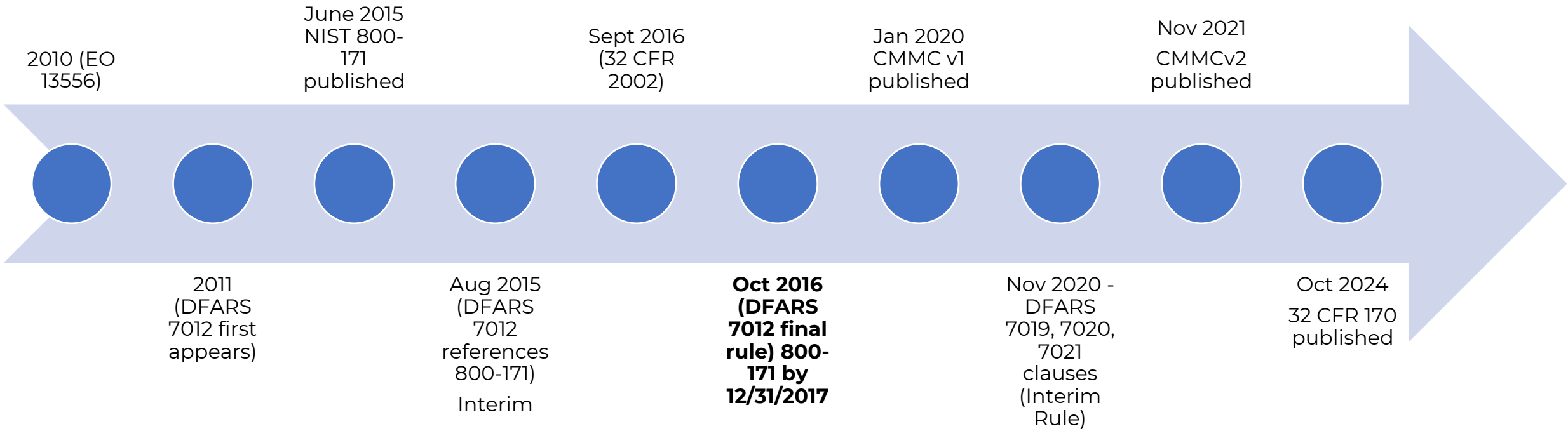
CMMC

#COGRFeb25

Cybersecurity Maturity Model Certification

COGR

Short History Lesson



#COGRFeb25

COGR

CMMC v2.0

Level 1	• Federal Contract Information • Basic Safeguarding Clause (15 controls)
Level 2	• Controlled Unclassified Information (CUI) • NIST SP 800-171 (110 controls)
Level 3	• "Priority Program"[1] • 24 additional controls from NIST SP 800-172

1: https://www.federalregister.gov/d/2024-22905/p-349

Does this affect me?

"***Federal contract information*** 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." (48 CFR 52.204-21)

"Controlled Unclassified Information (CUI) is **information the Government creates or possesses**, or that an entity **creates or possesses for or on behalf of the Government**, that **a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls**. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency." (32 CFR 2002.4)

No FCI or CUI? CMMC will not apply[2]

2: Inputs to fundamental research can be FCI or CUI, even if the output is not (CMMC Proposed Rule https://www.federalregister.gov/d/2023-27280/p-185)

3rd Party verification

- Turns out relying on people to self-report that they are compliant with NIST 800-171 doesn't work so well.
- CMMC is a program by the Department of Defense to require a 3rd party certification that a particular (sub-)contractor is meeting all of NIST 800-171 controls, as verified by the CMMC Assessment Guide (based on NIST 800-171A)
- Provides a "commercial" extension of the DIBCAC (Defense Industrial Base Cybersecurity Assessment Center)

Assessments

- Level 1: FCI
  - self-assess annually, enter affirmation in Supplier Performance Risk System (SPRS)
- Level 2: CUI
  - self-assess annually (affirm in SPRS)
  - pay a 3rd party (C3PAO) for assessment every 3 years
    - Some contracts will allow self-assessment every 3 years (we have some guidance from the DoD)
  - Report your score at least every 3 years to the SPRS - DFARS 252.204-7019
- Level 3: CUI priority program
  - *after* obtaining a Level 2 (C3PAO) certification, the DIBCAC will assess against Level 3 controls

3rd Party Assessment Guidance

- Follow CMMC Assessment Guides for all levels (including self-assessments!)
  - Level 1: Basic Safeguarding
    - **15** controls, **59** assessment objectives
  - Level 2: NIST SP 800-171 revision 2
    - **110** Controls, **320** assessment objectives
  - Level 3: NIST SP 800-172 (selected controls)
    - **24** controls, **88** assessment objectives
  - **Pass/Fail** (some allowance for not 100% “passing”, but very limited)

