COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
703-875-8059

April 28, 2014

Ms. Hada Flowers
General Services Administration
Regulatory Secretariat Division (MVCB)
ATTN: Ms. Flowers
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 Council of Defense and Space Industry Associations (CODSIA)[1], 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. We 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. CODSIA appreciates this opportunity to share our perspectives and comment on the RFI.

CODSIA supports 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 process will help improve the cyber resiliency of the United States. Cybersecurity is critical to our companies as well—the protection of our customers, our brands, and our intellectual property are essential components of our business and 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. We share the goal of improving cybersecurity and, therefore, our interests are fundamentally aligned. As both providers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity

[1] CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of seven associations – the Aerospace Industries Association (AIA), the American Council of Engineering Companies (ACEC), the Information Technology Alliance for the Public Sector (ITAPS), the National Defense Industrial Association (NDIA), the Professional Services Council (PSC), TechAmerica, and the Chamber of Commerce of the United States. CODSIA's member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

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?

CODSIA does not believe that the plan is effectively focused or that the proposed approach taken by GSA-DoD in the Draft Implementation Plan for "***Improving Cybersecurity and Resilience Through Acquisition***" is a workable one. 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 – 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 and we would offer that it is critical to the success of this plan that it should be conducted at the front end of the implementation process.

In short, the plan is incorrectly focused and should be reoriented to assess HOW the government will be acquiring goods and services and WHERE they will be used, which should flow from mission-focused risk assessments done before anything is even acquired. Once these risks are identified, overlays can be established to guide acquisitions based on the risks in the mission or program and would be applicable to all goods and services to be deployed in that use. Only by looking at these questions, instead of focusing on WHAT the government may acquire, can we effectively assess risk and improve cybersecurity and resilience through acquisition.

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

CODSIA commends GSA and DoD on collaborating, meeting, and engaging with stakeholders to gain our input into this process. We encourage you to continue this process 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?

CODSIA believes 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 GSA-DoD work (it is currently simply listed as one of many references). In fact, we understand that the White House has directed federal agencies to use the Framework. GSA-DoD should consider using this opportunity to develop guidance on how federal agencies should "use business drivers to guide cybersecurity activities and considering cybersecurity risks as part of [an] organization's risk management processes."[2] In other words, GSA and DoD should develop "sector-specific guidance" in the manner in which many other sectors (such as the financial and energy sectors) are currently developing such tailored guidance for themselves.

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

A product-service-centric government-wide acquisition risk mitigation strategy has two main deficiencies. First, the product service categories approach focuses wrongly on categories that do not in and of themselves relate to cyber risks, and by focusing on the wrong things, leaves key elements of cybersecurity unaddressed. Second, by assuming that all risks come from products, this approach wrongly shifts the risk burden to vendors and contractors, many of which have no knowledge of or control over where or how the federal government deploys their products.

There are many reasons a product-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 of solutions and diversity of 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 would almost certainly differ for each use case and customer. Further, given the rapid pace of technological change, product categories we 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 ones for which we doubt GSA/DoD would have thought two weeks ago to put in a "risky" category, such as vents and soda machines. Per an article in the *New York Times*, "[the] greatest cybersecurity threats can hide in the unlikeliest of places."[3]

A separate potential negative consequence of the product-service-centric approach, unrelated to the federal government's cybersecurity risks but also extremely important, is the signal it would send to governments around the world that the U.S. government believes that cybersecurity is first and foremost based on products and services. U.S. industry, with the help of the U.S. government, has spent the past few years trying 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. It is imperative that GSA-DoD keep the international audience in mind in its guidance and develop policies that are workable globally.

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

CODSIA agrees that the government needs to develop an acquisition cyber risk management strategy to achieve the goals of the recommendations; however, the proposed product-service-centric approach is not adequate for this purpose. In order 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.

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?

CODSIA strongly disagrees 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 incorrectly assume 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:

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

- <u>The intended use of a product</u> – A product used for other purposes than 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, how that system relates to an agency mission, and 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 of processes that could impact cybersecurity, such as acquisition 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.

Because no entities, 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 recommendation 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?

CODSIA suggests that 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.

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, we believe the government should abandon any product service code-based approach to determining risk and instead focus on the means used to acquire goods and services (HOW) and understanding 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.

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.

In the interim, if you have any questions or need any additional information, please do not hesitate to contact Trey Hodgkins, Senior Vice President at ITAPS, who serves as the CODSIA project officer for this case, or Bettie McCarthy, CODSIA's administrative officer. Bettie can be reached at (703) 875-8059 or at codsia@pscouncil.org.

Respectfully submitted,

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

R. Bruce Josten
Executive Vice President, Government Affairs
Chamber of Commerce of the U.S.

Rachel S. Wolkowitz

Rachel Wolkowitz
Assistant General Counsel
TechAmerica

Mark Steiner

Mark Steiner
Senior Director, Federal/International
Programs
American Council of Engineering Companies

Alan Chvotk

Alan Chvotkin
Executive Vice President & Counsel
Professional Services Counsel