Issue Brief

New US Federal Compliance Rules for Sensitive Information

May 2021

By Cynthia Hudson-Vitale and Katherine Klosek

With thanks to Jarret Cummings, Senior Advisor, Policy & Government Relations, EDUCAUSE, and Clifford Lynch, Executive Director, Coalition for Networked Information

ASSOCIATION OF RESEARCH LIBRARIES

Introduction

A great deal of sensitive and valuable information is created, managed, and stored by researchers at universities in the United States. More and more of this information is digital, which means that effective cybersecurity practices have grown in importance and visibility. For data and information produced as part of a US federally funded research activity, the safeguarding of controlled, classified, and controlled unclassified information (CUI)[1] is subject to specific federal rules and regulations. Both the rules and regulations themselves, as well as the choices that federal funders are making about their applicability, have changed substantially in recent years. However, these issues are not new. Institutions will already be familiar with government regulations governing work that falls under International Traffic in Arms Regulations (ITAR), classified research at various levels, and Health Insurance Portability and Accountability Act (HIPAA) controls relating to biomedical patient data, though some institutions have chosen not to host research that is subject to some of these controls. Effective cybersecurity also plays a vital role in institutional compliance with federal and state privacy requirements, as well as broader best practices.

Recently, a number of US federal agencies (particularly the Department of Defense [DoD]) have been moving towards requiring cybersecurity certifications or assessments with potentially significant implications for the higher education research enterprise. To address these issues, higher education associations are working with the DoD to clarify that fundamental research—basic and applied, distinct from proprietary research—is not subject to the DoD's new Cybersecurity Maturity Model Certification (CMMC) requirements. Similar conversations with other federal funders may be needed in the future.

1 The Controlled Unclassified Information (CUI) program, administered by the National Archives and Records Administration, standardizes the way the US executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

These developments are occurring alongside—and to some extent in tension with—a growing push within institutions and by funders to make funded research data publicly available; this trend is further fueled by the growing move by researchers to embrace open scholarship practices.

For Association of Research Libraries (ARL) member libraries that provide support for and collaborate with researchers on open research and open science initiatives, cybersecurity requirements need special attention. Campus-based research offices, sponsored projects, information security offices, and research computing colleagues may be especially attuned to these requirements.

This issue brief includes information on current rules and activity in information policy and related cybersecurity practices in US research institutions and federal agencies. This brief should be especially useful for ARL member representatives participating in campus conversations about research support.

The cybersecurity certification and assessment guidelines are part of a trend in which the US federal government increasingly views protecting US research data from foreign government influence as a national security strategy. For a broader look at the "science nationalism" issue, see the Coalition for Networked Information (CNI) Executive Roundtable report, *International Tensions and "Science Nationalism" in a Networked World: Strategies and Implications*.

The Issues

Federal Cybersecurity Policies

In higher education, cybersecurity is on the agenda of EDUCAUSE, the Council on Governmental Relations (COGR), Association of American Universities (AAU), Association of Public and Land-grant Universities (APLU), and American Council on Education (ACE). CNI

is also tracking these issues. Together these organizations are seeking clarification on the implications of new federal cybersecurity policies for higher education research, particularly policies from the DoD. In 2020, half of DoD's basic research budget was spent at universities that either contract directly with the department or indirectly as subcontractors. DoD's Cybersecurity Maturity Model Certification (CMMC) framework was initially implemented through an interim federal rule that took effect at the end of November 2020; the rule also requires compliance with US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 requirements (see the appendix of this issue brief for details). DoD is phasing in compliance with the rule over the next five years, with plans for 2021 focusing on piloting the certification requirements with a limited number of DoD contracts. This five-year phase-in is intended to allow time for the independent CMMC Accreditation Body to accredit enough CMMC third-party assessor organizations (C3PAOs) to provide certification assessments across defense industrial base (DIB) organizations.

In comments on the DoD Assessment Methodology and Cybersecurity Maturity Model Certification Framework rule (note the correction to the regulation identifier number), higher education stakeholders asked DoD to clarify that fundamental research is excluded from the new requirements because fundamental research activities do not include the categories of information that the rule is meant to protect, and the requirements could lead to unnecessary burden and expense for academic institutions. The higher education stakeholders noted that other agencies that fund university research or protect sensitive data are also monitoring the CMMC framework for potential application to their contracts and agreements, making the request for DoD to clarify the status of fundamental research in relation to CMMC even more important.

COGR recently surveyed its members about the difficulty of obtaining fundamental research determinations for DoD-funded projects. The

survey revealed that the lack of clarity on the presence or absence of CUI is one barrier to the negotiation of fundamental research determinations.