Estimated Costs of a CMMC Assessment

Annually	"Small" entities	"Other than small" entities
Level 1 Self-Assessment (annually)	$5,977/year	$4,042/year
Level 2 Self-Assessment (every 3 years)	$37,196/3 years	$48,827/3 years
Level 2 Certification (every 3 years)	$104,670/3 years	$117,768/3 years
Level 3 Certification (every 3 years)	$12,802/3 years	$44,445/3 years

https://www.federalregister.gov/d/2024-22905/p-1229

What's not included in DoD cost estimates

- In order to get a Level 3 certification, you have to have already gotten (and paid for) a Level 2 certification

	"Small"	"Other than small"
Level 3 Certification + Required Level 2 (every 3 years)	$117,472/3 years	$162,213/3 years

- Implementation costs for Levels 1 and 2 are not included in the (CMMC) analysis at all
- Level 3 implementation costs are analyzed as they're "new", but are not included in these tables

Implementation Costs (information from CMMC rule as well as FAR CUI rule)

Annually	"Small" entities	"Other than small" entities
Level 1 Implementation	No estimate	No estimate
Level 2 Implementation	Non-recurring: $175,700 Recurring: $103,800/yr	Non-recurring: $683,400 Recurring: $574,000/yr
Level 3 Implementation	Non-recurring: $2,700,000 Recurring: $490,000/yr	Non-recurring: $21,100,000 Recurring: $4,120,000/yr

https://www.federalregister.gov/d/2024-30437/p-92 (Level 2)
https://www.federalregister.gov/d/2024-22905/p-1411 (Level 3)

Who does all this?

CMMC is NOT only an IT/Security “Problem”

- Yes, most of the controls are going to fall to your IT or Security groups
- Many will fall to your physical teams (building management, etc)
  - All Physical controls (PE)
- Some will fall to HR
  - background screening
  - personnel termination/transfer
- Depending on your organization, many can also fall to researchers
  - Training requirements
  - Not posting information publicly
  - Physical security of lab space

Documentation!!

Culture Change

CMMC implementation typically goes against university culture that promotes openness and sharing – also potentially confusing PIs that don't have to worry about it.

Culture Change is Organizational Change and should be managed as such.

Hogan Lovells

HIPAA Security Rule
Notice of Proposed Rulemaking

February 2025

Executive Summary

- On December 27, 2024, the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) issued a proposed rule modifying the HIPAA Security Rule
- The proposed rule would require HIPAA covered entities and business associates to enhance cybersecurity protections for individuals' electronic PHI
- The proposal *significantly* revises the Security Rule's existing requirements pertaining to administrative, physical, and technical safeguards
  - The Security Rule was last modified in 2013 (primarily to extend to business associates, per the HITECH Act)
  - Otherwise the Security Rule has remained substantially unmodified since 2003
- Public comments on the NPRM are due March 7, 2025
- The current Security Rule remains in effect
- The Trump Administration could maintain this timeline, delay/seek new comments, decline to proceed with a final rule

HIPAA Basics

- HIPAA covers "protected health information" (PHI) – information in any form that is created or received by a covered entity and:
  - relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and
  - identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- Includes information transmitted in oral, paper or electronic form

Who must comply with HIPAA?

- Covered Entities (CEs)
  - Health care providers (e.g., hospitals, pharmacies, physicians)
    - Who engage in standard transactions
  - Health plans
  - Health care clearinghouses
- Business Associates (BAs)
  - An entity that creates, receives, maintains or transmits PHI on behalf of a covered entity to perform a function or activity for that CE
    - E.g., claims processing, quality assurance, benefit management, data aggregation, administrative services
    - BA s are BAs by virtue of their roles; liable even if don't enter into a business associate agreement (BAA)

Who must comply with HIPAA?

