Cybersecurity Implementation and Updates from the University Perspective

October 23, 2025

COGR

Advancing Effective Research Policy

www.cogr.edu

www.linkedin.com/company/cogr

Cybersecurity Implementation and Updates from the University Perspective

October 23, 2025

Speakers:

Thomas Burns, Assoc. Vice Provost, Research Compliance, Johns Hopkins University

Kelly Hochstetler, Assoc. Vice President for Research, University of Virginia

Allen DiPalma, Exec. Director, Office of Research Security & Trade Compliance, University of Pittsburgh

Moderator:

Kevin Wozniak, Director of RSIP

COGR

Is your institution planning on meeting any of CMMC compliance requirements at any level? (*Assumption: Your Institution also plans to meet the lower-level requirements as well)

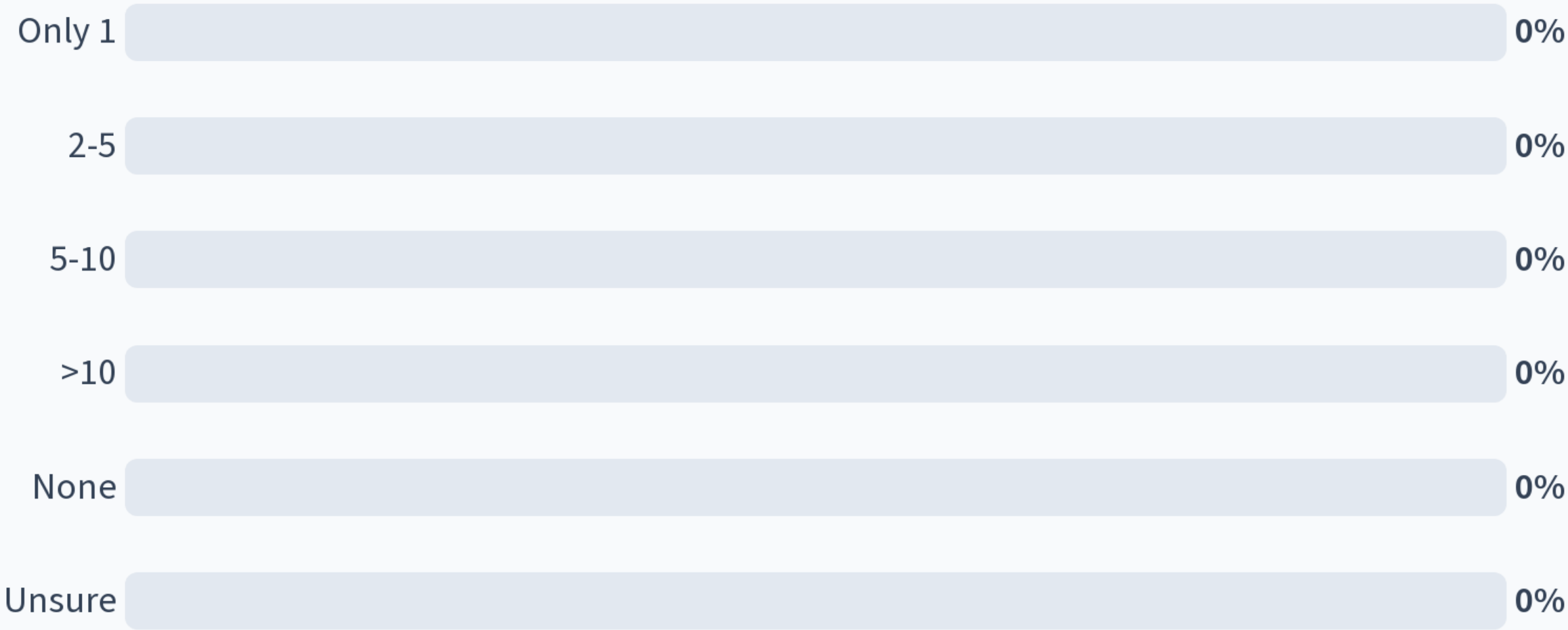
Yes, Level 1 only	0%
Yes, Level 2 and Level 2 self-certification	0%
Yes, Level 2 third-party assessment*	0%
Yes, eventually Level 3 certification*	0%
No, at least not at this time	0%

How would you describe your institution's current readiness for CMMC compliance?

