

June 5, 2023

Stacy Murphy
Deputy Chief Operations Officer/Security Officer
Office of Science and Technology Policy
Executive Office of the President
1650 Pennsylvania Ave., NW
Washington, DC 20504
researchsecurity@ostp.eop.gov

RE: Comment on Research Security Programs

Dear Ms. Murphy:

EDUCAUSE (educause.edu) thanks the Office of Science and Technology Policy (OSTP) for the opportunity to comment on the draft [Research Security Programs Standard Requirement](#) (i.e., the Standard Requirement). As a nonprofit association that advances higher education through information technology (IT), EDUCAUSE represents over 2,100 colleges, universities, and related organizations. IT and cybersecurity leaders and professionals from across higher education collaborate as part of our community to advance research cybersecurity. The following feedback on the cybersecurity protocols of the Standard Requirement reflects their knowledge and expertise.

Key Themes

EDUCAUSE member representatives believe that the Standard Requirement protocols for cybersecurity do not adequately support two of the three priorities for the guidance. They do not consider the protocols to be the most effective and appropriate ways to protect research cybersecurity, nor do they think that the protocols provide the clarity necessary to facilitate “easy, straightforward, and minimally burdensome compliance.”

Higher education cybersecurity leaders and professionals continue to stress that risk management approaches to research cybersecurity offer better options for reaching the cybersecurity goals that institutions and federal agencies share. Checklist approaches like the Standard Requirement protocols mandate that all covered institutions apply the same measures to all research activities regardless of need or fit. Thus, they deprive institutions of the ability to assess the cybersecurity needs of different types of research and allocate limited resources in ways that address the associated risks.

The proposed cybersecurity protocols largely replicate the requirements in “[Basic Safeguarding of Covered Contractor Information Systems](#),” which is intended to cover Federal Contract Information (FCI). The FCI safeguards may seem basic, but they require interpretation in practice and may not fit research environments appropriately. As a result, researchers and institutions could face prohibitive compliance costs in relation to given

research grants where the cybersecurity needs of those projects would not otherwise produce such costs.

OSTP may be able to mitigate this problem through guidance that acknowledges the necessity of institutional discretion in interpreting what the protocols mean in a given research context. That would allow institutions, as part of their research security programs, to document how they apply the protocols to different categories of research or related activities. The Standard Requirement could (and should) also allow for institutions to identify and document the use of alternative approaches that are equally or more effective in achieving appropriate cybersecurity outcomes while better accommodating research and institutional needs. If an agency developed concerns about an institution's approach, then the agency and institution could negotiate changes starting from documented baselines in the institution's research security program.

As discussed below, the meaning and application of the FCI safeguards are not nearly as straightforward when transferred from the FCI context to research environments. This reinforces our call for the Standard Requirement to explicitly endorse institutional discretion in the interpretation and application of the protocols. Ideally, though, OSTP would replace the proposed protocols with a requirement that institutions develop research cybersecurity plans based on appropriately delineated risk assessment and risk management approaches.ⁱ OSTP could (and should) work with the research cybersecurity community to define the parameters for such plans and develop resources highlighting effective practices. Guidance provided for this requirement could identify core *objectives* for research cybersecurity without tying institutions to specific measures in all cases regardless of need, fit, or continued relevance. This approach would foster near-term research cybersecurity progress while supporting long-term continuous improvement through efforts such as the [Regulated Research Community of Practice \(RRCoP\)](#) funded by the National Science Foundation (NSF).ⁱⁱ

Response Topics

The Standard Requirement information request identifies five topics on which OSTP seeks input. EDUCAUSE has organized its comments accordingly.

Clarity (Are the protocols clear and do they allow for straightforward adoption?)

- Overarching points
 - The protocols do not set clear markers or metrics for compliance. If institutions must establish implementing requirements and compliance metrics for the protocols via institutional policy, the Standard Requirement should make that understanding explicit.
 - Preventing ransomware is cited as a key rationale for the protocols, but the requirements focus on the confidentiality of data; this disconnect reinforces the value of having OSTP set research cybersecurity objectives and institutions identify effective solutions.
- OSTP should explain the rationale for the reference to OMB M-21-31 in **Protocol 1** since M-21-31 relates to activity logging and not access authorization.

- If the reference indicates an expectation that institutions adopt the M-21-31 logging requirements, OSTP should reconsider including it in Protocol 1.
- Neither M-21-31 nor the protocol specify the scope of systems that M-21-31 requirements would cover, which is necessary for compliance/cost management.
- Many institutions outsource relevant services; wholesale implementation of M-21-31 requirements would dramatically increase the costs of such services.
- **Protocol 1** lacks key compliance information (e.g., a definition of “processes acting on behalf of authorized users” and specifics on where authority to authorize users should reside) in the absence of direct references to a relevant compliance guide, such as [NIST SP 800-171A](#).
- **Protocol 2** also lacks key compliance information (e.g., the basis for determining the transactions/functions that authorized users are permitted to execute).
- Given the centrality of academic freedom to academic research, **Protocol 4** requires a much more detailed explanation of the extent of control required for compliance.
- **Protocol 7** should indicate what constitutes a key internal information system boundary; given the prevalence of inter-institutional research, nuanced guidance on determining external boundaries should also be provided.
- The training section states that an institution must conduct tailored training if a “research security breach” occurs, but the term is not defined or scoped.
 - Definitions of “security incident” and “research security incident” are provided, but not referenced in the relevant paragraph. If OSTP intended for the paragraph to refer to those terms, it should revise the text accordingly.
 - Aspects of “security incident” approximate elements of a “breach” definition; in cybersecurity, however, “incident” and “breach” have distinct meanings, and the lack of a “breach” definition will create confusion in this context.

