



February 2, 2024

Regulatory Secretariat Division
Office of Governmentwide Acquisition Policy
General Services Administration
1800 F Street NW
Washington, DC 20405

RE: Comments in response to FAR Case 2021-017, “Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing,” submitted electronically at <https://www.regulations.gov/commenton/FAR-2021-0017-0001>

To Whom It May Concern:

On behalf of EDUCAUSE, COGR, and the Association of American Universities (AAU), we would like to thank you for the opportunity to provide input from the higher education community on [Federal Acquisition Regulation \(FAR\) Case 2021-017](#), which discusses the proposed rule to govern cyber incident reporting and information sharing for federal contractors. Our organizations are described as follows:

- As the association for advancing higher education through information technology (IT), EDUCAUSE represents nearly 2,200 colleges, universities, and related organizations. Higher education IT leaders and professionals at all levels work together through EDUCAUSE to develop and strengthen the role of technology in helping colleges and universities to achieve their missions.
- COGR is an association of over 200 public and private United States research universities and affiliated academic medical centers and research institutes. It focuses on the impact of federal regulations, policies, and practices on the performance of research conducted at member institutions and advocates for sound, efficient and effective regulations that safeguard research and minimize administrative and cost burdens.
- AAU is an association of 69 U.S. and two Canadian leading research universities that transform lives through education, research, and innovation. AAU member universities collectively help shape policy for higher education, science, and innovation; promote best practices in undergraduate and graduate education; and strengthen the contributions of leading research universities to American society.

The notice of proposed rulemaking (NPRM) identifies the goal of the FAR revisions to be “increas[ing] the sharing of information about cyber threats and incident information between the Government and **information technology and operational technology service providers**”

(emphasis added) consistent with Executive Order (E.O.) 14028.¹ The NPRM notes that this goal derives from the executive order’s intention to foster “increased protection of Government networks.”² However, the NPRM appears to propose applying cybersecurity incident reporting mandates to *all* federal contractors that may use information and communications technology (ICT) in the performance of their contracts, regardless of whether those contracts pertain to the provision of information technology or operational technology goods and services to federal agencies:

The proposed rule would require the new incident reporting clause to be included in all contracts involving ICT that are subject to the FAR,

This rule proposes to add a new clause at FAR 52.239–ZZ, Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing Information and Communications Technology. The clause is prescribed at FAR 39.108(b) for use in all contracts and solicitations....

This proposed rule will impact all contractors awarded contracts where ICT is used or provided in the performance of the contract. The Government does not have a way to track awards that may include ICT in support of the product or service being offered to the Government, so DoD, GSA, and NASA assume that 75 percent of all entities are awarded contracts that include some ICT. Of the 75 percent of entities awarded contracts with some ICT, it is assumed that 4 percent of those entities may have a reportable cyber incident.³

Given that the proposed FAR changes are intended to improve cybersecurity information sharing “between the Government and information technology and operational technology service providers,” **the inclusion of a cyber incident reporting requirement in all federal contracts does not appear justified.** It is extremely hard to imagine any contractor not using ICT to some extent, especially based on how broadly it is defined⁴ in the proposed rule, “in the performance of the contract.” In the case of colleges and universities, it is a virtual certainty that ICT would be involved in the performance of a federal contract, even if the use in question is for basic administrative purposes.

When we take into account that a large volume of federal contracts with higher education institutions are for fundamental research projects, however, the relevance of imposing cyber incident reporting responsibilities on all of them becomes even harder to understand. By and large, possible cyber incidents in such projects pose little if any cybersecurity risk to the agencies for which the research is being conducted; they generally do not entail direct access to federal computer networks or information systems or the transfer of data or technology in formats that would lend themselves to efforts to compromise federal networks or systems. And

¹ Department of Defense, General Services Administration, and National Aeronautics and Space Administration, “[Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing](#),” *Federal Register*, Vol. 88, No. 190, October 3, 2023, p. 68055.

² *Ibid.*

³ *Ibid.*, p. 68058.

