March 13, 2017

Subject: HSAR 2015-001 Safeguarding of Controlled Unclassified Information (82 FR 6429)

Attn: Ms. Shauna Duggans

Dear Ms. Duggans:

The Association of American Universities (AAU) comprises 62 leading research universities that advance society through education, research, and discovery. AAU members collectively help shape policy for higher education, science, and innovation; promote best practices in undergraduate and graduate education; and strengthen the contributions of research universities to society.

The Association of Public and Land-grant Universities (APLU) 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 235 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 Council on Governmental Relations (COGR) is an association of over 190 research-intensive institutions in the United States. COGR works with federal agencies and research sponsors to develop a common understanding of the impact the federal policies, regulations and practices may have on the research conducted by the membership.

EDUCAUSE is a non-profit association of information technology (IT) leaders and professionals committed to advancing higher education. With a membership of approximately 2,400 colleges, universities, and related organizations, EDUCAUSE strives to further the role of IT in higher education through professional development, knowledge creation, advocacy, and community building.

Our associations remain concerned about the implications of the compliance requirements for protecting Controlled Unclassified Information (CUI) in non-Federal information systems such as those operated by our member institutions. While we fully agree with the importance of protecting information, we have worked closely with NIST and NARA to try to ensure that the NIST SP 800-171 security requirements can be implemented in a manner that will minimize the burdens on our institutions. Some of our associations previously submitted comments which the agencies took into account in developing their final requirements and rule on CUI (http://www.cogr.edu/sites/default/files/Joint_COGR_AAU_Letter_to_NIST_on_Controlled_Unclassified_Information.pdf; http://www.aau.edu/WorkArea/DownloadAsset.aspx?id=16276).

Unfortunately, the proposed HSAR 2015-001 rule appears to confuse rather than clarify the applicability of government security requirements applicable to CUI. Many of the proposed new categories of CUI set forth by DHS in the proposed rule do not correspond to categories in the NARA CUI Registry. This conflicts with the

standardized approach established by Executive Order 13556 as implemented by the NARA Final Rule on CUI (81 FR 63323). According to the NARA Rule, the CUI Registry:

> *Is the authoritative central repository for all guidance, policy, instructions, and information on CUI" (35 CFR 2002.10(a)(1))...CUI categories and subcategories are the exclusive designations for identifying unclassified information that a law, regulation, or Government-wide policy requires or permits agencies to handle by means of safeguarding or dissemination controls. All unclassified information throughout the executive branch that requires any kind of safeguarding or dissemination control is CUI. Agencies may not implement safeguarding or dissemination controls for any unclassified information other than those controls permitted by the CUI Program…Agencies may use only those categories or subcategories approved by the CUI EA and published in the CUI Registry to designate information as CUI (2002.12).*

Included among the new CUI categories in the proposed DHS rule is information that DHS receives pursuant to information sharing agreements with state, local and private sector partners (3052.204-7X(a)(4)). The parameters of this type of information are very uncertain and seemingly could apply to any information included in such agreements. It is difficult to reconcile this proposed category of CUI with the uniform CUI structure envisioned in the NARA Rule. Also, the effect would be to subject any shared information to security requirements for Federal information systems, which appears to directly conflict with the objectives of the NARA CUI Program.

We note that footnote 5 distinguishes the information system security requirements in the proposed rule that are focused on Federal agency operated information systems - including contractor information systems - from the requirements of NIST SP 800-171 that apply to non-federal entities (including university contractors) that handle, process, use, share or receive CUI. While we appreciate the distinction, unfortunately it is not fully reflected in the proposed rule. The proposed HSAR policy statement states that the requirements apply to "any situation where contractor employees may have access to CUI (3004-470-3(a))." The instruction provided to contracting officers is to insert the HSAR Safeguarding clause when "contractor … employees will have access to CUI" (3004-470-4(b)). This language should be clarified to clearly align with the language in footnote 5 so as to make it clear that contracting officers should not apply the language to contractor information systems.

The NARA Final Rule draws a clear distinction between FISMA requirements that apply to protection of Federal information and Federal information systems under FISMA Publication 200 and NIST SP 800-53, and situations when non-executive branch entities are not using and/or operating an information system or maintaining and/or collecting federal information "on behalf of" an agency. In the latter case, NIST SP 800-171 security requirements apply (p.63330). It has been the experience of our member institutions that this distinction is not well understood by Federal agencies, who continue to misapply FISMA requirements to non-Federal information systems not operated "on behalf of" agencies (as defined in the NARA Rule). We are concerned that by relegating this distinction to a footnote, similar misunderstandings may occur in the case of DHS, leading to inconsistent and inappropriate application of the HSAR requirements.

We appreciate the statement in the proposed rule that "Neither the basic clause or its alternates should ordinarily be used in contracts with educational institutions" (3004-470-4(a)). However, given the confusion over the scope of the rule, there may be some impact, especially if other agencies follow DHS's lead. As the initial agency acquisition regulation issued subsequent to the NARA rule, we believe that the inconsistency in the HSAR rule with the NARA CUI rule will set an unfortunate precedent. While we expressed concerns to NARA about some aspects of the NARA rule when it was proposed, we welcomed the uniformity and predictability of

one overarching set of government-wide rules for safeguarding CUI. Failure on the part of DHS, or for that matter, any agency to adhere to policies consistent with the NARA rule will result in undue burdens and unnecessary costs for our member institutions. This also is inconsistent with current efforts launched by this administration to reduce undue and excessive government regulations.

With this in mind, we recommend that DHS revise statements about the scope of their rule, such as those quoted above, to clarify or remove the language about "accessing" CUI (we note a statement about the need to "ensure adequate security for CUI that is accessed by contractors" also is included in the Background statement). Our associations further recommend that the content of footnote 5 be moved upfront to the Background statement. This change would help to greatly improve the clarity of the scope of the rule and avoid unnecessary misinterpretations and misunderstandings. Finally, the proposed rule should be revised to be made fully consistent with the existing NARA requirements.

We appreciate the opportunity to comment. Please contact Tobin Smith at AAU toby.smith@aau.edu (202-408-7500), Sarah Rovito at APLU srovito@aplu.org (202-478-6065), Robert Hardy at COGR rhardy@cogr.edu (202-289-6655 x114), or Jarret Cummings at EDUCAUSE jcummings@educause.edu (202-331-5372) if you have any questions.

Tobin Smith, AAU
Sarah Rovito, APLU
Robert Hardy, COGR
Jarret Cummings, EDUCAUSE