- Covered Entities (CEs)
  - Health care providers (e.g., hospitals, pharmacies, physicians)
    - *Who engage in standard transactions*
  - Health plans
  - Health care clearinghouses
- Business Associates (BAs)
  - An entity that creates, receives, maintains or transmits PHI on behalf of a covered entity to perform a function or activity for that CE
    - E.g., claims processing, quality assurance, benefit management, data aggregation, administrative services
    - BA s are BAs by virtue of their roles; liable even if don't enter into a business associate agreement (BAA)

Hybrid Entities under HIPAA

- Hybrid entity
  - Separates HIPAA covered functions from non-HIPAA functions
  - HIPAA functions
    - E.g., health care provider functions that engage in standard transactions
    - Internal business associates
  - Research functions may not need to be included:
    - Research components, even if they function as a health care provider may be, but are not required to be, included in the health care component of the hybrid entity if they do not engage in standard electronic transactions
    - Requires identifying research studies to which HIPAA applies
- Understand your institution's HIPAA structure when considering the applicability of the

Types of Safeguards Required by the Security Rule

The categories remain the same

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

HHS's Stated Purpose and Goals

- The proposal "seeks to strengthen cybersecurity by updating the Security Rule's standards to better address ever-increasing cybersecurity threats to the health care sector" and "to reflect advances in technology and cybersecurity"

- According to HHS, the proposal is intended to revise the Security Rule to address:
  - changes in the environment in which health care is provided
  - significant increases in breaches and cyberattacks (particularly ransomware attacks against health care)
  - common deficiencies OCR observed during investigations into Security Rule compliance of regulated entities
  - other cybersecurity guidelines, best practices, methodologies, procedures, and processes
  - court decisions that affect enforcement of the Security Rule

- HHS further notes that the proposal is in support of President Biden's commitment to improving the cybersecurity of critical infrastructure (which has been a broad federal government priority across recent administrations)

Summary of Key Themes

- Shifts away from the historical focus on flexibility/scalability
  - Existing approach: some provisions are *addressable* and others *required*
  - New approach: Security Rule provisions *are all requirements*, even for ones previously interpreted as optional
  - Defines *more granular and prescriptive requirements* to implement, maintain, and document regulated entities' implementation of the required security measures

- Increases accountability:
  - new requirements requiring regulated entities to review and test written policies/procedures/controls *at least once every 12 months* or in response to environmental or operational changes, and modify as reasonable and appropriate

- Requires regulated entities with "deploy technical controls" instead of the current "implement" throughout the Technical Safeguards, to clarify the requirement to actually *operationalize* certain policies/procedures through technical controls

Key changes to Administrative Safeguards

New Safeguards

- **Technology Asset Inventory**
  - New general standard requiring regulated entities to conduct and maintain (1) an accurate and thorough written inventory and (2) a network map of the entity's electronic information systems and all technology assets that may affect the confidentiality, integrity, or availability of ePHI
- **Compliance Audit**
  - New general standard requiring regulated entities to conduct a compliance audit at least once every 12 months to ensure compliance with the Security Rule
- **Security Awareness Training**
  - Replaces all previous specifications with new specifications on training content, timing of initial and refresher trainings, ongoing education activities, and training records
- **Patch Management**
  - New general standard requiring regulated entities to implement written policies and procedures for applying patches and updating the configuration(s) of the entity's relevant electronic information systems, with defined intervals of 15 days for critical-risk patches and 30 days for high-risk patches

Key changes to Administrative Safeguards

New Safeguards

- **Business Associate Contracts and Other Arrangements**
  - New "written verification" specification requiring that business associates verify at least once every 12 months for covered entities (and that downstream business associates verify at least once every 12 months for business associates) that they have deployed Security Rule technical safeguards to protect ePHI via
    - written analysis of the business associate's relevant electronic information systems by a subject matter expert, and
    - written certification that the analysis has been performed and is accurate
- **Delegation to Business Associate**
  - New general standard: a covered entity or business associate that delegates actions/activities to a business associate remains liable for compliance with the Security Rule

Key changes to Administrative Safeguards

Enhanced Safeguards

- **Risk Analysis**
  - Upgrades previous implementation specification to general standard; requires greater specificity for conducting risk analyses
- **Information Access Management**
  - New specifications on authentication management (including MFA) and network segmentation
- **Risk Management**
  - New specifications on planning, priorities, and implementation of security measures in response to identified risks
- **Information System Activity Review**
  - New specifications on policies/procedures, scope, record review, record retention, and response
  - Includes identification of activities that are to be reviewed and be escalated to incidents
- **Workforce Security**
  - New specifications requiring 1-hour removal of access after termination, notification of certain regulated entities within 24 hours when a workforce member's access to ePHI or certain electronic information systems is changed or terminated, and other account management enhancements

