MEMORANDUM

TO: **Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST)**

FROM: **Council on Governmental Relations**
Contact: Robert Hardy, rhardy@cogr.edu; (202) 289-6655

EDUCAUSE
Contact: Jarret Cummings, jcummings@educause.edu; (202) 331-5372

Association of American Universities
Contact: Tobin Smith, toby_smith@aau.edu; (202) 408-7500

` **Association of Public and Land-grant Universities**
Contact: Deborah Altenburg, daltenburg@aplu.org; (202) 478-6039

American Council on Education
Contact: Terry Hartle, thartle@acenet.edu; (202) 939-9355

DATE: **August 2, 2019**

SUBJECT: **Response to NIST Request for Public Comment on SP 800-171B, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets***

These comments are submitted on behalf of the Council on Governmental Relations (COGR), EDUCAUSE, the Association of American Universities (AAU), the Association of Public and Land-grant Universities (APLU), and the American Council on Education (ACE). A brief description of each of these respective organization follows.

- **The Council on Governmental Relations (COGR)** (www.cogr.edu) is an association of 188 public and private U.S. research universities and affiliated academic medical centers and research institutes. COGR concerns itself with the impact of federal regulations, policies, and practices on the performance of research conducted at its member institutions.
- **EDUCAUSE** (www.educause.edu) is a non-profit association and the foremost community of information technology (IT) leaders and professionals committed to advancing higher education. The EDUCAUSE membership encompasses over 1,800 colleges and universities, over 400 corporations, and dozens of other associations, system offices, and not-for-profit organizations. EDUCAUSE strives to support IT professionals and the further advancement of information technology in higher education through analysis, advocacy, community-building, professional development, and knowledge creation.

- **The Association of American Universities** (www.aau.edu) was founded in 1900 and is composed of 60 of America's leading research universities. AAU's member universities earn the majority of competitively awarded federal funding for research that improves public health, seeks to address national challenges, and contributes significantly to our economic strength, while educating and training tomorrow's visionary leaders and innovators.
- **The Association of Public and Land-grant Universities** (APLU) (www.aplu.org) is a research, policy, and advocacy organization dedicated to strengthening and advancing the work of public universities in the U.S., Canada, and Mexico. With a membership of 239 public research universities, land-grant institutions, state university systems, and affiliated organizations, APLU's agenda is built on the three pillars of increasing degree completion and academic success, advancing scientific research, and expanding engagement.
- **The American Council on Education** (ACE)(www.acenet.edu) is a membership organization that mobilizes the higher education community to shape effective public policy and foster innovative, high-quality practice. ACE represents over 1,700 college and university presidents as well as the executives at related associations, and it is the only major higher education association to represent all types of U.S. accredited, degree-granting institutions. As such, ACE serves as the major coordinating body for the nation's colleges and universities.

Specific Concerns and Comments

Our member institutions agree with the goal of protecting Controlled Unclassified Information (CUI) resident in nonfederal systems and organizations. According to a recent report, our institutions have a higher degree of compliance with the NIST SP 800-171 Security Requirements for CUI than other types of defense contractors (https://sera-brynn.com/wp-content/uploads/2019/05/Reality_Check_DFARS_2019.pdf).

However, our member institutions need a better understanding of how and when sponsoring agencies will apply the enhanced requirements of NIST SP 800-171B. The NIST publication provides very little guidance on how agencies will determine whether a particular grant or agreement will involve a "critical program" and/or "high value asset." Much appears left to agency discretion, leading to concerns that agencies may over-classify information and/or apply the requirements on a project-by-project basis. Our concern is that institutions and their researchers need a way to know in advance whether the 800-171B requirements will apply to the programs and projects they seek to pursue.

