PSC PROFESSIONAL SERVICES COUNCIL

The Voice of the Government Services Industry

April 8, 2013

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Ms. Honeycutt:

On behalf of the Professional Services Council (PSC), I am pleased to submit the following comments on the National Institute of Standards and Technology (NIST) Request for Information (RFI) titled "Developing a Framework To Improve Critical Infrastructure Cybersecurity" that was published in the Federal Register on February 26, 2013.[1] PSC appreciates the opportunity to comment on the cybersecurity framework that the president tasked NIST with developing in Executive Order 13636.[2] We also appreciate that NIST is seeking broad industry feedback on the development of the framework and we hope that NIST's efforts are followed by other agencies that share responsibility for implementing Executive Order 13636.

Founded 40 years ago, PSC is the voice of the government professional and technical services industry. PSC's more than 350 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 association's members employ hundreds of thousands of Americans in all 50 states.

PSC supports Executive Order 13636 because it seeks to spur efforts to improve our nation's ability to protect critical infrastructure from cyber attack or unauthorized intrusion. Of particular interest to the federal contracting industry is subparagraph 8(e) of the executive order, which requires the General Services Administration, the Department of Defense, and the Department of Homeland Security, in conjunction with the Federal Acquisition Regulatory Council, to provide recommendations to the president on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration. The recommendations will also address what steps can be taken to harmonize and make consistent existing procurement requirements related to

[1] Developing a Framework To Improve Critical Infrastructure Cybersecurity, 78 FR 13024, February 26, 2013, available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-26/pdf/2013-04413.pdf
[2] Executive Order 13636-Improving Critical Infrastructure Cybersecurity, February 12, 2013, available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

cybersecurity. We are separately working with these agencies as they develop their recommendations. Although the February 26 NIST framework RFI is not focused on subparagraph 8(e) of the executive order, we believe that several key considerations should inform both the NIST framework and in the implementation of subparagraph 8(e). For example, the effectiveness and utility of the framework and any related standards and guidance will depend significantly on the extent that the framework can (1) utilize core properties and characteristics that can be applied consistently across all federal contracting and critical infrastructure sectors and (2) provide a scalable approach responsive to the size of the relevant entity as well as its specific cybersecurity risk profile and needs. We firmly agree with NIST's stated observation in the RFI that "there are core cybersecurity practices that can be identified and that will be applicable to a diversity of sectors and a spectrum of quickly evolving threats."[3]

The development of a cybersecurity framework is a critical first step in developing workable general standards for cybersecurity and information protection. Because the final framework will likely serve as the baseline approach for cybersecurity across a broad and diverse industry segment, it is essential that it contain key attributes that can be easily replicated and incorporated in future cybersecurity efforts, particularly those focused specifically on the federal contracting community. To date, there are a number of initiatives underway within the federal contracting arena that address cybersecurity that, absent close consideration and coordination, may lead to discrepancies between the NIST framework and acquisition-related cybersecurity standards and provisions. Examples of federal cybersecurity-related initiatives under development that would apply specifically to federal contractors include:

- DFARS Case 2013-D018 – Requires reports to DoD on Penetrations of Networks and Information Systems. This rulemaking is required by Section 941 of the Fiscal Year 2013 National Defense Authorization Act,[4] which requires certain contractors to report to DoD cyber intrusions of their covered networks and information systems and allows DoD access to covered networks and information systems so that DoD can study the penetration and ascertain if DoD information may have been exfiltrated. This DFARS case is currently in the draft interim rule stage.
- DFARS Case 2012-D050 – Supply Chain Risk. This rulemaking is a result of Section 806 of the Fiscal Year 2012 National Defense Authorization Act[5] and requires the risk evaluation of information technology contractors' supply chains on national security systems. This DFARS case is currently in the draft interim rule stage.
- DFARS Case 2011-D039 – Safeguarding Unclassified DoD Information. This rulemaking seeks to provide standards and structures for the safeguarding of unclassified information. This DFARS case is currently in the draft proposed rule stage.
- FAR Case 2012-028 – Contractor Access to Protected Information. This rulemaking addresses contractor access to protected information provided by the government, generated for the government, or provided by a third party and marked by the provider to indicate that protection is required. This FAR case is currently in the draft proposed rule stage.