Key changes to Administrative Safeguards

New and Enhanced Safeguards

- **Security Incident Procedures & Contingency Plan**
  - Strengthens requirements for planning for contingencies and responding to security incidents by requiring regulated entities to establish:
    - Written procedures to restore the loss of critical information systems and data within 72 hours and to restore other systems and data based on the criticality analysis
    - Written incident response plans and procedures documenting how workforce members are to report suspected/known incidents and how the entity will respond to suspected/known incidents
    - Implement written procedures for testing and revising written security incident response plans and contingency plans

Key changes to Physical Safeguards

Enhanced Safeguards

- **Access Management and Validation Procedures**
  - written policies and procedures that constitute the facility security plan must apply to all of the regulated entity's facilities and equipment contained within those facilities
  - Written procedures to authorize and manage a person's role-based access to facilities
- **Physical Maintenance Records**
  - Adds security cameras to list of physical safeguards requiring policies and regular review
- **Test every 12 months**
  - Consistent with other proposed requirements, test written policies at least every 12 months and implement any needed updates
- **Workstations**
  - New definition to capture full scope of technology and related physical safeguards
  - Requires disposal and removal policies for ePHI (e.g., for photocopiers, other technology)

Key changes to Technical Safeguards

Enhanced Safeguards

- **Audit Trail and System Log Controls**
  - Redesignates and expands the existing "Audit controls" standard and modifies to require a regulated entity to deploy technology assets or technical controls that record and identify activity in all relevant electronic information systems, not merely electronic information systems that create, receive, maintain, or transmit ePHI
- **Encryption and Decryption**
  - Encryption at rest and in transit
    - Exceptions to the proposed specification
    - Where an exception would apply, a regulated entity must implement alternative measures and compensating controls
- **Authentication**
  - New specification requiring:
    - Use of Multi-factor authentication (MFA)
      - Some exception
      - Where an exception would apply, a regulated entity must implement alternative measures and compensating controls

Key changes to Technical Safeguards

New Safeguards

- **Access Controls**
  - New specifications on:
    - Administrative and increased access privileges
    - Log-in attempts
    - Network segmentation
    - Data control limitations to approved users and technology assets
- **Vulnerability Management**
  - New general standard that includes specifications on:
    - Vulnerability scanning
    - Monitoring for known vulnerabilities and remediating
    - Penetration testing
    - Patch and update installation
- **Information Systems Backup and Recovery**
  - New general standard that would require regulated entities to deploy technical controls to create and maintain backups of relevant electronic information systems, and review and test the effectiveness of such controls at least once every six months or in response to environmental or operational changes

Group Health Plans and Plan Sponsors

Expands Scope of Rule to New Entities

- Require group health plans to include in their plan documents requirements for their group health plan sponsors to:
  - Comply with the administrative, physical, and technical safeguards of the Security Rule
  - Ensure that any agent to whom they provide ePHI agrees to implement the administrative, physical, and technical safeguards of the Security Rule
  - Notify their group health plans upon activation of their contingency plans without unreasonable delay
- Plan sponsors > employers who offer group health plans to employees

FAR CUI Rule

#COGRFeb25

(Proposed)
FAR CUI Rule

COGR

Differences from CMMC (1)

- Optional 3rd party verification ("Validation Actions"- up to each agency)
- Introduces the SF-XXX (number TBD) that is supposed to tell you what is/is not CUI at the Category level
- Standardizes on NIST 800-171 revision 2 and SP 800-172
  - Except each agency can dictate additional controls necessary at their discretion
- Federal Contractor Information (FCI) is now Covered Federal Information (CFI)
- The FAR CUI Rule includes requirements that were only in DFARS 7012 on the DoD side
  - 8 hour "suspected incident" reporting requirement (vs 72 for DoD)
  - Preservation of evidence for 90 days in case of incident
  - Must use FedRAMP Moderate Cloud Service Providers

Differences from CMMC (2)

- Requires training on CUI at the frequency defined by the agency (on the SF-XXX)
- Requires submission of a System Security Plan and Plan of Actions and Milestones to an agency upon request
- Requires contractors to report when they think they've seen unmarked CUI
  - And safeguard it properly until the Government Contracting Officer confirms it is/is not CUI
- **Scoping is different** in 800-171 than CMMC, don't do more than you have to.

Scoping for NIST SP 800-171

- Very subtlety different than CMMC

- Does the asset process, store or transmit CUI? In-scope
- Does the asset provide security protections for a CUI Asset? In-scope
- Does the asset do neither? Out-of-scope
  - No concept of Contractor Risk Managed Assets

- 800-171 (not CMMC!) allows for assets to not meet all 110 controls
  - If it can't (older technologies, manufacturing equipment, etc.)
  - There's a business reason it can't (be prepared to explain yourself)