How is your institution planning to implement CMMC Level 1 requirements?

Contract- or Project-specific plans	0%
Dedicated enclave(s)	0%
Dedicated cloud environment(s)	0%
Institution-wide	0%
More than one of the above	0%
We won’t accept CMMC Level 1, at least not at this time	0%

How many CMMC Level 1 environments does your institution plan to register with SPRS?



What is your institution's biggest challenge in preparing for CMMC implementation?

Funding and resource allocation	0%
Understanding applicability and scope	0%
Coordinating across multiple departments (IT, research, compliance)	0%
Limited staff expertise in cybersecurity standards (e.g., NIST 800-18=71)	0%
Communicating requirements to PIs and research teams	0%

Who currently "owns" responsibility for CMMC compliance at your institution?

Central IT or information security office	0%
Research compliance/sponsored programs office	0%
Departmental IT or research units	0%
We don’t have a designated owner (yet)	0%
Unsure	0%

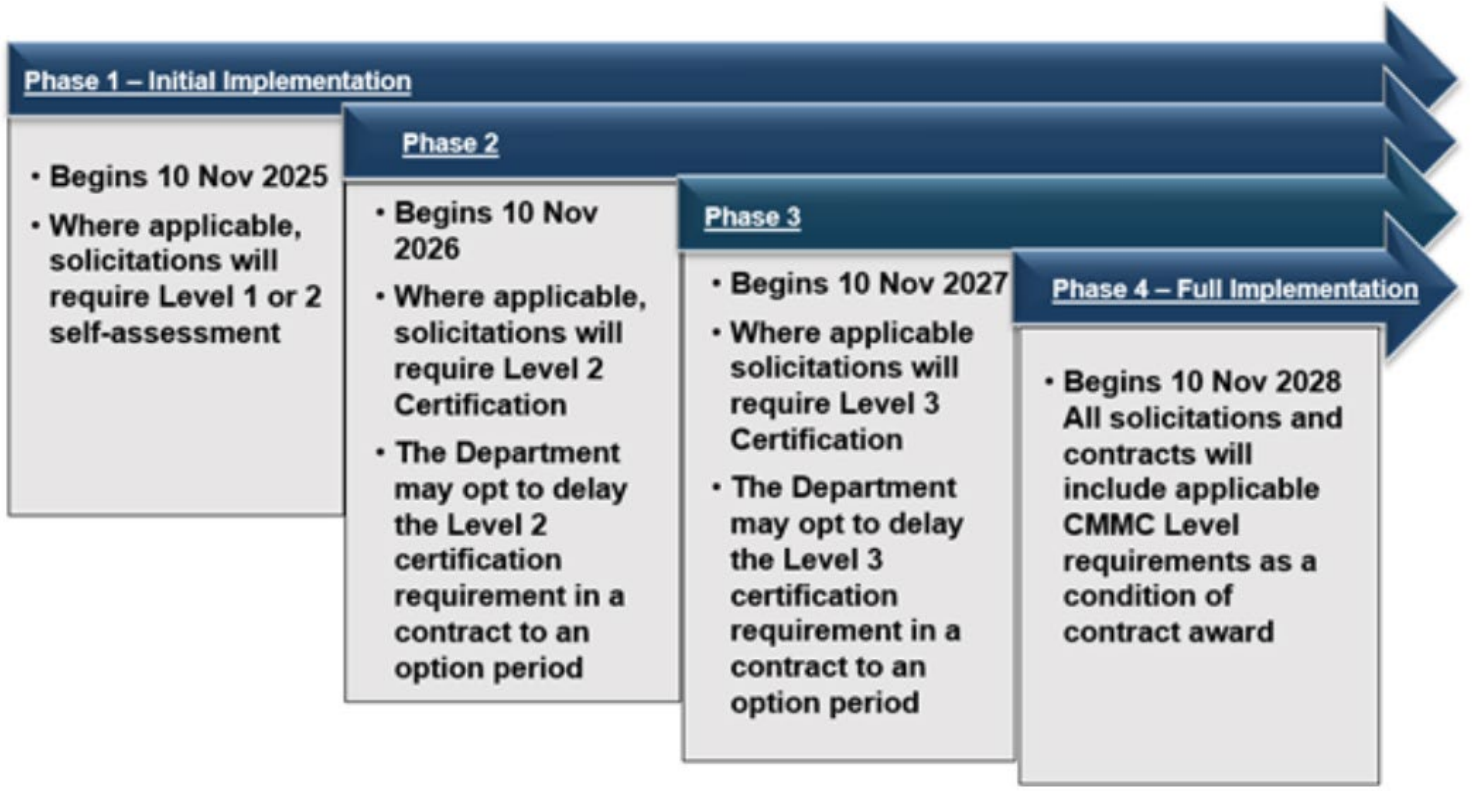
UVA FACTS

- 12 Academic Schools + College at Wise
- Comprehensive Health System
- 6 pan-U Institutes
- 3.2K FT Faculty
- 9K Graduate & Professional Students
- $714M (48th) FY23 HERD R&D
- $571M FY25 Awards
  - $437M Federal (direct & indirect)
  - $51M DOD (all mechanisms)
- Investment in NIST 800-171
  - 2018-2023 Bootstrapped
  - 2023-2025 Significant
- CMMC Level 2 Preparedness (~95%)
- CMMC Level 1 Preparedness (TBD)

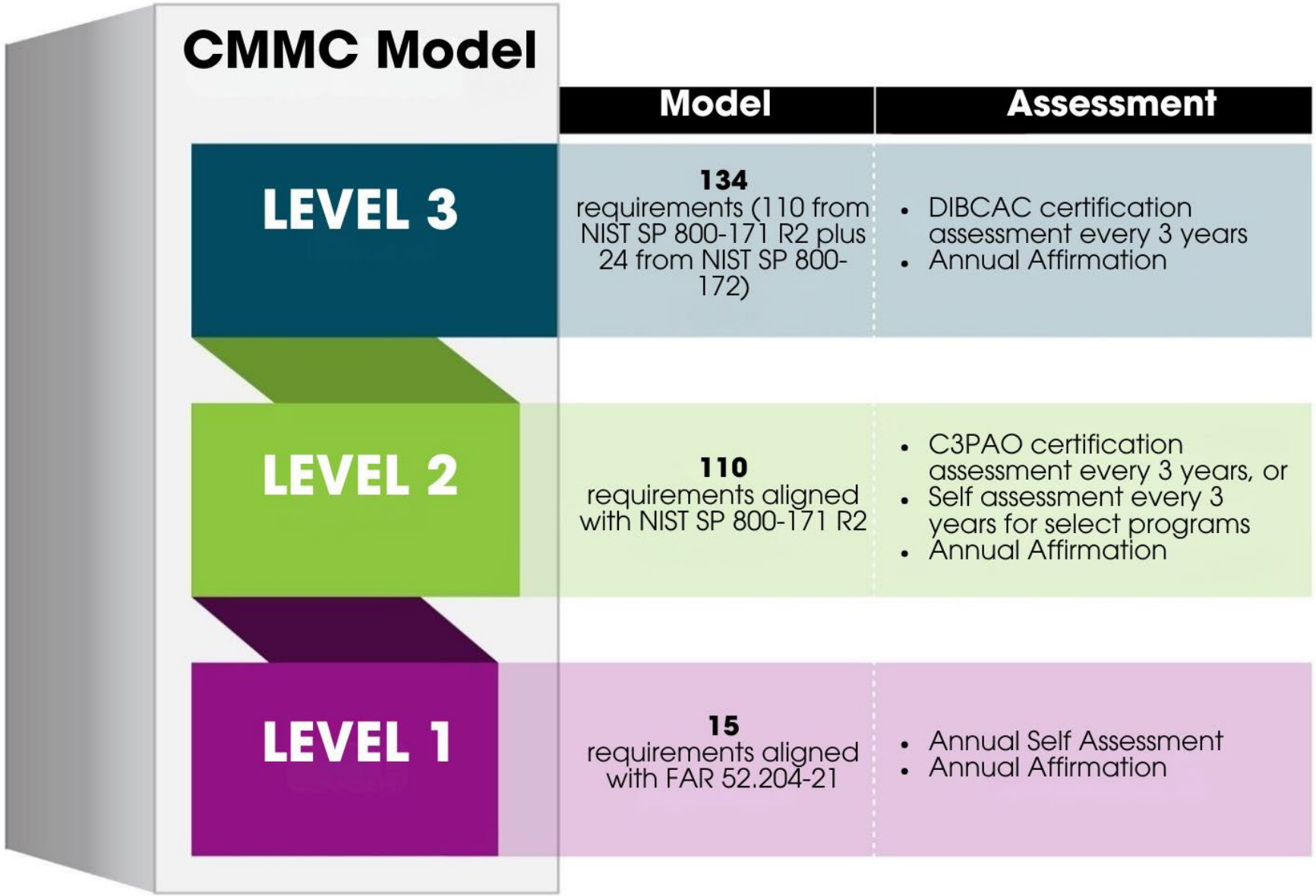
Cybersecurity Maturity Model Certification (CMMC)