Universities often see many terms and requirements included in contracts that are ultimately struck through negotiations as not applicable to the work being performed. The controls specified in the publication are not trivial, however, and cannot be adopted within most contract negotiation timeframes or without significant institutional planning and investment. Therefore, it is imperative that universities have a solid and consistent basis on which to anticipate when these enhanced security requirements may be applied and what degree of

flexibility the institution will have in responding. Unfortunately, the footnoted references to OMB Memorandum M-19-03 and the Federal CIO's high value asset process in 800-171B do not provide the clear, concise explanation of the criteria governing agency use of those designations that will allow stakeholders to anticipate and avoid significant difficulties. In addition, the referenced documents suggest that agencies might consider "adversary and criminal interest" as a sufficient basis for imposing 800-171B requirements, which could lead to their overly broad application.

More detail on our concerns follows.

1. The lack of information in 800-171B about when its enhanced requirements will apply creates a high degree of uncertainty that is likely to negatively impact the efficient pursuit of research at universities on behalf of federal research agencies. In the absence of a mandate that agencies state the applicability of 800-171B in funding announcements, awardees may face huge administrative burdens when they learn only at the time of a grant or contract about agency intentions to impose these controls. The degree to which agencies may impose burdensome paperwork to establish compliance also goes unaddressed in 800-171B. Our member institutions therefore have significant, legitimate concerns about whether they will be able to comply within timeframes that meet the government's contractual needs. More specifically:

- The NIST special publication should directly state the criteria for designating a "critical program" or "high value asset." As previously noted, 800-171B does provide two references, but those pertain to federal information systems. That leaves open the question of whether and how, for example, agencies might assign designations pursuant to the DHS program for high value asset identification established by OMB Memorandum M-19-03, given that 800-171B expressly concerns non-federal systems.
- A case-by-case approach to making critical program and/or high value asset determinations is problematic. Unlike the CUI registry with its well-defined categories of information, the threat-centric approach proposed in 800-171B appears subjective and *ad hoc*. It also appears inconsistent with the National Archives and Records Administration (NARA) guidance that agencies may not implement safeguarding or dissemination controls other than those permitted by the CUI program.
- In the absence of clear guidance, we are concerned that each agency is likely to apply its own, arbitrary interpretation to what is a "critical program," "high value asset," or "advanced persistent threat." Areas that are of high value to U.S. adversaries include a very wide range of technology and research (e.g., artificial intelligence, super computers, medicine, specialized materials, biologics, genetics, agriculture, computer science). While some agencies may view fundamental research in these areas as falling under "critical program" or "high value asset" designations, or as subject to advanced persistent threats, applying 800-171B security controls in such cases would violate National Security Decision Directive 189. The NIST guidance should make clear these controls are inappropriate for fundamental research.

2. The compliance costs associated with 800-171B are potentially prohibitive. The estimates in the DOD cost analysis range up to $66M total for DOD contractors. For large defense contractors that routinely manage critical programs or high value assets, these costs may be justifiable; for universities that may occasionally receive such designations on an individual grant, contract or other agreement, the costs cannot be justified.

- DOD apparently has a particular subset of defense contractors in mind in its cost estimates accompanying the SP 800-171B draft. However, nothing in the NIST materials restricts the 800-171B requirements to that set of contractors. The potential for underestimating the overall cost of compliance, much less the per-organization cost of compliance for any entity that does not match the DOD's selected population, seems reasonably high. It may be that the compliance costs will be incurred only by isolated enclaves and not an institution's entire operating network, but there is no way of making that determination with the available information.
- For example, one of our institutions estimates that managing a deception network, developing and operating a threat hunting team, and implementing related steps could easily cost it $1–$3M/year. Over 5 years there could be a cost of $5–$15M for just those two controls. Regardless of whether capabilities like these are developed in house or outsourced, they entail both upfront as well as ongoing expenses.
- In addition, many research universities are public and must conform to legislatively mandated procurement processes, some of which can last a year or more for large programs.

3. Managing both sets of security requirements for CUI (800-171 and 171B) is unduly burdensome and bureaucratic as well as costly. It essentially requires building a 171 environment and adding the 171B requirements on top. There is potential for confusion, both on the part of agencies and universities, as to which set of requirements applies in a given instance. If the concerns are such that enhanced protection is considered necessary, one possibility would be to classify the information, rather than establishing an additional control regime. Moreover, while 800-171B refers to equally effective alternative measures, it should provide specific examples as well as guidance on how that equivalent effectiveness may be determined, again to avoid undue confusion and compliance issues.