[3] 78 Fed. Reg. 13026
[4] P.L. 112-239
[5] P.L. 112-081

- FAR Case 2011-020 – Basic Safeguarding of Contractor Information Systems. This rulemaking addresses safeguarding of unclassified information but still requires protection from disclosure, or special handling. This FAR case is currently in the draft final rule stage.

PSC, either individually or through its affiliation with the Council of Defense and Space Industry Associations (CODSIA), has provided written comments on several of the regulatory initiatives above and we have included links to those statements for your reference.[6]

In addition to the above rules that are still in the development stage, PSC notes that DoD only recently published a final rule regarding the Defense Industrial Base Voluntary (DIB) Cybersecurity and Information Assurance (CS/IA) program.[7] PSC also provided comments to DoD on the DIB CS/IA final rule.[8]

Federal contractors that are authorized to handle federal classified info have additional control, access and reporting requirements. They are also subject to other cybersecurity and information protection requirements on a contract-by-contract basis. Requirements that contractor employees complete basic security awareness training, are subject to security clearance procedures and suitability determinations, and that contractors are Federal Information System Management Act (FISMA) compliant are a few examples of where contractors are subject to additional safeguards. Subparagraph 8(e) of the executive order and this NIST framework should address these issues. Due to the benefits of pursuing core cross-sector standards, practices and uniformity, it is important that NIST coordinate closely its framework development with GSA, DoD, DHS and the FAR Councils so that the acquisition-specific recommendations relating to paragraph 8(e) of the executive order are consistent with NIST's industry baseline efforts.

PSC strongly believes that the NIST cybersecurity framework should be developed prior to the further development or implementation of new sector-specific cybersecurity requirements for government acquisitions. PSC believes the development of the cybersecurity framework should drive acquisition requirements, not vice versa. To the extent that the individual acquisition cybersecurity initiatives contain elements that would be duplicated in a broader framework, NIST should incorporate these elements; however, acquisition-related provisions should not be included in the NIST framework solely for the purpose of ensuring that there is consistency between the framework and existing acquisition-related cybersecurity provisions.

In fact, to ensure that consistency is achievable across the framework and the federal acquisition arena, PSC recommends that the various cybersecurity initiatives underway in the FAR and DFARS be

---

[6] CODSIA Comments on FAR Case 2011-020 available at:
http://www.pscouncil.org/PolicyIssues/CybersecurityInformationProtection/CODSIA_Comments_on_FAR_Safeguarding_Contractor_Information_Systems_Proposed_Rule.aspx
CODSIA Comments on DFAR Case 2011-D039 available at:
http://www.pscouncil.org/PolicyIssues/CybersecurityInformationProtection/CODSIA_Comments_on_DFARS_Proposed_Rule_on_Safeguarding_Unclassified_Information.aspx

[7] Defense Industrial Base (DIB) Voluntary Cybersecurity and Information Assurance (CS/IA) Activities, DOD–2009–OS–0183/RIN 0790–AI60, 77 Fed. Reg. 27615, May 11, 2012.

[8] PSC Comments on DIB CS/IA Activities available at:
http://www.pscouncil.org/PolicyIssues/CybersecurityInformationProtection/Comments_on_DoD_Interim_Final_Rule_on_Defense_Industrial_Base__DIB__Voluntary_CS_IA_Activities.aspx

suspended until the initial NIST framework is completed. We will also be making this recommendation to the acquisition regulatory leadership. While PSC recognizes that NIST has little control over the implementation of ongoing DFARS and FAR initiatives, we believe that coordination with the FAR and DFARS Councils could result in greater consistency between the NIST framework and separate initiatives. As stated above, it should be the NIST framework that serves as the foundation for other government cybersecurity initiatives. Therefore, it is logical to suspend non-final FAR and DFARS initiatives until the initial framework has been established and the requirements of paragraph 8(e) of the executive order have been satisfied.

PSC appreciates this opportunity to provide input on the development of the NIST framework and would look forward to working with you, and others, as implementation of the cybersecurity executive order advances.

If you have any questions, please do not hesitate to contact PSC Executive Vice President and Counsel Alan Chvotkin or PSC Vice President of Government Relations Roger Jordan.

Sincerely,

Stan Soloway
President & CEO