- Federal Agency: Department of Defense
- Mechanism(s): Contracts (and OTAs?)
- DFARS 252.204-7021
- Timeline: 3 Years starting November 10, 2025
- Initial Impacts: Solicitations and Vendor Profiles

CMMC Timeline



In some procurements, DoD may implement CMMC requirements in advance of the planned phase


CMMC Model
Model
Assessment
LEVEL 3
134 requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)
DIBCAC certification assessment every 3 years
Annual Affirmation
LEVEL 2
110 requirements aligned with NIST SP 800-171 R2
C3PAO certification assessment every 3 years, or
Self assessment every 3 years for select programs
Annual Affirmation
LEVEL 1
15 requirements aligned with FAR 52.204-21
Annual Self Assessment
Annual Affirmation

CMMC Level 1 - Requirements

- Federal Contract Information (FCI)

  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

- Basic Safeguarding Requirements (FAR 52.204-21)
- Annual self-assessment w/ Results Entered in the Supplier Performance Risk System (SPRS)
- Annual (re)affirmation of compliance
- All assets that process, store, or transmit FCI
- No POA&Ms permitted

CMMC Level 1

Access Controls (AC)

- Authorized Access Control
- Transaction & Function Control
- External Connections
- Control Public Information

Physical Protections (PE)

- Limit Physical Access
- Escort Visitors
- Physical Access Logs
- Manage Physical Access

Media Protection (MP)

- Media Disposal

Identification & Authentication (IA)

- Identification
- Authentication

Systems and Communications Protection (SC)