4. The NIST special publication may not adequately account for the level of complexity and sophistication required to deploy a number of the controls, such as disrupting the attack surface through unpredictability, moving target defense, and non-persistence. We believe that legitimate questions exist about whether even companies with large security budgets have the ability to effectively put in place the wide-range of requirements being proposed in this special publication. One cannot reasonably expect universities to implement them rapidly in the context of a given, often relatively brief contract negotiation. For the following reasons, the guidance should provide for multi-year or phased-in adoption of the controls, which again

should be established in relation to clear criteria for critical program/high value asset designation and information classification schema as illustrated by the NARA CUI Registry.

- Many of the security controls involve costly tactics and counterintelligence activity as opposed to defensive security measures. Examples include penetration testing by designated agents and red teams; deception to confuse and mislead adversaries; no-notice social engineering attempts against individuals to gain unauthorized access; the conduct of enhanced personnel screening (vetting) for individual trustworthiness (even when the CUI level does not warrant enhanced vetting); and misleading adversaries through a combination of misdirection, tainting, or disinformation. One might reasonably question the cost versus benefit calculation associated with deploying such advanced measures in relation to unclassified information. It is also unclear how these steps might impact academic research, given a university context in which academic freedom and freedom of expression are considered essential to the research enterprise.
- Many of the described controls are for an environment that is optimized for operational use and not one designed for research and innovation that relies on extremely expensive, sensitive, and complicated scientific equipment like lasers, mass spectrometers, etc., that are used by multiple people for multiple projects. In many cases, due to the rapidly changing environment and unique research needs, there would not be a baseline to which a device could be reverted without introducing prohibitive costs and lengthy delays. This ever-changing research environment also makes it more difficult to deviate from a baseline to create diversity for misdirection, tainting, and disinformation techniques.
- In particular, the requirement (3.6.1e) for a 24/7 Security Operations Center (SOC) staffed by personnel creates prohibitive operational cost, especially for federally funded research projects at universities. Organizations should be allowed to tailor their approach to meet the objective of continuous monitoring using their own best-fit combination of technology and personnel rather than a specific requirement to use human beings. For example, the objectives of such monitoring, including detection, alerting, and response, can often be accomplished through the use of automated tools. Note that this approach would also be consistent with industry trends toward increased reliance on automation for such tasks.

Conclusion

Thank you for the opportunity to help inform this important process. We hope that NIST will consider our comments and clarify:

- The criteria and processes for designating critical programs and high value assets outside of federal information systems;
- The parameters that will ensure consistency among federal agencies in the application of such designations and thus the 800-171B requirements;

- The flexibility and discretion that agencies and institutions will have in determining which controls truly fit with the unclassified information in question given the context of the research being conducted; and
- The cost mitigation strategies that agencies and institutions might pursue to ensure that appropriate security is maintained without diverting limited resources from vital research objectives.

We also ask that NIST open a new, longer comment period after providing a revised draft containing the requested clarifications. This will allow universities to more fully consider the potential impact of the 800-171B requirements based on a more complete picture of their scope and agency/institutional discretion in relation to them. Institutions will particularly want to gauge the extent to which a revised draft reflects that NIST has worked with other federal agencies to:

- Consider the administrative burden of the proposed requirements, and
- Clarify or establish a common approach to applying them, including guidance for multi-year or phased-in adoption of 800-171B controls.

Overall, we believe that significant, unnecessary, and costly complications would arise from attempting to apply 800-171B as currently written in the context of fundamental research performed at universities. These complexities could prohibit some universities from undertaking important research projects on behalf of the federal government, ultimately harming, not helping, to protect national security. Therefore, in addition to the clarifications we have requested, we urge NIST to clearly state in the publication that these requirements are inappropriate for fundamental research activities.