⁴ *Ibid.*, p. 68066.

yet, given the definition of “security incident” on which the proposed rule relies, a minor problem on a graduate research assistant’s device, such as installing an innocuous but unauthorized browser extension, could require filing a federal cyber incident report:

Security incident means actual or potential occurrence of the following—

- (1) Any event or series of events, which pose(s) actual or imminent jeopardy, without lawful authority, to the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;
- (2) Any malicious computer software discovered on an information system; or
- (3) Transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.⁵

Minor infractions of institutional “security policies, security procedures, or acceptable use policies” of the type described are not unusual in academic environments, where student learning and experimentation is very much part of the norm, and they are certainly something that colleges and universities consistently work to curtail through awareness-raising, education, and training. Applying federal cyber incident reporting requirements to them as well, however, would add administrative burdens while making no meaningful difference to federal cybersecurity.

If we are being overly broad in our interpretation of what “all contracts involving ICT” and “where ICT is used or provided in the performance of the contract” mean in this context, then further clarification that the proposed requirements will be incorporated in all contracts or solicitations for information technology and/or operational technology products and services should resolve the issue and prevent further misinterpretation by institutions and federal contract management staff alike. Similarly, if the government is concerned about possible instances in which a higher education institution’s work under a contract might entail substantive exposure to cybersecurity risk for a federal network or system, however limited such instances might be, then it could identify the level of engagement with federal networks or systems that would generate a relevant degree of risk and apply the proposed reporting requirements to relevant contracts.

If the proposed FAR revisions truly are intended to apply cyber incident reporting requirements to all federal contracts that might entail the use of any ICT, however far removed such use might be from actual cybersecurity risk to the federal government, then the government should recognize that it will be starting down a slippery slope to a significant “signal versus noise” problem in relation to cyber incident reporting. As noted above, the

⁵ Ibid.

proposed ICT and security incident definitions are very broad. In the case of colleges and universities, and particularly in the research context, they will often have to be interpreted in their application by frontline faculty, staff, and research assistants. Given the potential impact that compliance failures might have on the continuation and payment of a contract—as the proposed rule notes, contractor compliance will be “material to eligibility and payment under Government contracts”⁶—faculty and staff will be inclined to report anything that might conceivably fall under the proposed requirements, “just in case.”

The practical realities of how faculty and staff will likely experience the proposed FAR reporting mandates “on the ground” make the government’s assumption that 4% of covered contractors will experience a reportable incident seem like a gross underestimation. Or put another way, the government may assume that 4% of affected contractors will experience a reportable incident, but it faces a significant probability that covered contractors will report at a substantially higher rate to ensure that they avoid a compliance failure. As a result, the overall value of reporting under the proposed FAR changes will be compromised as the burden of separating truly relevant reports from overreports grows exponentially.

The proposed software bill of materials (SBOM) requirements are equally concerning. Per the NPRM, “This rule proposes a new requirement for contractors to develop and maintain a software bill of materials (SBOM) for any software used in the performance of the contract regardless of whether there is any security incident.”⁷ In the context of software provided to federal agencies or used directly to support agency operations or objectives, this requirement may make sense. Such software has a direct bearing on the level of cybersecurity risk to which agencies might be exposed. However, in the context of federal contracts for fundamental research, for example, the requirement presents daunting challenges for institutional tracking and management of software that in many, if not most, cases open the sponsoring agency to no cybersecurity risk.

Fundamental research is likely to entail the use of highly specialized software that is specific to the academic discipline in question, may have been developed many years ago locally for distinct research needs, and to which the sponsoring agency is unlikely to have any exposure. **Asking researchers, their students and assistants, and their institutions to develop and maintain SBOMs for such packages will continuously siphon time and resources away from the research for which the agency has contracted without actually improving federal agency cybersecurity.** This also assumes that the vendors of such highly specialized software will be willing and able to fulfill the proposed requirements in a timely fashion, which may not be the case. Without a clear connection to the cybersecurity risks that federal agencies actually face, the sacrifice of time and resources from the research that the federal government is seeking to compile SBOMs for software of minimal risk to the government seems very hard to justify.