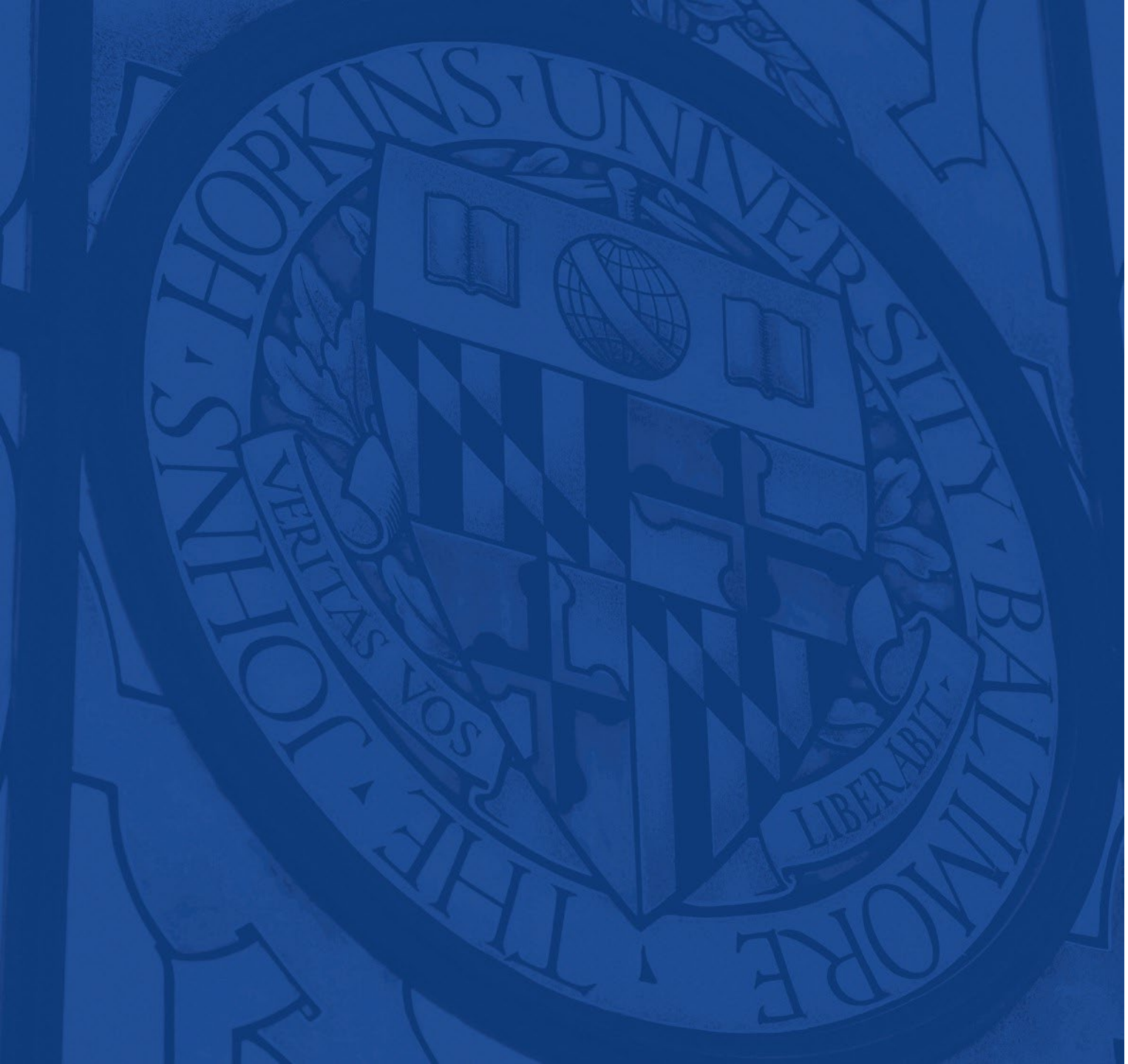
- Boundary Protection
- Public-Access System Separation

System and Information Integrity (SI)

- Flaw Remediation
- Malicious Code Protection
- Update Malicious Code Protection
- System & File Scanning

UVA Implementation Challenges

- Scoping: How many environments?
- Assessment: Which assets?
- Ownership: Who's responsible?
    - Programmatic
    - IT Assets
    - Academic or Health System
    - Personnel
- Physical Security
    - Public Buildings
    - Shared/Multi-use Spaces



JOHNS HOPKINS
UNIVERSITY & MEDICINE

Cybersecurity and CMMC 2.0 Compliance at JHU

JHU at a Glance

- 11 Schools and Divisions
- 3700 FT Faculty
- $3.3B federal R & D expenditures FY23
- $857M NIH funding FY24
- 2021-2023 Significant institutional investment towards NIST 800-171 compliance
- 2025 Research IT secure infrastructure compliant with NIST 800-171 Rev. 2/3

Cybersecurity at JHU

- Research IT environment- centrally managed enclave/secure environment approved by University CISO/CIO to comply with NIST 800-171 standard (May 2025). **CMMC Levels 1 and 2 assessments are specific to this enclave**
- Specialized research centers and groups (located off-campus) that handle classified/restricted research and CUI.
  - Energetics Research Group (separate CAGE)
  - Human Language Technology Center of Excellence
- School and Department-level environments- locally managed. These are not NIST compliant and not currently in-scope for CMMC assessments

