COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22209
codsia@codsia.org

April 11, 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); Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001) – CODSIA Case 2017-002

Dear Ms. Duggans:

On behalf of the undersigned members of the Council of Defense and Space Industry Associations (CODSIA),[1] we offer the following comments on the Department of Homeland Security (DHS) proposed Homeland Security Acquisition Regulation (HSAR) on Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001) that was published in the Federal Register on January 19, 2017. This letter goes into detail on several issues CODSIA members have with this proposed rule.

This proposed rule is problematic for several reasons. First and foremost, it goes beyond the framework allowed and established by the National Archive and Records Administration (NARA) Final Rule on Controlled Unclassified Information (CUI) effective November 14, 2016. In NARA's Final Rule on CUI, it states "agencies may use only those categories or subcategories approved by the CUI Executive Agent (established by Executive Order 13556 as NARA) and published in the CUI Registry to designate information as CUI." The Final CUI rule also explicitly states that it "overrides agency-specific or ad hoc requirements when they conflict." Despite these descriptive limitations, the proposed rule by DHS has added four new categories of CUI not recognized by NARA. One of these categories, "Homeland Security Agreement Information," is defined in a way that would allow DHS to determine what is DHS CUI in individual contracts. In these respects, the proposed HSAR departs from core principles of the NARA Final Rule: first, that there be a basis in statute, regulation or government-wide policy to establish a CUI category, and second, that all federal departments and agencies should utilize the categories of CUI identified in the CUI Registry and not create new categories unilaterally.

Additionally, the proposed HSAR CUI ignores NARA's requirements to use the National Institute for Standards of Technology (NIST) Special Publication 800-171, Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations, to safeguard

[1] At the suggestion of the Department of Defense, CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues. CODSIA consists of seven associations – the Aerospace Industries Association, the American Council of Engineering Companies, the Associated General Contractors of America, the Information Technology Alliance for Public Sector, the National Defense Industrial Association, the Professional Services Council, and the U.S. Chamber of Commerce. CODSIA acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. Together these associations represent thousands of government contractors and subcontractors. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

CUI when contractors are hosting, transmitting or using CUI. This DHS omission is contrary to the proposition that there should be one set of safeguards (SP 800-171) for all CUI regardless of the agency that originated or acquires the CUI. DHS conflates security requirements for contractors who use DHS CUI to operate a federal information system on behalf of the agency with those contractors who have access to DHS CUI by the agency. The DHS proposal requires both types of contractors to provide adequate security to protect CUI as defined by DHS policies and procedures without explaining who is responsible for identifying or designating DHS CUI. While NARA's Final CUI rule states that federal agencies are not to impose federal information system requirements on non-federal information systems, the proposed HSAR does just that by not distinguishing between the two types of information systems, thereby placing a requirement on non-federal information systems despite NARA's rule indicating that such non-federal systems are to use the NIST SP 800-171 to safeguard CUI. Many DHS contractors perform work for multiple agencies. The proposed HSAR presents the undesirable prospect that safeguarding requirements for DHS CUI will be different from what other agencies require for the same information type or, worse. By leaving to future determination what safeguards it will expect its suppliers to apply to CUI, DHS will make it very difficult for contractors to implement cybersecurity measures that will satisfy DHS as well as other agencies. Federal agencies should strive for consistency in the identification and designation of CUI, and in the cyber safeguards non-federal entities are to apply.

These are just a few of the many instances in which the HSAR CUI does not align with the NARA CUI Final Rules and is illustrative of the inconsistencies that exist between the proposed rule and the CUI Final Rule used by other federal agencies.

Moreover, other requirements that would be imposed by the proposed rule could prove to be quite costly and burdensome for contractors. For instance, the proposed HSAR CUI could be interpreted to require that contractors meet the security requirements of NIST SP 800-53 when safeguarding CUI at DHS prior to collecting, processing, storing, or transmitting CUI. It appears a contractor will need to have gone through the DHS ATO process and demonstrated its capabilities to meet the HSAR requirements. This process thwarts the "do once, use many" efficiencies established under FedRAMP, which this proposal ignores. To the extent possible, the Government should be tying new regulatory requirements on cybersecurity controls to the FedRAMP program, which was arguably developed specifically to address this type of randomization. This will impose significant responsibilities on DHS, will require a great expense to the contractor and, thus, DHS will end up limiting competition. Furthermore, this proposed rule applies to all contractors, including small businesses, contractors and subcontractors that are providing commercial items acquired under FAR Part 12, and other subcontractors performing on contracts. This would further erode the DHS access to innovative technology and increase the number of obstacles to market entry to the DHS supply chain for these companies as well as new start-ups with innovative technical ideas. Considering that all commercial organizations worldwide, all businesses, and the public use information systems to conduct their everyday activities, it is reasonable to conclude that this rulemaking will have a significant impact to all American companies, and the entire global supply chain. Therefore, we recommend that DHS exclude commercial items.

Lastly, there are many issues that need clarification before the proposed rule can be advanced. For instance, does the proposed rule cover information shared with ISAO's or ISAC's on software vulnerabilities? Would the ISAO or ISAC require flow down of the clauses to ensure

that their members provide adequate protection in accordance with the DHS proposed rule? If so, this would impose a significant barrier for private sector entities to participate in information sharing.

Conclusion

In conclusion, this rule contains many flaws that not only contradict existing regulations but also make it harder for businesses to comply as well as compete in the DHS marketplace. CODSIA considers the rule ill-considered and not properly coordinated with other agencies that follow and support the principles of the NARA Final Rule. Moreover, the Rule adds burdens to DHS and its contractors that differ from what is required or expected by others. Accordingly, CODSIA requests that DHS withdraw Homeland Security Acquisition Regulation on Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001) as requested in our March 10, 2017 letter. If DHS declines to withdraw the proposed rule, then CODSIA requests that DHS delay implementation of the entire rule or suspend the rulemaking process altogether pending further progress with the expected general federal FAR CUI Rule. CODSIA strongly recommends that DHS not proceed to finalize this rule until it can address all of industry's concerns and comply with the NARA CUI Framework. If DHS proceeds, this will open the door for the return to the ad hoc agency specific policies, procedures, and markings for the safeguard and control of this information that NARA and FAR rules are designed to prevent. This inconsistency has historically resulted in increased costs and confusion as industry is forced to adapt and respond to a myriad of agency-specific security requirements.

We thank you for your attention to our comments and your consideration of our recommendations. If you have any questions, or need any additional information, please do not hesitate to contact Ms. Pam Walker, Senior Director, Federal Public Sector Technology, ITAPS, who serves as our point of contact for this request, at pwalker@itic.org.

Respectfully submitted,

John Luddy
Vice President National Security
Aerospace Industries Association

Jessica Salmoiraghi
Director of Federal Agencies and
International Programs
American Council of Engineering
Companies

Jimmy Christianson
Regulatory Counsel
Associated General Contractors of America

A.R "Trey" Hodgkins, III, CAE
Senior Vice President, Public Sector
Information Technology Alliance for the
Public Sector

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22209
codsia@codsia.org

James Thomas
Assistant Vice President for Policy
National Defense Industrial Association

Alan Chvotkin
Executive Vice President and Counsel
Professional Services Council

Neil L. Bradley
Senior Vice President & Chief Policy Officer
U.S. Chamber of Commerce