April 28, 2014

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

RE: Information Technology Sector Coordinating Council (IT SCC) comments in response to Notice OMA-2014-01, for the Draft Implementation Plan for Improving Cybersecurity and Resilience through Acquisition, Version 1.0

Dear Ms. Flowers:

Thank you for the opportunity to provide comments relating to the implementation of the recommendations contained in the Final Report of the Joint Working Group on Improving Cybersecurity and Resilience through Acquisition issued by the Department of Defense (DoD) and General Services Administration on January 23, 2014.

We recognize the considerable efforts of the DoD and GSA to involve industry in the development process and appreciate the commitment to a collaborative approach for this important effort. As the designated Information Technology (IT) Sector industry representative body to the U.S Government for critical infrastructure and cybersecurity policies and practices, the IT SCC strongly supports the government's efforts to improve the security of cyberspace. IT SCC member companies deliver products and services used by consumers, enterprises, and governments around the world, and many also provide IT security-related solutions and services, so we understand the serious nature of cyber security threats and we are committed to working with our industry and government partners, including the U.S. Government, to help address those threats.

General Comments on the Draft Implementation Plan

Foremost, we understand the reasoning behind the selection of Recommendation IV of the Report, "*Institute a Federal Acquisition Cyber Risk Management Strategy*" as a starting point for implementation. Beginning with this recommendation provides a foundation and general framework for subsequent recommendations to be implemented. We caution, however, that the Draft Implementation Plan must focus on the following issues if any resulting policy is to be effective and sustainable.

Specifically, the IT SCC recommends that this risk framework should focus on the following items:

- Properly identifying risks, evaluate these risks both for probability of occurrence and impact of occurrence, as well as identification of appropriate measures to mitigate against identified threats, vulnerabilities, and consequences.

- We also believe that it is essential that any new requirements are harmonized with FISMA, FIPS, FedRamp, and other existing security frameworks so as to avoid conflicting requirements.

- Consider the global nature of the IT supply chain and the economic impact to both the purchasing agencies and suppliers. The complexity and geographic diversity of the global IT supply chain will make implementation of some SRCM policies challenging to impose. Specific requirements for suppliers will also add additional cost, which will affect the purchase price of IT products that the Government purchases. Any policy requirements should be sensitive to both the application of risk management practices for specific IT purchases, as well as the cost impact of specific requirements that may be proposed.

- Follow a technology neutral approach. While it is acceptable for procurement policies to specify security objectives, the decisions regarding how to meet those objectives, including what technologies to use or how and where to build them, must be left up to the vendor that would like to sell to a government entity. We urge GSA expressly state in all policy documents that any new requirements for cybersecurity standards will be technology neutral.

- Avoid requirements on county of origin. Security is a function of how a product is made, used, and maintained, not where it is built. We caution strongly against any procurement approach that would mandate where ICT products are built or what country they come from. Policies should instead focus on the conformance of a product to a recognized security assurance standard or on the standards, processes, and policies followed during product development.

- Recognize current industry standards and best practices. U.S. ICT companies contribute to developing such standards on a global, voluntary, and consensus-based basis through a range of organizations including formal standards development bodies as well as consortia and alliances.

- Avoid selecting a single standard. It is important to stress that there is no single standard or set of practices is applicable across the board for the IT industry. Cybersecurity risk management is complex, including many different types of technologies, global supply chains, and a large number of different and evolving standards. Risk management policies should be sensitive to these facts and accept multiple standards and industry best practices as part of a comprehensive supply chain risk management policy.

- Adopt specific requirements for Government agencies to purchase only from authorized sellers and resellers. Despite ongoing warnings from government, industry, and academic reports, the U.S. Government continues to purchase products and services from unauthorized sources to reduce cost and conserve resources. Cost savings is important, but evidence suggests that buying from unauthorized sources increases risk that the government may receive counterfeit, tainted, or even malicious equipment. The Government should consider a government-wide policy that requires purchasing from trusted and authorized sources, and if there is a compelling

case to acquire outside of that domain, such information should be documented in a Justification and Authorization and approved by a Designated Approving Authority.

Response to RFI Comment Framework and Questions

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

The IT SCC is concerned that the approach taken does not establish a workable framework for risk assessment and management. The approach focuses on Product Service Codes (PSCs) and seeks to assign risks based on those groupings of products, which assumes risk is generated only in the product or services 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.

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

IT SCC commends GSA-DoD for their efforts to build a collaborative approach, and encourages that the process continue for this recommendation and the remaining recommendations contained in the January 2014 GSA-DoD report.

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

IT SCC encourages GSA-DoD to focus on creating a risk-based process that focused on the missions to be performed and aligns with other federal and industry standard risk management practices and categories. The NIST Cybersecurity Framework, released in February 2014, provides specific guidance that should be taken into account, as do current FIPS polices.

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

By focusing on products for risk assessment and mitigation, the policy fails to address user-based risks that must be part of a comprehensive cyber security risk management program. In addition, 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.