CMMC Level 2 Self Assessment

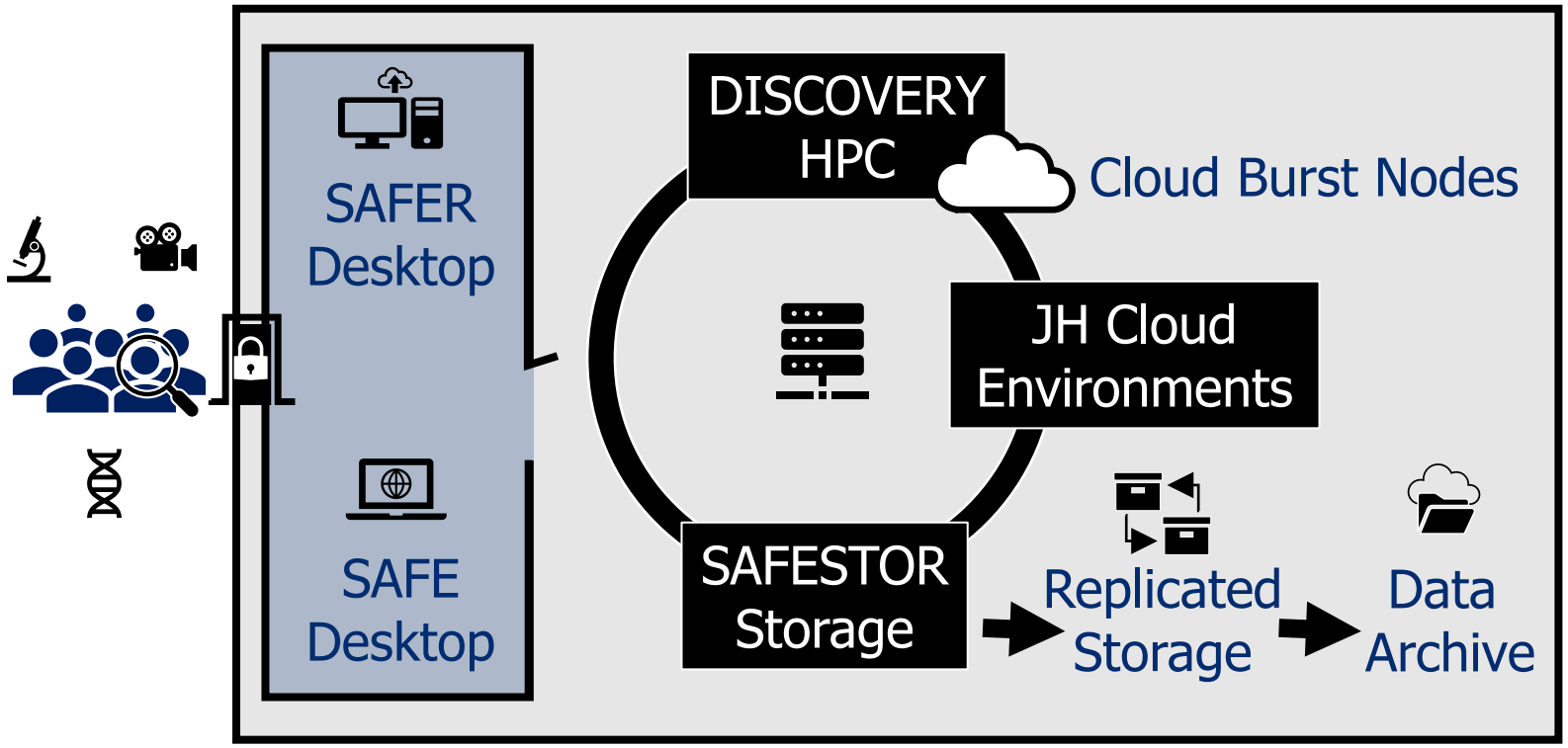
- Broad Protection of CUI
- Either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation and annual affirmation, verify compliance with the 110 security requirements in NIST SP 800-171 Revision 2.
- In-Scope: Assets that process, transmit or store CUI (+ Security Protection Assets, Risk Managed Assets, Specialized Assets)
- Assessment valid for three years from CMMC Status Date
- POA&Ms permitted for Conditional CMMC Status for 180 days

