November 2024

FAMU FLORIDA A&M UNIVERSITY
OFFICE OF ENTERPRISE RISK MANAGEMENT

Risk Alert

Meaningful. Actionable. Timely.

Research Security:
DoD Issued the CMMC 2.0 Final Rule Impacting DoD Research Funding at Institutions of Higher Education

The Department of Defense (DoD) on October 15, 2024 issued the final rule for the Cybersecurity Maturity Model Certification (CMMC), establishing rigorous cybersecurity requirements for all institutions involved in DoD-funded research. This rule takes effect on December 16, 2024, and mandates that any organization handling Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) must comply with specific cybersecurity standards to protect sensitive government data. Compliance is not optional; it is a prerequisite for securing or retaining DoD research funding. Failure to meet these standards could result in the loss of current grants, disqualification from future funding opportunities, and damage to our institution's reputation as a reliable research partner. Achieving and maintaining CMMC compliance is essential to FAMU's strategic goals, including our

Why This Matters to FAMU's Strategic Priorities:

Achieving and maintaining CMMC compliance is not just a regulatory requirement; it's an opportunity to strengthen FAMU's position as a leader in research excellence, secure federal funding, and enhance our reputation as a trusted partner. While non-compliance poses risks to key strategic priorities, meeting these standards can drive us forward.

- **Student Success**: Compliance ensures continued access to DoD funding, supporting research opportunities for students and enabling hands-on experience with advanced projects. This access enriches students' academic journey and positions FAMU as a hub for innovation and learning.
- **Academic Excellence**: Protecting our research and intellectual property not only safeguards academic integrity but also enhances our ability to attract top faculty and secure high-impact projects. By meeting cybersecurity standards, FAMU can position itself as a leader in secure, high-stakes research.
- **Leveraging the Brand**: Demonstrating cybersecurity resilience strengthens FAMU's brand as a reliable research partner. CMMC compliance showcases our commitment to secure research, attracting industry partnerships and increasing our visibility in high-profile research areas.
- **Fiscal Health**: Federal research funding, including DoD grants, is crucial for financial stability. CMMC compliance secures these funding streams, supporting financial resilience and growth opportunities for FAMU in research-driven initiatives.
- **Organizational Effectiveness**: Compliance with federal cybersecurity standards promotes operational efficiency, minimizing disruptions and aligning FAMU with best practices. This not only prevents compliance-related setbacks but also streamlines processes across the university.

Alert Type

Awareness | Watch | **Warning**

"Achieving excellence in research requires more than innovation—it demands vigilance. CMMC compliance is not just a regulatory requirement; it's a commitment to safeguarding our future, protecting our research, and securing the path to R1 status. The time to act is now!"
– FAMU Deputy COO & Chief Risk Officer Deidre Melton

Potential Consequences of Inaction:

- **Loss of Critical Funding:** Non-compliance with CMMC standards could lead to the immediate loss of DoD research grants, repayment of grant funds, and prevent access to future funding opportunities. This financial setback would jeopardize ongoing projects, impact our research capabilities, and threaten FAMU's financial stability.
- **Legal and Financial Penalties:** Non-compliance could result in penalties up to $10,000 per control, with a minimum of 110 controls required for evaluation. These fines, combined with the risk of disbarment from future federal contracts under the Civil Cyber Fraud Initiative, could have devastating financial and operational consequences.
- **Operational Disruptions and Setbacks:** Inadequate cybersecurity protections increase the risk of cyber incidents that could disrupt academic programs, research, and administrative operations. Such disruptions may lead to shutdowns of critical services, hindering FAMU's ability to deliver an uninterrupted experience for students and faculty.
- **Erosion of Trust Across Stakeholders:** Failure to protect research data and comply with federal standards could break the trust of students, faculty, donors, and government partners. Restoring confidence after a security lapse is costly and time-consuming, risking long-term damage to the university's reputation and mission, and making it difficult to compete for high-profile grants and partnerships essential for R1 Carnegie status.

Call to Action: Leadership, IT, Research, and Assurance Must Lead the Charge

The responsibility for safeguarding FAMU's future rests on coordinated efforts across leadership, IT, research, and assurance teams. Each group plays a critical role in ensuring we meet CMMC compliance and secure our position as a leading research institution. Strategic discussions must happen now to ensure long-term success in becoming a premier research institution and obtaining R1 status.

