Cybersecurity Maturity Model Certification (CMMC)

Scenario
Charlotte Blair is the chief information security officer (CISO) at a public research university in the southeast United States. The university president, who moved into that role two years ago, has indicated his intention to expand the institution’s research budget and reach, particularly in the area of federal research grants. The university already hosts several high-profile researchers working with Department of Defense (DoD) projects, and the goals of the institutional leaders and the state legislature include broadening existing work while persuading prestigious researchers in related fields to come to the institution and establish new programs of work. This growth in the research portfolio will also raise the institution’s profile and help attract students interested in working in those fields.

For some time, Blair has been keeping an eye on evolving federal cybersecurity regulations that govern contracts, recognizing that not being able to demonstrate compliance with those regulations will disqualify the institution from applying for certain grants. At the same time, getting ahead of evolving rules and cultivating the knowledge and skills to comply with such regulations positions the institution well to compete for grants that don’t—or don’t yet—stipulate that compliance.

In particular, NIST Special Publication 800-171 articulates security standards related to Controlled Unclassified Information (CUI). A growing number of DoD contracts require compliance with 800-171, and these grants cover many of the areas of planned research growth at the institution. The Cybersecurity Maturity Model Certification (CMMC) program addresses compliance with 800-171, and Blair charges her staff with pursuing that certification. The work needed to achieve the certification can also be applied to other institutional areas, even those that aren’t subject to compliance requirements, such as institutional research that uses sensitive data, medical research that uses protected health information, and other projects that depend on sensitive data. In these ways, the university is preparing to be ready if and when areas such as financial aid needs to comply with those requirements in the future.

1 What is it?

The Cybersecurity Maturity Model Certification (CMMC) is a set of policies and practices that address the protection of federal Controlled Unclassified Information (CUI) data through administrative, physical, and technical controls. According to the U.S. Department of Defense (DoD), the loss of CUI from the Defense Industrial Base (DIB) has led to increased risk to the economy and to national security. To reduce this risk, DoD has worked with the DIB sector to enhance the protection of CUI in unclassified networks. The program incorporates a set of cybersecurity requirements into acquisition programs and provides DoD increased assurance that contractors and subcontractors are meeting these requirements. CMMC is critical to organizations that support or feed into the DIB, and this applies to colleges and universities that are performing DoD contracts.

2 How does it work?

CMMC 2.0 consists of three maturity levels. Level 1 is meant to protect Federal Contract Information (FCI). Levels 2 and 3 cover advanced policies and practices focused on improving institutional security maturity and reducing risk from advanced persistent threats. Partners and suppliers to the DIB will have their cybersecurity posture compared to CMMC criteria to determine how well prepared they are to handle cybersecurity threats and also how well cybersecurity is integrated into their organizational culture. Only some Level 2 and all Level 3 assessments require third-party certification. The outcome of this audit could be a neutral-party verification of cybersecurity readiness. Institutions whose research portfolio will be impacted by CMMC requirements should begin the process of identifying gaps. An important first step is to determine the scope of CMMC compliance. The grants and contracts office should have information on all active DoD contracts. If the research office does not have this information compiled, now is the time to do so. “CMMC Basics—The Full Details” outlines steps for compliance, which includes understanding requirements, developing a plan, documenting practices, testing and validating results, and periodically reevaluating progress.

3 Who’s doing it?

CMMC can be applied to all higher education, not just research-focused institutions. Digital and/or paper spaces where CDI/CUI and/or FCI are located at institutions conducting DoD-sponsored research—either as primes or subcontractors—must obtain CMMC certification at the level appropriate to the work.
Cybersecurity Maturity Model Certification (CMMC)

Some research institutions intend to pursue CMMC Level 1 certification for their entire institution, though entire institutions do not need to be CMMC certified. Other federal or state agencies may embrace CMMC, potentially even the Department of Education.

