Date: March 15, 2017

Attention: Ms. Shauna Duggans

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

Dear Ms. Duggans:

Background:
Executive Order 12829, "National Industrial Security Program," establishes the National Industrial Security Program Policy Advisory Committee (NISPPAC) as an advisory committee acting through the Director, Information Security Oversight Office (ISOO). The Director, ISOO serves as the Chairman of the Committee, and is responsible for implementing and monitoring the NISP, developing directives implementing the Order, reviewing agency implementing regulations, and overseeing agency and industry compliance. The Committee's total membership of 24 voting members is comprised of 16 representatives from those executive branch departments and agencies (including the Chairman) most affected by the NISP and eight non-government representatives of contractors, licenses, or grantees involved with classified contracts, licenses, or grants. The purpose of the NISPPAC is to advise the Chairman on all matters concerning the policies of the National Industrial Security Program (NISP), including recommended changes to those policies, and to serve as a forum to discuss policy issues in dispute.

In addition to the eight non-government representatives, a group comprised of the leaders from: Aerospace Industries Association Industrial Security Committee (AIA ISC); the ASIS International Defense and Intelligence Council (ASIS D&IC); NCMS Inc., the Society of Industrial Security Professionals (NCMS); the National Defense Industrial Association Industrial Security Committee (NDIA ISC); the Professional Service Council (PSC) and two working groups, the Industrial Security Working Group (ISWG) and the Contractor Special Security Working Group (CSSWG) collectively known as the “MOU Group” work together to act on behalf of the best interest of the industry organizations they represent and by extension, all private sector members of the NISP. The individual representatives from the “MOU Group” support the NISPPAC in several important ways, including participation in working groups, and making recommendations to the NISPPAC on proposed and revised national security policies.

The eight non-government representatives of the NISPPAC as well as the organizations comprising the “MOU Group,” represent over 13,000 cleared facilities within the NISP and over 200,000 uncleared facilities that may be entrusted with the protection of CUI. We have been following policy changes concerning CUI for the past eight years and have a vested interest in the methodologies we will be required to implement for its protection.

Discussion:
We are extremely disappointed in the proposed rule and feel it is contradictory to CUI Federal Regulation 32 CFR, Part 2002 as it will impose a parallel set of standards upon industry which in turn opens the door for the return to the ad hoc agency specific policies, procedures, and markings for the safeguard and control of this information. This inconsistency has historically resulted in increased costs as industry attempts to adapt and respond to the myariad of agency security requirements for the same information. Additionally, the final NARA CUI Rule states: "Agencies may use only those categories or subcategories approved by the CUI EA [Executive Agent NARA] and published in the CUI Registry to designate information as CUI." Clearly, the proposed DHS regulation fails to follow this requirement. Although the concerns with this rule are many, highlights of our concerns are as follows:

- The proposed HSAR rule creates four new categories/sub-categories of CUI that are not in the NARA CUI Registry: Homeland Security Agreement Information, Homeland Security Enforcement Information, Operations Security Information, and Personnel Security Information. Troublesome is the "Homeland Security Agreement Information" category. This category identifies CUI as any information contained in an information-sharing agreement. This type of "catch all" category runs counter to the CUI Program. It circumvents Executive Order 13556 and permits an agency to protect anything put into an information sharing agreement; thus defeating the categorization structure established through the on-line CUI Registry (www.archives.gov/cui) by not being tied to a particular type of information.

- The proposed HSAR rule fails to reflect the information systems safeguarding requirements of the CUI Federal regulation (32 CFR 2002) and allows DHS full discretion on what electronic safeguarding controls to apply to contractors for any category of CUI. The proposed rule does this (allowing DHS to levy any information systems controls whatsoever on non-Federal information systems and treat them according to its agency-specific policies) by making no distinction operationally in the way non-Federal contractor information systems and DHS agency information systems are treated, a distinction made in the CUI regulation (32 CFR 2002) and in the Federal Information Security Modernization Act of 2014 (FISMA).

