GENERAL SERVICES ADMINISTRATION

[Notice-OERR-2013-01; Docket No. 2013-0002; Sequence 10]

Joint Working Group on Improving Cybersecurity and Resilience through Acquisition

AGENCY: Office of Emergency Response and Recovery, U.S. General Services Administration (GSA).

ACTION: Request for information.

SUMMARY: On February 12th, 2013, the President issued the Executive Order for Improving Critical Infrastructure Cybersecurity (Executive Order 13636). In accordance with Section 8(e) of Executive Order 13636, within 120 days, the General Services Administration and the Department of Defense, in consultation with the Department of Homeland Security and the Federal Acquisition Regulation Council, are required to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and address what steps can be taken to harmonize, and make consistent, existing procurement requirements related to cybersecurity.

Public outreach is a critically important activity for implementation of the Executive Order. In an effort to obtain broad stakeholder involvement, the General Services Administration and the Department of Defense are publishing

this Request for Information (RFI) seeking information that can be used in the Section 8(e) report.

DATES: Effective date: Submit comments on or before **[Insert 30 days after publication in the Federal Register.]**

ADDRESSES: Submit comments in response to Notice-OERR-2013-01 by any of the following methods:

- Regulations.gov: http://www.regulations.gov. Submit comments via the Federal eRulemaking portal by searching for "Notice-OERR-2013-01". Select the link "Submit a Comment" that corresponds with "Notice-OERR-2013-01". Follow the instructions provided at the "Submit a Comment" screen. Please include your name, company name (if any), and "Notice-OERR-2013-01" on your attached document.
- Mail: General Services Administration, Regulatory Secretariat (MVCB), ATTN: Hada Flowers, 1275 First Street, NE., 7th Floor, Washington, DC 20417.

Instructions: Please submit comments only and cite "Notice-OERR-2013-01", in all correspondence related to this case. All comments received will be posted without change to http://www.regulations.gov, including any personal and/or business confidential information provided.

FOR FURTHER INFORMATION CONTACT: Mr. Emile Monette, U.S. General Services Administration, at emile.monette@gsa.gov or 703-605-5470.

SUPPLEMENTARY INFORMATION:

A. Background.

On February 12th, 2013, the President issued the Executive Order for Improving Critical Infrastructure Cybersecurity (E.O. 13636) and the Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21). In accordance with Section 8(e) of Executive Order 13636 (EO), within 120 days, the General Services Administration and the Department of Defense, in consultation with the Department of Homeland Security and the Federal Acquisition Regulation Council, are required to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and address what steps can be taken to harmonize, and make consistent, existing procurement requirements related to cybersecurity. Among other things, PPD-21 requires the General Services Administration, in consultation with the Department of Defense and the Department of Homeland Security, to jointly provide and support government-wide contracts for critical infrastructure systems and ensure

that such contracts include audit rights for the security and resilience of critical infrastructure.

In order to accomplish the task required by EO Section 8(e), the General Services Administration (GSA) and the Department of Defense (DoD) have formed the "*Joint Working Group on Improving Cybersecurity and Resilience through Acquisition*," (Working Group) with GSA as the lead agency. The Working Group is comprised of topic-knowledgeable members selected from the DoD, GSA, the Department of Homeland Security (DHS), the Office of Federal Procurement Policy (OFPP), and the National Institute of Standards and Technology (NIST). The Working Group is coordinating its efforts to obtain input from the stakeholder community, including industry, academia, and federal, state, and local government.

Public outreach is a critically important activity for implementation of the EO and PPD. In an effort to obtain broad stakeholder involvement, the Working Group is publishing this Request for Information (RFI) seeking information that can be used in the Section 8(e) report. To the extent applicable, the Section 8(e) recommendations will also lay the foundation for establishment or identification of the government-wide cybersecurity contracts required by PPD-21.

The Working Group is also directly engaged with the DHS Interagency Task Force (ITF). The ITF has been established to lead implementation of the EO and PPD-21, including, among other things, stakeholder engagement. The ITF has established working groups to accomplish the major deliverables and action items required by the EO and PPD, and this RFI for the Section 8(e) report is one element of the larger outreach efforts underway to address the requirements of the EO and PPD.

The importance of common language cannot be overstated. It is apparent that a common lexicon is one of the critical gaps in harmonizing federal acquisition requirements related to cybersecurity.

Given the limitations of the unsettled definition of the word, for purposes of this RFI, the term "cybersecurity" is given a broad meaning that includes information security and related areas, like supply chain risk management, information assurance, and software assurance, as well as other efforts to address threats or vulnerabilities flowing from or enabled by connection to digital infrastructure.

In responding to the questions below, please highlight any applicable distinctions in responses related to classified and unclassified acquisitions.

FEASIBILITY AND FEDERAL ACQUISITION: In general, DoD and GSA seek input about the feasibility of incorporating cybersecurity standards into federal acquisitions. For example:

1. What is the most feasible method to incorporate cybersecurity-relevant standards in acquisition planning and contract administration? What are the cost and other resource implications for the federal acquisition system stakeholders?