⁶ Ibid, p. 68055.

⁷ Ibid, p. 68056.

In the case of more standard software packages for administrative or data management/transfer purposes, unless and until the vendors in question develop and maintain SBOMs for their products, colleges and universities will have to confine themselves to using only software from vendors with publicly available SBOMs for federally contracted research. Depending on the software environment of the institution, this could require the purchase of otherwise standard software distinct from that procured for the institution as a whole, imposing additional costs and burdens on the research projects in question.

Finally, in instances where software may be developed for a research project, which could easily occur given the unique research needs of a given project in a given field, the requirement to provide an SBOM “upon the initial use of such software in the performance of [the] contract” and to provide a revised SBOM to the agency whenever the software “is updated with a new build or major release”⁸ could create an undue burden on the researcher or research team. Considerable trial-and-error could be involved in the development of specialized software for particular research purposes, and what constitutes “initial use” and a “new build or major release” in such circumstances, which are distinct from the normal commercial software development process, may be subject to a wide range of interpretation. Ensuring compliance with a provision written for a commercial software context in a non-commercial, fundamental research context has the potential to further draw resources away from the research that the government sought without any substantive advance in the government’s cybersecurity posture.

In terms of the timeline for incident reporting presented in the proposed rule, the requirements to report within eight hours of an incident’s discovery and provide updates every 72 hours thereafter until remediation activities have been completed may make sense in the context of vendors supplying IT systems, software, and services to federal agencies. It is reasonable to assume that such products and services may be integral to agency operations, such that incidents involving them could have immediate, national effects requiring agency as well as vendor response. In the context of fundamental research contracts, however, **the mandated reporting deadlines would be unnecessary and detrimental to the research for which the government has contracted.**

Again, in the vast majority of cases of which we can conceive, the cybersecurity risks to the contracting agencies from a potential incident in the fundamental research context would be vanishingly small. At the same time, most researchers and their teams would not have the type of operational coverage, much less cybersecurity coverage, to identify, assess, and report on an incident in eight hours or less, much less to produce updates every 72 hours until full remediation. Even if the college or university in question has a “24/7” security operations center (SOC), which is by no means a given, the lag between a faculty member or research assistant discovering an incident and then registering it with the SOC could easily exceed the required reporting window depending on the time, day, and/or date when the incident is discovered. Moreover, many institutions themselves rely on contract services for cyber incident

⁸ Ibid, pp. 68066-67.

response, and the proposed reporting deadlines would likely increase the cost to the institution of such services considerably, further draining funding away from actual research activities.

At the same time, the proposed requirement assumes a clear, shared understanding of what constitutes “discovery that a security incident may have occurred”⁹ under the rule. Markers for making that determination are not provided in the proposed rule, which in many cases will leave the matter to the judgment of the frontline research staff. This brings the rule back around to the “signal-to-noise” quagmire we discussed previously. Given the consequences that a lack of compliance introduces and the uncertainty about what is sufficient to indicate that a relevant incident “may have occurred”—and in the fundamental research context, why it would be of interest to the contracting agency—most researchers, research staff, and/or research institutions will likely default to reporting anything that could conceivably cross the “may have occurred” threshold, making it that much harder for actual incidents that pose a real risk to federal agencies to rise to the surface. Imposing a blanket requirement arising from one contracting context—ICT software, systems, and services procured by and for federal agencies—to **all** contracting contexts can easily be self-defeating if universal alignment between all contracting contexts does not exist—and as the fundamental research arena illustrates, it does not.

