Information Technology Industry Council

IT Alliance for Public Sector

April 28, 2014

Ms. Hada Flowers
General Services Administration
Regulatory Secretariat Division (MVCB)
1800 F Street, NW, 2nd Floor
Washington, DC 20405

Re: Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition [Notice-OMA-2014-01; Docket No. 2014-0002]

Dear Ms. Flowers:

On behalf of the Information Technology Alliance for Public Sector (ITAPS)[1] and the Information Technology Industry Council (ITI), [2] we are responding to the request for comments from the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition regarding the federal government instituting a federal acquisition cyber risk management strategy. ITAPS and ITI commend the General Service Administration (GSA) and Department of Defense (DoD) for continuing to engage industry and obtain broad stakeholder feedback as the two agencies seek to implement the six recommendations contained in the GSA-DoD report released January 23, 2014. ITAPS and ITI appreciate this opportunity to share our perspectives and comment on the RFI.

ITAPS and ITI support the federal government's efforts to strengthen its cybersecurity posture as it relates to acquisition planning and contract administration. Improving and strengthening our nation's cyber posture is rightly a top priority for our government and changing how the federal government integrates security into its own acquisition processes will help improve the cyber resiliency of the United States.

We share the goals and interests of the government on this issue because cybersecurity is critical for our member companies, as well. The protection of our customers, our brands, and our intellectual property

[1] The IT Alliance for the Public Sector (IT Alliance, ITAPS), a division of ITI, is an alliance of leading technology companies (including ICT companies and the defense industrial base (DIB)) offering the latest innovations and solutions to public sector markets. With a focus on the federal, state and local levels of government, as well as on educational institutions, the IT Alliance team advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more.

[2] The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading information and communications technology (ICT companies). ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. Visit www.itic.org to learn more.

1101 K Street, NW, Ste. 610
Washington, DC 20005
202.737.8888
www.itic.org
itaps.itic.org

- which are essential components of our business - is critical to our ability to grow and innovate in the future. We seek to maintain the highest levels of integrity in our products and services, regardless of

whether they are sold to commercial or government markets. Moreover, as both providers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy, and we are committed to working with the U.S. federal government to improve cybersecurity in its acquisition of goods and services.

Joint Working Group Implementation Plan Approach

a. In general, is this part of the Implementation Plan, as described, a workable approach? What, if anything needs to be added or removed?

ITAPS and ITI do not believe the Draft Implementation Plan for "Improving Cybersecurity and Resilience Through Acquisition" is focused effectively, or that the proposed approach taken by GSA-DoD in the Plan is workable. The approach incorrectly focuses on Product Service Codes (PSCs) and seeks to assign risks based on those groupings of products. Such an approach assumes that the risk is generated only in the product or service to be acquired and overlooks some of the most important identifiers of cyber risk, in particular, the criticality of the mission or program and the intended use of the goods and services acquired for the support of that mission or program.

Additionally, no plan to improve cybersecurity and resilience through acquisition can be expected to succeed without some assessment of the risks inherent in the various processes and practices that are or will be used by the government for acquisition. Some acquisition practices, like using the lowest priced item if technical specifications are met, or lowest-priced, technically acceptable (LPTA), do not support effective risk mitigation practices, and in fact, may actually increase risk. Currently, the Plan does not include such an assessment. We believe that, for the plan to be successful, it is critical that such a risk assessment be conducted at the front end of the procurement.

In short, the Plan is focused incorrectly and should be reoriented to assess how the government intends to use the goods and services to be acquired and where those goods and services will be used, which should flow from the completion of pre-acquisition, mission-focused risk assessments. Once these risks are identified, overlays can be established to guide acquisitions based on the risks in the mission or program and which would be applicable to all goods and services to be deployed in that use. Only by first understanding the intended use of goods and services sought and where those goods and services will be used can the government assess the actual goods and services it may acquire, mitigate risk, and improve cybersecurity and resilience through the acquisition and on to contract close-out.

b. Is the Plan development process adequate and appropriate to obtain stakeholder input?

ITAPS and ITI commend GSA-DoD on engaging and collaborating with stakeholders to gain input into this process. We encourage you to continue this engagement as you refine the implementation plan for this particular recommendation, as well as during the development of the implementation plans for each of the five remaining recommendations in the January 2014 GSA-DoD report.

c. What additional assumptions, clarifications, or constraints should be expressed in the Plan?