Senior Leadership Team must champion cybersecurity compliance, prioritize it within strategic planning, establish a compliance timeline, and allocate the necessary resources. Your role is crucial in ensuring that compliance becomes a core part of FAMU's path to R1 status and beyond.

- Are we allocating sufficient resources—financial, technological, and personnel—to support CMMC compliance efforts across the university?
- Do we have a clear understanding of our current compliance position, the risks and potential impacts of non-compliance on our research funding and reputation?
- What are our escalation and decision-making processes if CMMC compliance issues arise?
- How can we communicate the importance of CMMC compliance across the university to ensure alignment and buy-in at all levels?

IT Professionals are the frontline defenders, tasked with securing our digital infrastructure. It is essential to implement advanced security measures, maintain continuous system monitoring, and address vulnerabilities to meet CMMC standards.

- Are our current security measures (e.g., firewalls, multi-factor authentication, and data encryption) adequate to meet CMMC requirements?
- How frequently are we conducting system monitoring and vulnerability assessments to ensure continuous protection of CUI and FCI?
- Do we have incident response and disaster recovery plans specifically designed for handling CMMC-related data breaches?
- What additional training or resources do our team members need to maintain and enhance cybersecurity compliance?

Knowledge is Power: Learn More About CMMC

- ***Department of Defense – All About CMMC***
- ***The National Law Review – CMMC Level 2: The Good, The Bad, and The Ugly***
- ***Pillsbury Law – The Department of Defense Issues Final Rule Establishing CMMC 2.0***
- ***Aspire Cyber Podcast: How UCF's Knight Shield is Revolutionizing Cybersecurity Compliance***
- ***EisnerAmper - Cybersecurity for DoD Contract Information: Navigating Regulations and Risks***

Researchers and Faculty must be proactive in ensuring compliance with CMMC guidelines in all DoD-related projects. Your commitment to safeguarding CUI and FCI will be key to maintaining our competitive edge in federal research funding.

- Do we fully understand the CMMC guidelines and the specific requirements for handling CUI and FCI in our projects?
- How are we ensuring that all research data and project materials are securely stored, transmitted, and accessed?
- Are we conducting regular reviews of our research processes to ensure ongoing compliance with CMMC standards?
- What steps are we taking to protect research data, including implementing secure access protocols and handling sensitive information responsibly?
- Are we collaborating with IT and Compliance teams to stay informed of any updates or changes in cybersecurity requirements for DoD-funded research?

Office of Compliance and Ethics must lead the charge in conducting ongoing assessments and ensuring all departments adhere to cybersecurity requirements. Your role is to continuously monitor regulatory changes and guide departments through compliance.

- How frequently are we assessing each department, college, and school's adherence to CMMC requirements?
- Do we have a clear framework for tracking and monitoring regulatory changes related to CMMC, and how are we communicating those updates?
- What proactive steps are we taking to support departments, colleges, and schools that may need assistance in achieving and maintaining compliance?
- Are we documenting all compliance activities to provide evidence of our adherence to CMMC standards if audited?
- How are we working with Audit and IT to address identified risks and implement corrective actions?

Division of Audit must regularly review cybersecurity controls and processes to ensure they meet CMMC standards. Your role includes identifying gaps, recommending corrective actions, and providing management with the necessary insights to mitigate risks.

- Are we regularly reviewing cybersecurity controls and processes to ensure they align with CMMC standards?
- What gaps or weaknesses have we identified in the current cybersecurity framework?
- How often are we conducting audits specifically focused on CUI and FCI protection across departments, colleges, and schools?
- Are we providing actionable recommendations to leadership and IT to mitigate risks and strengthen compliance?
- How are we following up on audit and advisory findings to ensure that corrective actions are implemented effectively and promptly?

Final Words: A Unified Commitment to CMMC Compliance

CMMC compliance is essential for safeguarding FAMU's research, securing funding, and advancing toward R1 Carnegie status. By uniting leadership, IT, researchers, compliance, and audit teams in this effort, we position FAMU as a trusted, resilient institution ready to meet regulatory demands and embrace new opportunities.

Scan for More ERM Resources

This publication was enhanced using artificial intelligence