The government itself indicates a degree of uncertainty and confusion about how to make the necessary determination that would lead to reporting in the NPRM’s discussion of the “[d]efinition of incident”:

What, if any, additional implementation issues would your entity face complying with different definitions of an incident? How would your entity make the distinction between “imminent jeopardy” and “actual jeopardy,” and what effect could that have on the number of reported incidents that did not end up actually affecting confidentiality, integrity, and availability of information or an information system?¹⁰

The salient issue is not how a research team or institution would determine what constitutes “imminent jeopardy.” What will matter to them is what the contracting agency, the Cybersecurity and Infrastructure Security Agency (CISA), and/or the relevant law enforcement agency view as constituting “imminent jeopardy.” Ideally, the NPRM would have included an analysis reflecting the issuing agencies’ collective thinking on the matter, which respondents would then have the opportunity to address via their comments.

In the absence of such an analysis, **EDUCAUSE, COGR, and AAU urge the agencies to release a supplemental rulemaking notice** that:

- Provides a proposed definition of “imminent jeopardy” for public comment, and

⁹ Ibid, p. 68066.

¹⁰ Ibid, p. 68058.

- Clarifies the rationale for the apparent application of requirements appropriate for vendors of ICT goods and services to the government to all federal contractors that might use any ICT in performing their contracts, regardless of the actual cybersecurity risks involved.

Other issues of concern include:

- The extent of incident data preservation,
- Agency access to systems and personnel (especially in academic research contexts where student participation and the use of personal devices would be normal and acceptable), and
- Customization tracking that affected contractors may have to do under the proposed rule.

These requirements could be highly burdensome and intrusive, especially in relation to activities that pose little if any risk to federal agency cybersecurity.

Likewise, the requirement that malicious code samples be provided to CISA within eight hours of discovery largely carries with it the problems identified in relation to cyber incident reporting. In addition, though, the provision as currently written does not appropriately scope the submission requirement to software and systems directly involved in contract performance. This could lead to further “signal-to-noise” problems as researchers and institutions conclude that overreporting in the face of requirements subject to a significant degree of interpretation is the only safe path.

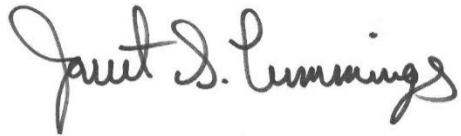
In conclusion, the NPRM presents proposed FAR changes that may be appropriate to their original context—providers of ICT products and services to federal agencies. However, the apparent decision to incorporate the cyber incident reporting provisions identified in the NPRM to **all** federal contracts forces the application of the provisions to areas of federal contracting, such as fundamental research, for which they are inappropriate and counter-productive. The same holds for the proposed SBOM requirements, where the proposed provisions do not account for the unique and unnecessarily burdensome impacts they would have on academic research environments.

EDUCAUSE, COGR, and AAU recommend that the proposing agencies pause and issue a supplemental rulemaking notice to clarify key elements of the proposed regulations so effective public comment can truly take place. In addition to the points for a supplemental notice previously mentioned, the agencies might also take the opportunity to explore how the provisions proposed in the NPRM could be shaped and applied on a risk management basis. Our associations are confident that incorporating a risk management approach into the rule would eliminate its application to fundamental research contracts in general. Such a development would best serve the needs and interests of the federal government as well as of the colleges, universities, and researchers that are trying to help federal agencies fulfill their missions.

As presently written, however, the proposed requirements would have a direct, adverse impact on federally funded research at higher education institutions. The cost of such research to the

federal government would likely increase significantly as a result without the agencies in question seeing any appreciable improvement in their cybersecurity posture.

Sincerely,

A handwritten signature in black ink that reads "Jarret S. Cummings". The signature is written in a cursive style with a large initial "J".

Jarret S. Cummings
Senior Advisor
Policy and Government Relations
EDUCAUSE

A handwritten signature in blue ink that reads "Robert Hardy". The signature is written in a cursive style with a large initial "R".

Robert Hardy
Director
Research Security and Intellectual Property
COGR

A handwritten signature in black ink that reads "Tobin L. Smith". The signature is written in a cursive style with a large initial "T".

Tobin L. Smith
Senior Vice President
Government Relations and Public Policy
Association of American Universities