Feasibility (What aspects of the protocols raise implementation concerns?)

- **Protocol 3** may create cost and operational problems since it could be read as barring the use of personal devices, including by students, on federal projects.
 - Many institutions would face significant resource challenges if they had to issue an institutionally controlled device to anyone working on a federal project.
 - Managing such challenges would likely require institutions to raise the floor on the size of the grants they could support, constraining opportunities for researchers and the availability of research to agencies.
- **Protocol 3** may discourage inter-institutional collaboration and the use of third-party/cloud services that are central to the research enterprise; OSTP should confirm that standard industry practices for securing such activities and services will suffice for compliance.

- **Protocol 6** does not account for the fact that specialized research equipment/resources may not accommodate authentication, reinforcing the need to allow institutions to deploy equally or more effective alternative measures with appropriate documentation.
- **Protocol 8** lacks scope, raising the concern that any project with a publicly accessible component may require its own subnet; this may be infeasible for both cost and network architecture reasons, reinforcing the need for institutional discretion regarding the use of appropriate alternative measures.

Compliance (If institutions have to self-certify on compliance within a year of the final Standard Requirement being published, what concerns does that raise?)

- Please see the “Clarity” and “Feasibility” comments above as they have a direct bearing on the potential for institutional compliance difficulties.
- Regarding **Protocol 9**, defining what constitutes an information or system “flaw” and a “timely manner” are essential to institutional compliance. Both terms are vague and could lead to varying interpretations within and across institutions; guidance confirming that such issues are matters of institutional discretion to be addressed via institutional policy could resolve this concern.
- **Protocol 12** requires revision to allow for current and future practices.
 - Real-time scanning as files are downloaded or accessed is no longer effective practice for research institutions; they generally deploy applications that screen for and block malicious files before an end-user can access them.ⁱⁱⁱ
 - OSTP should revise this protocol to stress the deployment of measures that limit the distribution and accessibility of malicious files to end-users.
 - This issue highlights again the need for the protocols to explicitly allow for the use of alternative measures that are equally or more effective than the protocols.
- If OSTP decides to maintain this list of protocols, it should work with the research cybersecurity community to identify and disseminate self-assessment guidance.
 - For example, Level 1 of the Department of Defense’s Cybersecurity Maturity Model Certification (CMMC) model also largely replicates the FCI safeguards.
 - Thus, OSTP could draw on the [self-assessment guide for CMMC Level 1](#) to inform institutional compliance with the Standard Requirement as well.

Burden (What could lessen the burden of implementing the Standard Requirement?)

- Please see the comments above about shifting to a risk management approach. Barring this, the Standard Requirement should acknowledge the necessity of institutional discretion (as reflected in institutional policy and documented in an institution’s research security program) in implementing the protocols.

- The guidance should also allow for the use of alternative measures that are equally or more effective since the protocols cannot account for all research contexts.
- EDUCAUSE asks that the compliance process allow for appeals in cases where compliance with a protocol is infeasible or unduly burdensome.

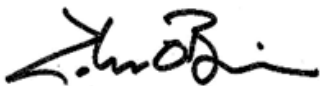
Equity (Are aspects of the protocols barriers to equity and non-discrimination?)

- Blanket application of the protocols plus problematic interpretations of some could lead institutions to raise the floor of the size of the grants that they can support.
 - Institutions near the \$50 million threshold, and especially those still working to overcome historical challenges to building research capacity, could be disadvantaged in growing their research portfolios as a result.
 - Likewise, early-career researchers could find their ability to “climb the ladder” limited as institutions find it difficult to support projects with smaller grant sizes.
- A one-year compliance period may pose major difficulties for resource-challenged institutions; OSTP should facilitate compliance in such cases by allowing institutions to submit a “Plan of Action and Milestones” (POA&M) when negotiating awards.

Conclusion

OSTP may find more detailed discussions of some points useful, and EDUCAUSE would be happy to expand on them as requested. In any case, EDUCAUSE urges OSTP to adopt a risk management approach to research cybersecurity. Barring that, OSTP should make clear that institutions have the discretion to interpret the protocols via institutional policy, with the expectation that such policies will be appropriately documented in an institution’s research security program. In addition, OSTP should explicitly allow for the use of alternative measures where equal or better outcomes can be achieved while accommodating research and institutional needs (again, as appropriately documented). Finally, OSTP should incorporate a POA&M process into its compliance approach to the Standard Requirement. This would ensure that institutions working in good faith to achieve compliance can continue to receive awards even if they cannot fully implement the cybersecurity protocols within the one-year deadline.

Best regards,



John O'Brien
President and CEO
EDUCAUSE

ⁱ The request from the EDUCAUSE community for the Research Security Programs Standard Requirement to adopt a risk-based approach to cybersecurity is consistent with similar requests from other affected stakeholders in relation to other aspects of the Standard Requirement. For example, EDUCAUSE understands that members of the Association of University Export Control Officers (AUECO) raised the concept of incorporating a risk-based approach to the “Foreign Travel Security” provisions of the Standard Requirement into the guidance with Rebecca Keiser, Chief of Research Security Strategy and Policy, National Science Foundation, during the recent [2023 AUECO Annual Conference](#).

ⁱⁱ The EDUCAUSE Higher Education Information Security Council (HEISC) 800-171 Compliance Community Group, which developed an [800-171 toolkit for higher education](#), is another example of collaborative cybersecurity efforts in higher education relevant to research. For more information on RRCoP, please see NSF Award [#2201028](#) as well as <https://www.regulatedresearch.org/>.

ⁱⁱⁱ E.g., endpoint detection and response (EDR) applications.