Secure & Compliant Research IT Environment

HIPAA/PHI Compliant Environment

Approved by JHM AI & Data Trust and IRB

NIST Compliant



Vital stats:

- 201 HPC nodes, including
  - 11K CPU cores
  - 120 T4 GPUs
  - 64 H100 GPUs
  - 144 H200 cloud GPUs
- 5PB SSD HPC Storage
- 6PB SAFESTOR NAS Storage
- 5PB Instrument Storage
- 50PB Large Scale Storage *(CY25)*
- Open OnDemand and CLI Access

JH Cloud Environments

- Microsoft Azure
- AWS

Considerations for Moving from CMMC Level 1 to Level 2

- Requires strategic investment of capital and resources from leadership
- Determine in-scope assets (institution-wide, enclave, CSP, project-level)
- Determine governance structure/reporting lines
- Gap analysis of SSP against NIST 800-171 controls/CMMC 2
- Communicate plans with stakeholders
- How/whether institution will seek to recover (considerable) costs

Office of Research Security & Trade Compliance

CMMC Level 2 Certification

Allen A. DiPalma, Executive Director

October 2025, COGR Membership Meeting

University of Pittsburgh Institutional Profile

- Private State Affiliated University in PA founded in 1787
- 747 Degrees and Certificate Programs offered among its 5 campuses
- Over 10,700 degrees and certificates issued in 2024
- Undergrad Students = 24,570; Grad Students = 9,509
- Full-Time Faculty = 5,333
- FY 2024 research expenditures = $1.2 billion
- Fundamental Research supported by Policy
- A formal exceptions process for restricted research is available
- CUI/CMMC: Slow Start, Strong Finish

Pitt's Journey to CMMC Level 2 Certification

- **2022:** Decision made to approve projects involving CUI. ORSTC partnered with IT Security and Sponsored Programs to formalize guidance and process which is found on Pitt's ORSTC Website.
- **2024:** Decision to pause CUI activities to pursue a **central solution** using Microsoft Azure GCC High and disallow CUI on University systems until this environment was "stood up".
- **Spring 2025:** Funds allocated to create GCC High environment. Obtained assistance through Schneider Downs and Summit 7.
- **Summer 2025:** Funds allocated to pursue CMMC Level 2 Certification on the Azure GCC High Environment.
- **Fall 2025:** Currently working with Schneider Downs, Summit 7 and Kratos leading to CMMC Level 2 Certification process initiation in December 2025.

Estimated Costs: Level 2 Cert + CUI Enclave

Vendor/Pitt Resource	Cost Description		Total Cost
Summit 7	Certification Project Implementation		
Schneider Downs	Certification Consulting Services		
	Certification CUI Enclave Consulting		
Kratos (C3PAO)	Certification - Assessment (Phase 1: Conduct the Pre-Assessment; Phase 2: Assess Conformity with Security Requirements; Phase 3: Compelete and Report Assessment Results; Phase 4: Issue Certificate)		
	Certification Plan of Action and Milestones		
Staff Time/Effort	Certification Security Staff Effort		
	Certification Office of Research Security and Trade Compliance		
Total Estimated CMMC Level 2 Certification Costs			**$320,185**
Total Estimated Cost for Creation and Maintenance of CUI Compliant (800-171) Environment			**$478,000**
Total Estimated First Year Cost for CMMC Level 2 Certification & CUI Environment			**$798,185**
Estimated 5 Year Cost for CMMC Level 2 Certification and Maintenance of CUI Environment			**$3,287,000**

Post Certification Challenges

- Explanation of variable costs to users: computing time, GCC High licenses, price for addition of software or other unique elements.
- Treatment of Costs: Direct Costs vs. Indirect Costs; Specialized Service vs. Individual Costs. Important for budgeting!
- Leadership messaging to the research community.
- Training for the community around CUI, restricted research, individual obligations around safeguarding in an open environment.
- Central office preparation and coordination: research security, export controls, sponsored programs, IT security, legal…
- Create a framework for coordinating the handling of confirmed violations.

University of Pittsburgh

Office of Research Security & Trade Compliance

Thank you.

https://www.researchsecurity.pitt.edu/

Poll Everywhere

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

COGR