The interim rule did not resolve these issues, and higher education groups are waiting to see if they will be addressed in the final rule, which is expected to be released in May 2021. ARL will continue to monitor the release of the final rule with colleagues at EDUCAUSE, AAU, COGR, ACE, and APLU.

Cybersecurity and Open Research/Open Science

Discussions and infrastructure around cybersecurity may also intersect with campus conversations related to open research, open science, and data management and sharing. Leading scientific societies and members of Congress recognize that openness is crucial to fundamental research. As many ARL libraries and their deans and directors are investing in and leading collaborations to support the public sharing of research outputs, clarifications around the exclusions of these federal policies is critical for supporting faculty research.

The DoD was included in the 2013 Office of Science and Technology Policy (OSTP) memorandum on "Increasing Access to the Results of Federally Funded Scientific Research." The most recent DoD public access policy, released in 2018, outlines a two-step process for compliance: (1) requiring a data management plan at the start of a research project deliverable to the Defense Technical Information Center, and (2) the sharing of data sets supporting published research results at the time of article publication.

The DoD policy is very clear that researchers whose data have national security concerns or controlled unclassified information concerns are not subject to the data sharing requirement. Within the data management plan any research project that has these outputs should

indicate that data will not be made available to the public.

Considerations:

- Senior library administrators should be aware that research-related security conversations are happening between university administration and campus IT. Higher education associations are seeking clarifications around exclusions for academic campuses.

- Library staff who provide training in data management should work closely with campus IT and research computing to articulate research data security storage and sharing options for faculty.

- Library staff who review data management plans should clarify with researchers that no national security research data or controlled unclassified information should be shared at the time of article or data publication.

Appendix

DoD Assessment Methodology and Cybersecurity Maturity Model Certification Framework

In fall 2020 the US Department of Defense (DoD) released an interim rule on Assessing Contractor Implementation of Cybersecurity Requirements that incorporates the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology and DoD Cybersecurity Maturity Model Certification (CMMC) framework into its contracting regulations. Under the interim rule, defense contractors subject to NIST SP 800-171 requirements are expected to submit the results of self-assessments in relatively short order, while CMMC requirements are expected to be added to an increasing number of defense contracts, and ultimately encompass all defense contracts, over the next five years. As noted above, higher education research and information technology groups are seeking clarification that neither the self-assessment mandate nor the CMMC requirements apply to fundamental research, but those remain open questions for now.

In brief, both the NIST SP 800-171 self-assessment and CMMC evaluate the applicability to federal contracts of NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, although in different ways and timeframes, and with different levels of external verification.

NIST SP 800-171 DoD Assessment Methodology

This assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800-171 security requirements not yet implemented by a contractor, and three assessment levels (basic, medium, and high), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment.

- A basic assessment is a self-assessment completed by the contractor.
- Medium or high assessments are completed by the government.

The assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The DoD contract clause requiring NIST SP 800-171 compliance self-cancels when a contracted project receives a fundamental research designation. Therefore, the NIST SP 800-171 CUI guidelines do not apply to fundamental research. On that basis, it should be clear that the NIST SP 800-171 self-assessment mandate in the interim rule (and the subsequent possibility of DoD-conducted "medium" and "high" assessments) similarly does not apply to fundamental research projects. Higher education groups remain hopeful that DoD will fully address this issue in the final version of the rule to eliminate any possibility of confusion.

Cybersecurity Maturity Model Certification (CMMC)

Building upon the NIST SP 800-171 DoD Assessment Methodology, the Cybersecurity Maturity Model Certification framework adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level.

CMMC is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect sensitive unclassified information such as federal contract information (FCI) and controlled unclassified information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

Level	Description
1	Consists of the 15 basic safeguarding requirements from Federal Acquisition Regulations clause 52.204-21
2	Consists of 65 security requirements from NIST SP 800-171 implemented via Defense Federal Acquisition Regulation Supplement clause 252.204-7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3
3	Consists of all 110 security requirements from NIST SP 800-171, 20 CMMC practices, and 3 CMMC processes
4	Consists of all 110 security requirements from NIST SP 800-171, 46 CMMC practices, and 4 CMMC processes
5	Consists of all 110 security requirements from NIST SP 800-171, 61 CMMC practices, and 5 CMMC processes

ASSOCIATION OF RESEARCH LIBRARIES

Association of Research Libraries
21 Dupont Circle, NW
Suite 800
Washington, DC 20036
T 202.296.2296
F 202.872.0884

ARL.org
pubs@arl.org