- By failing to incorporate the definition of "on behalf of' and the requirements of the CUI Federal regulation (32 CFR 2002) into the DHS regulation implementing the CUI Program for the contractor environment, and presenting itself to others as a major agency successful in thus pushing back on a Federal regulation, DHS undermines the CUI Program's implementation in the Executive branch. The CUI Executive Agent will have no basis to ask other agencies to modify their current agency-specific SBU safeguarding and dissemination practices for the non-Federal world, except perhaps for adopting CUI categories and their markings.

In light of the fact the proposed rule goes beyond the Final Rule on CUI and the intent under Exective Order 13556 to establish consistency for the marking and protection of CUI we respectively request DHS to withdraw Homeland Security Acquisition Regulation on Safeguarding of Controlled Unclassified Information (HSAR Case 2015-001). If DHS decides not to withdraw the proposed rule, it is our suggestion that the changes needed for this regulation be as follows:

- Remove any reference to the creation of the four new categories of CUI currently not recognized by NARA. Under the Final Rule on CUI it states, "agencies may use only those categories or subcategories approved by the CUI Executive Agent and published in the CUI Registry to designated information as CUI." If these categories are required then DHS should consult with the CUI Executive Agent (NARA) to ensure proper designation of any such information.

- The definition of "on behalf of" contained in 32 CFR 2002, needs to be incorporated and in general the proposed rule made consistent with the CUI Program's Federal implementing regulation (32 CFR 2002). The requirements and regulatory distinctions laid out in 32 CFR 2002.14 (g) and (h) regarding Federal and non-Federal information systems, which include an appropriate reference to the NIST SP 800-171, must be incorporated.

- Based on the clear wording of the NARA CUI Final Rule, NIST SP 800-171 establishes the safeguards contractors are to use when they host, transmit or use CUI: "The NIST SP 800–171, incorporated by reference in this final rule, establishes guidance for protecting CUI in nonfederal systems: (1) When the CUI is resident in nonfederal information systems and organizations; (2) when the information systems where the CUI resides are not used or operated by contractors of Federal agencies or other organizations on behalf of those agencies; and (3) when the authorizing law, Federal regulation, or Government wide policy listed in the CUI Registry for the CUI category or subcategory does not prescribe specific safeguarding requirements for protecting the CUI's confidentiality." The NARA CUI Final Rule makes plain the requirements for protection of CUI on non-Federal information systems and the proposed HSAR disregards that requirement.

- In addition, the HSAR regulation needs to be clear on which sections or provisions apply to Federal information systems and which apply to non-Federal information systems, as well as which standards apply to each. This must be done to avoid conflict with the combined requirements of the CUI Federal regulation (32 CFR 2002), NIST standards and guidelines, OMB policies, and ultimately, the FISMA, and to avoid sowing confusion as other agencies and contractors implement CUI requirements over the next year. In this regard, DHS must not create a parallel system to the CUI Program and impose a modified Federal Approval To Operate (ATO) process on contractors operating non-Federal information systems. Even in establishing requirements for contractors operating Federal information system for them, DHS must avoid creating needless regulatory burdens, including excessive documentation and the use of contracted assessments.

- The revisions to the HSAR must be coordinated as part of the DHS implementation of the CUI Program, per the milestones established by CUI Notice 2016-01: Implementation Guidance for the Controlled Unclassified Information Program (www.archives.gov/cui).

In conclusion, with the undermining of consistency and standardization of the handling requirements for all CUI categories, industry will be forced to cope with varying requirements set by various agencies, imposing a wasteful regulatory burden and creating a situation that the NARA CUI Program's standardization and consistency is meant to address. The costs associated with implementing these various requirements within individual companies will ultimately result in higher costs for the government and thus the taxpayer. We believe our warning of increased costs is borne out in the requirement to have parallel systems, redundant reporting mechanisms, multiple compliance schedules, required additional resources and manpower, the requirement to de-conflict contract requirements for companies supporting DHS and other agencies as well as a host of other items yet to be identified.

We thank you for the opportunity to comment and urge your consideration of the above. Please contact Michelle Sutphin at michelle.sutphin@baesystems.com (703-907-8356) if you have any questions.

Michelle J. Sutphin, ISP
NISPPAC Industry Spokesperson