

VIA ELECTRONIC SUBMISSION: sec-cert@nist.gov

January 15, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930
Email: sec-cert@nist.gov

Re: Comments in Response to the National Institute of Standards and Technology's Release of Draft Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (Initial Public Draft).

To Whom It May Concern:

EDUCAUSE respectfully submits these comments to the National Institute of Standards and Technology (NIST) in response to the above-referenced release and opportunity to comment regarding Draft Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (Initial Public Draft).

EDUCAUSE is a non-profit association and the foremost community of information technology (IT) leaders and professionals committed to advancing higher education. Our membership encompasses over 2,000 colleges and universities, over 300 corporations serving higher education IT, and dozens of other associations, state and federal agencies, 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/network building, professional development, and knowledge creation.

The culture of higher education is one that highly values autonomy, freedom, collaboration and sharing, decentralized administration, and distributed decision-making (i.e., faculty governance), particularly with respect to research and development activities. These cultural factors, combined with limited resources and a complex regulatory environment, may in some cases lead to confusion and inefficiencies in the protection of research funded by, and Controlled Unclassified Information (CUI) received from, the federal government. Thus, higher education institutions can benefit from reasonable, flexible security control standardization.

Jarret S. Cummings Director
Policy & External Relations
jcummings@educause.edu / Direct 202.331.5372

EDUCAUSE members with subject matter expertise in information security offer the following comments on Draft Special Publication 800-171 for NIST consideration in subsequent drafts:

- It would be helpful if the document contained additional, simplified information about generalized categories and data types considered CUI, rather than references back to the CUI Registry. Adding simplified categories would help institutions in the initial data identification and categorization efforts needed to follow Draft Special Publication 800-171.
- It would also be helpful if the document included guidance on when Draft Special Publication 800-171 applies and when other regulations, such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR), may supersede Draft Special Publication 800-171.
 - Note in particular that Student Records (covered by FERPA) are included as a subcategory in the CUI Registry.
- Draft Special Publication 800-171 includes a call-out box, “Cost-Effective and Efficient Implementation of CUI Requirements” (p. 7). It would be helpful if additional, non-prescriptive guidance regarding data protection were included in the document for those nonfederal organizations that are not able to segregate information system exclusively for CUI. Information system segregation can be difficult for higher education institutions due to the cultural factors previously mentioned.
- Draft Special Publication 800-171 includes a call-out box, “Establishing Expectations for this Publication” (p. vii). It would be helpful if the following statement in the call-out box were repeated in Chapter 3 of Draft Special Publication 800-171: “There are many potential security solutions that can be implemented by nonfederal organizations to satisfy the security requirements—that is, alternative, but arguably *equivalent methods* may be employed” (emphasis from original). Such language would highlight the expectation that nonfederal organizations have some flexibility in addressing the security requirements specified in Draft Special Publication 800-171.
- It would be helpful if each derived security requirement specified in Chapter 3 of Draft Special Publication 800-171 were mapped directly back to its corresponding control (and identifying number) as specified in Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix F—Security Control Catalog, rather than included as a bulk citation at the end of each section in Draft Special Publication 800-171.
- Section 3.5, Identification and Authentication, Derived Security Requirement (a): It would be helpful if the document contained additional flexibility on the use of multifactor authentication, or offered additional guidance regarding compensating

Jarret S. Cummings Director
Policy & External Relations

jcummings@educause.edu / Direct 202.331.5372

controls for those nonfederal organizations that have not yet adopted multifactor authentication or may be in the process of implementing multifactor authentication.

- Section 3.9 Physical Protection, Derived Security Requirements (a-c): It would be helpful if the document contained additional risk-based flexibility on physical protection requirements for nonfederal organizations. While some higher education institutional facilities have extensive physical security safeguards in place because of the nature of the services they support and/or the information they contain, most institutional buildings and rooms allow for unfettered public access.

It is anticipated that higher education institutions will see the biggest impact from Draft Special Publication 800-171 in the basic and applied research areas, where federal government data designated as CUI is provided to an institutional researcher. Information security is enhanced when such data, regardless of federal government source, is protected according to a single set of guidelines. That said, the higher education sector is comprised of an extremely diverse set of institutions that makes the application of “standards” and “practices” difficult to achieve without a significant degree of flexibility and nuance.¹ EDUCAUSE encourages NIST to incorporate sufficient flexibility into Draft Special Publication 800-171 to allow nonfederal agencies to fulfill the spirit of the specified security controls without prescriptive requirements.

We appreciate the opportunity to comment on Draft Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* and thank the agency for its consideration of our comments.

Sincerely,



Jarret S. Cummings
Director, Policy & External Relations
EDUCAUSE

¹ There are over 4,500 colleges and universities in the United States. Although seventy percent of those institutions are private or independent – and typically small- to mid-size – and 30 percent are public institutions that receive some level of state financial assistance and oversight, over 70 percent of students are educated at public colleges and universities that include two-year or community colleges. While a large university may be similar in many respects to a large enterprise in the private sector, most institutions of higher education are small and are the equivalent of a small business. Additionally, the not-for-profit sector of higher education is dependent on tuition, fees, private donors, and public assistance to support the educational and research mission