IT SCC agrees that the government needs to develop an acquisition cyber risk management strategy to achieve the goals of the recommendations. The proposed product-service-centric approach, however, will not be effective as currently outlined in the draft implementation plan. To achieve the goals of the recommendation, the government should 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, and also be appropriately harmonized with existing risk management efforts (e.g., FIPS, FedRAMP).

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

See specific comments above and in the next section. Because we believe the proposed taxonomy approach needs to be redefined, we believe the following major tasks and sub-tasks must be redefined.

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

IT SCC disagrees with using the category definitions and taxonomy identified in Appendix I to help develop any overlays. Please refer to our response to Question d.

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

The current draft approach based on a Product Service Code (PSC)-centric analysis would leave users to incorrectly assume they have addressed risk by examining products and services grouped by product service codes. This approach ignores the risk assessment requirements needed to determine which missions and operations are at the greatest risk, as well as how to address those specific risks.

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

- The design and development a product or service - The development process and/or process controls employed during the design and development phases of production, as well as the technological functions of a product or service affect the potential risks associated with that product, and so should be considered as part of an effective risk assessment system.

- The intended use of a product or service – A product or service 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 or service itself, including an understanding of the agency mission, how a system relates to an agency mission, an understanding of the environment in which the system will be deployed, an overall knowledge of the technology involved (including its limits), and an understanding of how the product's or service's intended use aligns 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. 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 or service 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 completely eliminate cybersecurity risks, the forgoing considerations (and others) demonstrate that cyber risk mitigation requires a multi-faceted approach. To be effective, the GSA-DoD implementation plans must reflect a multi-faceted approach.

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?

IT SCC recommends that the focus should be on the mission areas and acquisition practices of a program. Relying on 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.

Specific Comments on the Draft Implementation Plan Tasks and Sub Tasks

Major Task 1

Sub Task 1.a. Determine Taxonomy and Establish Category Definitions

IT SCC Comments: As stated above, relying on PSCs is an ineffective model that does not fully articulate or address risks, and this approach needs to be redesigned to focus on how the government will acquire products and services, and where they will be deployed. In addition, when developing a new taxonomy for this effort, it is important to avoid introducing confusion and duplication with regard to existing taxonomies, including those described by the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) Special Publications, and the CERT Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method. The new taxonomy should seek to harmonize these models to the extent possible, rather than risk adding duplication and complexity to an already complex system.

The overall approach, as defined in taxonomy, is the first step and should be completed before specific categories of IT products and services, as well as associated or IT-dependent products and services can be accurately defined.

Sub Task 1.b. Conduct Spend Analysis

IT SCC Comments: Determining costs associated with specific cybersecurity risks for specific categories of IT products and services, as well as associated or IT-dependent products and services, is a critical component for the final Implementation Plan. To conduct the spend analysis categories will first need to be defined based on the taxonomy of cyber security risks that has yet to be developed. For this reason, the spend analysis should follow the establishment of the taxonomy and set of specific category definitions.

Once the taxonomy and category definitions are established, the next step is to determine the objective criteria for making a determination as to which categories should be subject to increased requirements for supply chain risk management. The current Draft Plan, however, indicates that determination should essentially be based on the answer to the question, "Does this category present cyber risk to any possible end user." We believe that a complete set of objective determination criteria should be developed following the establishment of the taxonomy, and subsequent definition of individual product and service categories.

Major Task 2: Conduct Acquisition Risk Assessment and Prioritization

IT SCC Comments: The Acquisition Risk Assessment and Prioritization should first be designed in conjunction with the development of an appropriate taxonomy approach as noted in our responses above.

Major Task 3: Develop Methodology to Create Overlays

IT SCC Comments: The development of a methodology to create overlays should follow the establishment of Major Tasks 1 and 2. In addition, all work associated with Major Task 3 should be harmonized with other existing cyber risk management efforts, including NIST Special Publication 800-161, FedRamp, and other existing overlays. IT SCC believes it is important to understand how these instruments may be used before developing yet another set of overlays.

Sub Task 3.a. Determine Appropriate Security Controls

IT SCC Comments: The development of appropriate security controls should follow the establishment of Major Tasks 1 and 2.

Sub Task 3.b. Determine Appropriate Acquisition Mitigations

IT SCC Comments: The development of appropriate acquisition mitigations should follow the establishment of Major Tasks 1 and 2.

Sub Task 3.b. Determine Appropriate Other Safeguards

IT SCC Comments: The development of appropriate "other" safeguards security should follow the establishment of Major Tasks 1 and 2.

Again, thank you again for the opportunity to provide comments on the Draft Implementation Plan. As our comments demonstrate, we believe that a significant amount of progress has been made in developing a collaborative process by which government and industry can work to address SCRM issues. We also believe, however, that there is considerable work that needs to be done to create a responsible, practical, and sustainable SCRM plan for certain US Government Acquisitions. We look forward to continuing to work with you on the development of this plan.