**Why is it significant?**

As articulated in “Higher Education Regulated Research Workshop Series: A Collective Perspective,” cybersecurity compliance for regulated research covers several common elements. The first is clear ownership and support, with defined roles and responsibilities. Organizations are encouraged to leverage a tool like a RACI (responsible, accountable, consulted, informed) matrix to show how all stakeholders are involved. CMMC also requires a long-term investment to deliver compliant environment(s) that meet the evolving needs of the academic, administrative, and research missions of the institution. Periodic training and outreach communications are key to ensuring that stakeholders are aware of the requirements and their impacts. This training must include the IT professionals who support these environments. When developing a strategy and plan of action, audit controls must be included that will show evidence of the implementation of the controls. For the DoD, some types of environments may need to be audited by a third party every three years. Another significant consideration is how guidance for implementing National Security Presidential Memorandum 33 (NSPM-33) may impact fundamental research missions. In particular, the section “Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement” includes 14 basic cybersecurity controls—which are similar to CMMC 2.0 Level 1 controls—that colleges and universities should consider as a baseline.

**What are the downsides?**

The costs of CMMC compliance are a concern. As institutional leaders consider how to address cybersecurity deficiencies, cybersecurity will continue to be an allowable facilities cost under CMMC. This recognizes the critical nature of cybersecurity and supports CMMC compliance. Institutions can begin to build budgets to upgrade cybersecurity to the levels needed. Compliance can have an impact on IT support, forcing units to spend time on regulated data environments at the cost of supporting broader institutional needs. Ongoing training is necessary to keep stakeholders up-to-date on the evolving threat and risk landscape. In addition, requirements are not easy to implement and can have an impact on how researchers work with data. Finally, not implementing carries its own risks, such as not qualifying for new awards or the potential loss of current projects. Reputational damage could be far reaching, even beyond research, and is difficult to quantify.

**Where is it going?**

In September 2020, the DoD published an interim rule that implemented the DoD’s vision (CMMC 1.0) and outlined the basic features of the framework (tiered model, required assessments, and implementation through contracts). In November 2021, following a review of CMMC’s implementation, DoD announced CMMC 2.0, which introduced several key changes, including a streamlined model, reliable assessments, and flexible implementation. The changes reflected in CMMC 2.0 will be implemented through the government rulemaking process, which will include a public comment period. Stakeholder input is critical to meeting the objectives of the CMMC program, and the DoD will actively seek opportunities to engage stakeholders as it drives toward full implementation. Affected research programs will be required to comply once the forthcoming rules go into effect. Now is the time for institutions to assess whether their information security functions are resourced to support the broad imposition of security controls across the research mission. Research facilitators, research affairs staff, high-performance computing staff, and divisional staff should play a role in supporting cybersecurity, especially for security processes and controls. Institutions will need to significantly increase investments in cybersecurity and support for researchers over the next few years, and harnessing investments that are already in place is the best way to start.

**What are the implications for higher education?**

Maturity models such as CMMC are a powerful tool for evaluating and measuring programs. With CMMC being required today for DoD/CUI research, many organizations have either started or are looking to begin their journey of compliance. Other federal or state data sponsors in research might also embrace CMMC and NIST 800-171 as a security framework. The Department of Education has strongly suggested that it is considering using NIST 800-171—which provides “recommended security requirements for protecting the confidentiality of CUI when the information is resident in non-federal systems and organizations”—to protect financial aid and other portions of the student record. Institutions should evaluate their security programs and leverage CMMC Level 1 or NSPM-33 as a guide to basic cybersecurity controls that could be implemented institution-wide. Colleges and universities need to establish ownership and roles with vertical and horizontal communications across the organization and their partners. The path to compliance will involve both one-time and ongoing financial costs. These compliance and security frameworks are a long-term investment that will build trust with data sponsors and customers and provide the capability for expansion. Meeting these standards will be fundamental to the success of the higher education community in meeting its mission for the future.