January 16, 2015

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

RE: NIST Special Publication 800-171

Dear Sirs/Madams,

I am writing on behalf of the Association of University Export Control Officers (AUECO), a group of senior export practitioners at over 70 accredited institutions of higher learning in the United States. AUECO members monitor proposed changes in laws and regulations affecting academic activities and advocate for policies and procedures that advance effective university compliance with applicable U.S. export controls and trade sanction regulations.

AUECO is providing the following comments in response to the National Institute of Standards and Technology (NIST) Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. We recognize the importance of safeguarding Controlled Unclassified Information (CUI), regardless of where such information is located. AUECO applauds the NIST's recognition that there are many potential security solutions that may meet situation specific requirements for the protection of CUI and the consequent attempt to be non-prescriptive in the proposed guidelines.

AUECO believes that NIST 800-171 could be strengthened with additional definitions and clarifications. Specifically, the document is predicated on the need to protect sensitive unclassified federal information residing in non-federal systems, but the document does not provide a definition for what comprises "federal information."[1] Is "federal information" narrowly defined and limited to information provided by or created in activities funded by a federal agency; or does it broadly include all information with confidentiality or disclosure limitations imposed by federal regulation? If the former, does it matter if the information is generated as the result of grant funding as opposed to a cooperative agreement or contract? Universities handle a broad range of sensitive information controlled by a plethora of regulatory requirements such as student records controlled by the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99), health information controlled by the Health Insurance Portability and Accountability Act of 1996, financial information controlled by Payment Card Industry Data and Security Standards, and research information that may be controlled by the International Traffic in Arms

[1] NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, p.iii (abstract).*

Regulations (22 C.F.R. § 120-130) or Export Administration Regulations (15 C.F.R. § 730-774), to name a few. We have designed our information systems to protect such information as required, and are concerned that federal agencies will contractually impose additional requirements beyond the statutory requirements as a result of this guidance document. The guidance is clearly intended to be limited to "information" that "is owned by, is produced by or for, or is under the control of the United States Government" (USG)[2]; therefore, it would be helpful for the Special Publication to clarify to federal agencies responsible for CUI that the intent of the document is not to impose additional administrative burden on the University community. Likewise, we recommend adding a clear statement that the guidance proposed in the Special Publication does not apply to and does not create protection requirements for similar information (e.g., health or student information) which is not owned by, produced by or for the USG but may be resident on or transiting nonfederal systems.

AUECO believes that NIST 800-171 could have the unintended consequence of CUI overreach. According to the National Archives and Records Administration (NARA) website: "Executive Order 13556 "Controlled Unclassified Information" (the Order) establishes a program for managing all unclassified information in the Executive branch that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies." [emphasis added]

Federal Acquisition Regulation 48 CFR 27.404-4(a) *Contractor's release, publication, and use of data* prohibits any non-Department of Defense (DoD) federal agencies from placing restrictions on contracts for basic and applied research at colleges and universities except as provided in applicable statutes. It does not authorize restrictions based on "government wide policies." Any contract clause generated to establish CUI controls in federal contracts needs incorporate this restriction and notify the sponsoring federal agency of these restrictions when dealing with contracts for basic and applied research for colleges and universities.

AUECO believes that NIST 800-171 could be strengthened with clarifications within the proposed list of CUI Categories and Subcategories including the proposed Category "Export Control," proposed Subcategory "Research."

Within the CUI Category "Export Control" described as:
"Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information."

AUECO can find no statutory or government policy authorizing the control of the following CUI:

[2] Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556.

> "Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives."

The test of reasonableness is an inappropriate (and unauthorized) standard against which to determine whether or not information is controlled as export controlled CUI. AUECO recommends removal of this description entirely from the definition of export-controlled information.

"Technology", "technical data" and "sensitive nuclear technology" are already defined terms within the export regulations (see 15 CFR 774, 22 CFR 120.10, and 10 CFR 810.3) and should be used to determine whether or not information is "export-controlled" CUI. To be more precise, AUECO suggests using the following description:

> "Export-controlled "technology" subject to the Export Administration Regulations (EAR), "technical data" subject to International Traffic in Arms Regulations (ITAR) and "sensitive nuclear technology" subject to the Assistance to Foreign Atomic Energy Activities Regulations (AFAEAR); and license applications."

A more complete review of the statutory authorizations cited under the Export Control Category is warranted. Some of the statutory authorizations identified in this Category of CUI can only be described as "Inconsistent." For example, 42 USC 2077(a)* controls no information, but rather regulates the export of materials; nor does it identify any specific handling or marking requirements, as specified by the asterisk (*) marking of the Category. Similarly, 50 USC Appendix 2405(l)(5) describes an information sharing scheme that should be established for information sharing to ensure effecting monitoring of MTCR equipment, without describing any such policy or procedure that actually does establish these measures.

AUECO proposes that the CUI Category "Export Control" Subcategory "Research" be changed to "Export-Controlled Research." "Fundamental Research" referenced in 15 CFR 734.8(c) is a defined term outside of the scope of the ITAR and EAR. As a result, "fundamental Research" does not include CUI. Suggesting that the regulation is an authorization for controlling research as a subcategory of CUI is misleading. As such, the reference should be removed, or the alternative could be left in the listing if there was a disclaimer that this regulation does not authorize a subcategory of CUI. Statutory ITAR and EAR references comparable to 15 CFR 734.11 are missing from the statutory authorizations of the Subcategory.

In reviewing NIST 800-171, AUECO noted that there are 101 active controls, which exceed the 51 active controls deemed adequate by the DoD to control Unclassified Controlled Technical Information (CTI), as prescribed in Defense Federal Acquisition Regulations (DFAR), specifically, DFAR 252.204-7012 Safeguarding Unclassified Controlled Technical Information (see http://www.gpo.gov/fdsys/pkg/FR-2013-11-18/html/2013-27313.htm). Given that the DoD has already established the minimum information security standards for safeguarding CTI, AUECO suggests that the proposed NIST controls in NIST 800-171 be harmonized with those already in effect in DoD contracts by the issuance of the DFARS clause at 252.204-7012 in DoD issued contracts.

Finally, AUECO requests that NIST consider adding guidance for non-federal organizations on the use of third party systems, such as cloud computing service providers for CUI. The export control regulations have to date, not provided guidance to cloud users (as opposed to cloud service providers) as to when and under what conditions the use of third party information storage systems may be appropriate. The NIST guidance document presents an opportunity to provide this important clarification, particularly as it related to the Export Controlled information captured as CUI.

AUECO appreciates the opportunity to provide NIST with the above comments on the NIST Special Publication 800-171.

Sincerely,

Mary Beran

Chair
Association of University Export Control Officers
Email: auecogroup@gmail.com
Website: http://aueco.org