PSC PROFESSIONAL SERVICES COUNCIL
The Voice of the
Government Services Industry

April 13, 2017

Department of Homeland Security
Office of the Chief Procurement Officer, Acquisition Policy and Legislation
Attn: Ms. Shaundra Duggans
245 Murray Drive
Bldg 410 (RDS)
Washington, DC 20528

Subject: Homeland Security Acquisition Regulation (HSAR) Case 2015-001, Safeguarding of Controlled Unclassified Information (CUI)

Dear Ms. Duggans:

On behalf of the Professional Services Council (PSC), I am pleased to submit these comments on the proposed rule, HSAR Case 2015-001, Safeguarding of Controlled Unclassified Information (CUI). PSC is the voice of the government technology and professional services industry, representing the full range and diversity of the government services sector. As a trusted industry leader on legislative and regulatory issues related to government acquisition, business and technology, PSC helps build consensus between government and industry. Our nearly 400 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the trade association's members employ hundreds of thousands of Americans in all 50 states.

While we applaud the stated intent of the draft rule to increase transparency and make requirements more accessible and commonly understood, the proposed rule contains a number of troubling issues that must be resolved prior to any final issuance. So much progress has been made in recent years by: (a) aligning the government to common security controls through the National Institute for Standards of Technology (NIST) Special Publication 800-53, Recommended Security and Privacy Controls for Federal Information Systems and Organizations and the NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations, and (b) replacing the multitude of confusing and non-standard markings for sensitive but unclassified information through the National Archive and Records Administration (NARA) Final Rule on Controlled Unclassified Information (CUI). DHS's proposed rule must not undo this government-wide alignment to common rules, controls and taxonomy.

Our specific concerns with the DHS proposed rule include the following:

- **Consistency in the designation of CUI.** Our most important concern with the proposed rule is that it significantly deviates from the framework established by the NARA CUI Rule by adding additional DHS-unique categories of CUI. It is crucial that individual agency guidance not subvert NARA's substantive progress in aligning federal agencies to a common taxonomy. And it is particularly concerning if, as implied in the draft rule, the intent is to allow DHS to determine what "Homeland Security Agreement Information" is on a case-by-case basis in individual contracts.

- **Confusion on the use of NIST standards.** The proposed rule lacks clarity on the appropriate application of NIST SP 800-53 for federal agencies and their information systems and NIST SP 800-171 for non-federal agency systems. Footnotes in the draft rule downplay the applicability of NIST SP 800-171 and imply that the guidance is for the more limited set of systems covered by NIST SP 800-53. However, in other parts of the draft rule, contractors' internal business systems that do fall under the provisions of NIST SP 800-171 are specifically called out. DHS must maintain the applicability of NIST security controls in a consistent manner within the department and with the rest of the federal government to ensure consistent application of security controls across government. This point is particularly important given the fact that many DHS contractors perform work for multiple federal agencies, making it crucial to adhere to common requirements across government.

- **Consistency in ATO requirements and ensuring reciprocity.** The proposed rule in unclear on the limited applicability of NIST SP 800-53, at what point in the contracting process does a DHS ATO have to be completed and what the applicability of these rules is when acquiring commercial items under FAR Part 12. In the absence of more definitive guidance, unnecessary expenses may be incurred by potential offerors, or competition may be needlessly stifled, precluding access to best commercial solutions and innovative new technology. In addition, the rule fails to emphasize the need for reciprocity across federal agencies and the requirement to rely upon provisional authorizations and ATOs already obtained through other federal agencies.

- **Incident reporting.** There is a lack of consistency between DHS and DoD incident reporting requirements on what constitutes timely reporting of breaches. The DHS requirement to report incidents involving PII or SPII within one hour of discovery, and all other incidents within eight hours of discovery, is unreasonably short and inconsistent with other government requirements. As companies often do work for multiple federal agencies, it is important to have a consistent approach government-wide so that companies are able to set up a single compliant system and process. In addition, almost all states have enacted data breach notification requirements. Consistency between federal and state requirements, particularly given DHS's mission, should also be considered.

- **Consistency in cleared facility requirements.** Guidance on DHS CUI requirements for cleared facilities should be consistent with DoD cleared facility requirements.

- **Clarity of effort.** The proposed rule requests comment on making the Safeguarding of CUI clause applicable to all service contracts with the understanding that the clause would be self-deleting if it doesn't apply. It would be preferable for the government to include the clause only in those contracts where the clause is required. There is no realistic "self-deleting" function.

The proposed rule must not undo the progress made across the federal government on consistent security controls and CUI requirements. By diverging from this common path, DHS is creating addition costs and administrative burdens, increasing confusion and incurring potential delays in getting needed technology solutions deployed in government. We strongly recommend that DHS not proceed to finalize this rule until the department can address the issues in this letter.

PSC also joined in an April 11, 2017 letter on this proposed rule signed by associations that comprise the Council of Defense and Space Industry Associations (CODSIA).

Thank you for the opportunity to comment on this proposed rule. PSC would be pleased to discuss our comments and recommendations with you and others. In the interim, please feel free to contact me by email at wennergren@pscouncil.org or by phone at 703-778-7557, if you have any questions or need additional information.

Sincerely,

David M. Wennergren
Executive Vice President & Chief Operating Officer