ITAPS and ITI believe the Plan must create a risk-based process that is mission-focused. The NIST Cybersecurity Framework, released in February 2014, takes such an approach and should be much more integral to the recommendations intended to be applied government wide (it is currently simply listed as one of many references). In fact, we understand the White House has directed federal agencies to use the Framework. GSA-DoD should consider using this opportunity to develop guidance for federal agencies applying the NIST Framework to help them "use business drivers to guide cybersecurity activities and [consider] cybersecurity risks as part of [an] organization's risk management processes."[3] In other words, GSA and DoD should develop government-wide recommendations as government "sector-specific guidance" in the manner in which many other sectors (such as the financial and energy sectors) currently are developing for themselves.

d. Is the approach to developing an acquisition cyber risk management adequate to achieve the goals of the recommendation?

A product and-service-centric, government-wide acquisition risk mitigation strategy has two main deficiencies. First, the product/service categories approach incorrectly assumes an extant risk associated with these categories, leaving key elements of cybersecurity unaddressed. Without understanding the context that will surround the product/service, that is, the intended use and location, government access to product/service solutions will be reduced needlessly, and the government still will lack a holistic understanding of cybersecurity risk. Second, regarding products, by assuming, simplistically, that all risks come from products, this approach wrongly and unfairly shifts the risk burden (liability) to contractors, subcontractors, and vendors, many of which, have no knowledge of, or control over, the acquisition of their products or where and how the federal government deploys them.

There are many reasons a product and service-centric approach cannot mitigate the government's cybersecurity risks. Within any product category the government could use, the number of heterogeneous products and configurations is immense. Product "categories" belie the complexity and diversity of solutions and products in the market, which are constantly changing with technological innovation. In any given category, for example, some products could be internet-enabled or others not, which impacts their overall risk. This approach also ignores how products are configured, operated, and maintained, which almost certainly would differ for each use case and customer. Further, given the rapid pace of technological change, product categories in use today may not capture products that have yet to be invented. Finally, as very recent press reports have shown, cybersecurity risks can come from unexpected places, including categories once unimaginable and others, which, heretofore, were not have been considered "risky," such as vents and soda machines. As noted by the *New York Times*, "[the] greatest cybersecurity threats can hide in the unlikeliest of places."[4]

A separate, potentially negative consequence of the product and service-centric approach is unrelated to the federal government's cybersecurity risks, but extremely important. Specifically, use of this approach would communicate to other governments that the U.S. government believes cybersecurity, first and foremost, is based on products and services. U.S. industry, with the help of the U.S. government, has spent the past decade working to counter other governments' claims or beliefs that they can improve their own cybersecurity using product- or service-focused approaches. We have argued, with varying degrees of success, that cybersecurity must be based on risk management. Given

[3] *Framework for Improving Critical Infrastructure Cybersecurity Risk*, Version 1.0, p. 1.
[4] Hackers Lurking in Vents and Soda Machines, *New York Times*, April 7, 2014

the international interest in U.S. approaches, GSA-DoD should endeavor to develop policies that can be implemented with minimal disruption to the global marketplace.

ITAPS and ITI agree the government needs to develop an acquisition cyber risk management strategy to achieve the goals of the recommendations. The proposed product and service-centric approach, however, is not adequate for this purpose. To achieve the goals of the recommendation, the government should instead focus on a mission-specific risk-based approach to define and determine what steps must be taken to assure the products and services deployed in each program or mission area are consistent with their intended use.

e. Are the major tasks and sub tasks appropriate and will accomplishment of them result in achievement of the outputs/completion criteria identified?

Because we believe the proposed taxonomy approach is not the correct approach, we cannot support the related major tasks and sub-tasks.

f. Can the Category definitions and Taxonomy identified in Appendix I be used to develop Overlays?

ITAPS and ITI strongly disagree with using the category definitions and taxonomy identified in Appendix I to help develop any overlays. As we explained in our response to *Question b*. above, this approach will not improve the government's cybersecurity and resilience through acquisition.

i. If not, what further categorization/sub-categorization needs to be done to identify Categories that are "right-sized?"

As explained above, an approach using a product service code centric analysis would leave users to assume incorrectly that they have addressed risk by examining products and services grouped by product service codes. Such a risk mitigation plan ignores the more important risk assessment.

To understand, manage, and mitigate cyber risk government-wide, the government needs to account for the following:

- The inherent nature of a product – The development process and/or process controls employed and the technological functions of a product affect the risk associated with that product

- The intended use of a product – A product used for purposes other than those intended can open the door to cyber risk. Understanding the use for which a product is intended requires user competence in the product itself, including an overall knowledge of the technology involved (including its limits), an understanding of the system in which it will be deployed, an understanding of how that system relates to an agency mission, and an understanding of how the product's intended use should align with the agency need being fulfilled.