2. How can the federal acquisition system, given its inherent constraints and the current fiscal realities, best use incentives to increase cybersecurity amongst federal contractors and suppliers at all tiers? How can this be accomplished while minimizing barriers to entry to the federal market?

3. What are the implications of imposing a set of cybersecurity baseline standards and implementing an associated accreditation program?

4. How can cybersecurity be improved using standards in acquisition planning and contract administration?

5. What are the greatest challenges in developing a cross-sector standards-based approach cybersecurity risk analysis and mitigation process for the federal acquisition system?

6. What is the appropriate balance between the effectiveness and feasibility of implementing baseline security requirements for all businesses?

7. How can the government increase cybersecurity in federal acquisitions while minimizing barriers to entry?

8. Are there specific categories of acquisitions to which federal cybersecurity standards should (or should not) apply?

9. Beyond the general duty to protect government information in federal contracts, what greater levels of security should be applied to which categories of federal acquisition or sectors of commerce?

10. How can the Federal government change its acquisition practices to ensure the risk owner (typically the end user) makes the critical decisions about that risk throughout the acquisition lifecycle?

11. How do contract type (e.g., firm fixed price, time and materials, cost-plus, etc.) and source selection method (e.g., lowest price technically acceptable, best value, etc.) affect your organization's cybersecurity risk definition and assessment in federal acquisitions?

12. How would you recommend the government evaluate the risk from companies, products, or services that do not comply with cybersecurity standards?

COMMERCIAL PRACTICES: In general, DoD and GSA seek information about commercial procurement practices related to cybersecurity.

For example:

13. To what extent do any commonly used commercial standards fulfill federal requirements for your sector?

14. Is there a widely accepted risk analysis framework that is used within your sector that the federal acquisition community could adapt to help determine which acquisitions should include the requirement to apply cybersecurity standards?

15. Describe your organization's policies and procedures for governing cybersecurity risk. How does senior management communicate and oversee these policies and procedures? How has this affected your organization's procurement activities?

16. Does your organization use "preferred" or "authorized" suppliers or resellers to address cybersecurity risk? How are the suppliers identified and utilized?

17. What tools are you using to brief cybersecurity risks in procurement to your organization's management?

18. What performance metrics and goals do organizations adopt to ensure their ability to manage cybersecurity risk in procurement and maintain the ability to provide essential services?

19. Is your organization a preferred supplier to any customers that require adherence to cybersecurity standards for procurement? What are the requirements to obtain preferred supplier status with this customer?

20. What procedures or assessments does your organization have in place to vet and approve vendors from the perspective of cybersecurity risk?

21. How does your organization handle and address cybersecurity incidents that occur in procurements? Do you aggregate this information for future use? How do you use it?

22. What mechanisms does your organization have in place for the secure exchange of information and data in procurements?

23. Does your organization have a procurement policy for the disposal for hardware and software?

24. How does your organization address new and emerging threats or risks in procurement for private sector commercial transactions? Is this process the same or different when performing a federal contract? Explain.

25. Within your organization's corporate governance structure, where is cyber risk management located (e.g., CIO, CFO, Risk Executive)?

26. If applicable, does your Corporate Audit/Risk Committee examine retained risks from cyber and implement special controls to mitigate those retained risks?

27. Are losses from cyber risks and breaches treated as a cost of doing business?

28. Does your organization have evidence of a common set of information security standards (e.g., written guidelines, operating manuals, etc)?

29. Does your organization disclose vulnerabilities in your product/services to your customers as soon as they become known? Why or why not?

30. Does your organization have track-and-trace capabilities and/or the means to establish the provenance of products/services throughout your supply chain?

31. What testing and validation practices does your organization currently use to ensure security and reliability of products it purchases?

HARMONIZATION: In general, DoD and GSA seek information about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition requirements related to cybersecurity and how the federal government might address those conflicts.

For example:

32. What cybersecurity requirements that affect procurement in the United States (e.g., local, state, federal, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can any such conflicts best be harmonized or de-conflicted?

33. What role, in your organization's view, should national/international standards organizations play in cybersecurity in federal acquisitions?

34. What cybersecurity requirements that affect your organization's procurement activities outside of the United States (e.g., local, state, national, and other) has your organization encountered? What are the conflicts in these requirements, if any? How can

any such conflicts best be harmonized or de-conflicted with current or new requirements in the United States?

35. Are you required by the terms of contracts with federal agencies to comply with unnecessarily duplicative or conflicting cybersecurity requirements? Please provide details.

36. What policies, practices, or other acquisition processes should the federal government change in order to achieve cybersecurity in federal acquisitions?

37. Has your organization recognized competing interests amongst procurement security standards in the private sector? How has your company reconciled these competing or conflicting standards?

DATED: May 7, 2013

Darren Blue, Associate Administrator for the GSA Office of Emergency Response and Recovery

[Billing Code: 6820-89]

[FR Doc. 2013-11239 Filed 05/10/2013 at 8:45 am; Publication Date: 05/13/2013]