- People compliance – People must adhere to agency protocols around the use of technology. This adherence involves not only cybersecurity procedures, such as

authentication protocols, but also the procedures that could impact cybersecurity, such as acquisition procedures and physical security procedures.

- Organizational compliance – Organizations must demonstrate leadership, identifying changes in the risk universe and aggressively enforcing people compliance.

- Anticipated product technology evolution/utilization – A technology that is anticipated to evolve rapidly and/or enjoy immediate infusion into government networks may require more scrutiny than a mature product. Again, however, any decisions in this regard must be made in an overall risk management context. In some cases, a mature product that supports a very critical agency mission could attract more risk (*e.g.*, interest from bad actors) than a newer technology that supports a less critical mission.

- Chain of custody – In the course of delivering a product to the government, each change of hands represents a potential risk point, as does any modification of the product at the point of delivery. Products purchased from non-authorized sources (the topic of another recommendation in the January 2014 GSA-DoD report) are likely to pose a greater risk than those purchased through legitimate channels. This issue, again, has implications for processes that impact cybersecurity, like acquisition and workforce training.

Because no entity, including the federal government, can achieve zero cyber risk, the forgoing considerations (and there may be others) imply that cyber risk mitigation is multi-faceted. Despite this, the GSA-DoD Plan does not include a multi-faceted approach today.

ii. Is there a Taxonomy and Category definition used by your organization (or market segment) in its own procurement activity that the government might adopt? How does it relate to the Taxonomy in Appendix I?

Notwithstanding any taxonomy that may be used by companies, it must be noted that they do not rely solely on product categories for purposes of assessing and assigning risk without understanding a wide array of other factors.

g. Assuming the comparative Category risk assessment will be comprised of three elements – threat, vulnerability and impact – what factors of each element should be used to conduct the assessment?

ITAPS and ITI suggest the government focus on programs' mission areas and acquisition practices. Using product service codes does not take into consideration how the product or service will be used and therefore cannot provide a full picture of threats, vulnerabilities, and impact.

h. Other than cyber risk, what, if any, other aspects of a Category (e.g., annual spend) should be considered in development of the prioritized hierarchy of Categories?

As stated in our responses above, the government must conduct risk management based on the mission and use of the product or service. Using levels of annual spend as part of a risk assessment rooted in PSCs furthers the artificial impression that cyber security can be achieved by narrowing a product-focused assessment onto those products that incur a higher annual spend than others. Both the focus

on PSCs and on annual spend are faulty for purposes of determining cybersecurity risk and will not provide the assurance the government seeks through this exercise.

i. In addition to information security controls derived from the Cybersecurity Framework and other relevant NIST guidance and international standards, what other procedural or technical safeguards that address business cyber risk should be included in the Overlays (e.g., source selection and pricing methodology, source selection evaluation criteria minimum weighting and evaluation methodology, etc.)?

As stated above, the government must conduct an assessment of the acquisition practices and processes used to obtain goods and services, including source selection, pricing methodology, and evaluation criteria in order to effectively use acquisition to mitigate cybersecurity risk. We also believe the NIST Framework should be much more prominently featured in a new risk management approach being developed by GSA-DoD.

Conclusion

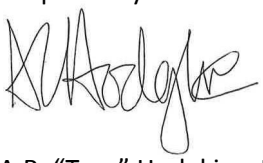
As stated above and in the accompanying visualization below (Figure 1), we believe the government should abandon any product service category (PSC)-based approach to determining risk. Instead, the government should focus on the means used to acquire goods and services (how), the intended use of the goods or services and the risks in each mission or program area where the goods and services will be deployed (where), which should be based on mission-focused risk assessments. Only by understanding these important risk variables can we establish appropriate protocols to effectively improve cybersecurity and resilience through acquisition.

Figure 1

Thank you again for the opportunity to respond to this request for information and share our viewpoints. We look forward to working with GSA-DoD as you refine this implementation Plan, and we are available at any time to elaborate on our response and/or work with GSA-DoD on mapping out an

alternative approach as we have suggested (based on agency mission/risk management). We also look forward to commenting on the future RFIs you will issue to develop plans to implement the remaining five recommendations contained in the January 2014 GSA-DoD report. Should you have any questions regarding these comments, please feel free to contact Pamela Walker, Senior Director of Homeland Security at (202) 626-5725 or pwalker@itic.org.

Respectfully submitted,



A.R. "Trey" Hodgkins, III
Senior Vice President, Public Sector

Danielle Kriz
Director, Global Cybersecurity Policy