Information Technology Industry Council

May 9, 2013

Emile Monette
Senior Advisor
Office of Acquisition Management
Federal Acquisition Service
General Services Administration

RE: ITI comments in response to GSA RFI Notice-FAS-2013-01: Improving Cybersecurity and Resilience through Acquisition

Dear Mr. Monette:

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to GSA's RFI Notice-FAS-2013-01: Improving Cybersecurity and Resilience through Acquisition.

ITI is the premier voice, advocate, and thought leader in the United States for the information and communications technology (ICT) industry. ITI's members comprise the world's leading technology companies, with headquarters worldwide. Most service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. Supply chain security is critical to us—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. Cybersecurity is rightly a priority for all governments. We share the goal with governments 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 policy. We acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with—and drive—global norms.

ITI commends the President for directing GSA and DOD, in consultation with DHS and the Federal Acquisition Regulation (FAR) Council, to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration and what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity. We also appreciate GSA's commitment to public outreach in this process, particularly given the extremely short time frame. However, industry engagement should continue well beyond the issuance of GSA's final report. The time frame in which GSA is developing this report is recognized both by GSA and industry as exceedingly fast and we believe it does not allow for full exploration of all of the issues raised or for meaningful industry input. It is especially unfortunate that the timeline requires GSA to write its draft report before the RFI period will end and all industry responses are received. Thus, it is imperative that this be the start of long-term engagement with industry throughout the policy development process and implementation.

As a trade association, we cannot answer many of the organization-specific questions in the RFI. We have copied below in bold those questions to which we are responding. In addition to

answers to those questions, immediately below we list some guiding tenets we think GSA's recommendations should include. We elaborate on these in our answers to the questions.

Guiding tenets for GSA's recommendations

Any new procurement policies should:

- Be globally compatible/draw from global standards.
- Be technologically neutral.
- Be harmonized across federal agencies to the extent possible.
- Be harmonized with ongoing updates to FISMA.
- Be based on a set of reasonable industry practices and product assurance standards.
- Avoid any new government-specific accreditation regime, including third-party accreditation.
- Increase expertise on the government side.
- Be based on risk management.
- Be simple and streamlined.
- Carefully examine whether the "lowest cost technically acceptable (LCTA)" approach makes sense for all procurements.

Feasibility and federal acquisition

In general, DoD and GSA seek input about the feasibility of incorporating cybersecurity standards into federal acquisitions.

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?

We appreciate that GSA is looking at incentives, particularly given current budget restraints. There are a number of incentives—many of which we do not believe would add substantial costs—the government could provide to vendors and to their products and services that comply with global industry standards. These include:

- Expediting of necessary security clearances for designated points of contact in industry where such clearances are needed;
- Simplifying and expediting contracting;
- Greater flexibility to allow for upgrades without whole new assessments if the upgrade is built by the original vendor;
- No blacklisting of vendors for security concerns without the ability of the vendor to address the perceived concerns; and
- Better positioning as trusted vendors.

Any incentives that are instituted should be consistently adopted so that readily available waivers will not reward companies and their products and services that do not comply with global

industry standards. Incentives also must be steady and predictable so that companies can factor them into their decisions to participate in government contracts.

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

We agree with the importance of security assurance. However, no new government-run certification and security testing regimes should become part of new acquisition requirements. Many ICT providers adopt security practices and have a variety of methods of conveying those practices to their customers. These may range from attestation, to having products certified against global standards, to having their processes accredited against global standards. Not only would new government-run regimes be redundant with these processes, but they would likely add cost and bureaucracy with no demonstrable impact on security. To the extent that certifications or accreditations are to be required, they should only be to existing global certification or accreditation regimes already used by industry to attest to global standards (e.g. certification to ISO/IEC 15408 [the Common Criteria standard], to ISO/IEC 27000, or any other global standards necessary for the procurement in question).

Continuing to rely on existing, market-driven global conformity assessments related to cybersecurity risk management has key benefits:

- It allows for the conformance assessment industry to move at a pace more closely tied to the pace at which threats develop and at which industry designs, develops and implements solutions that respond to these threats.
- There are standards for how to appropriately conduct conformity assessment that are based on global consensus and are globally deployed.

Rather than developing a new conformity-assessment scheme, we recommend that GSA seek an approach that allows for company attestation/ evidence of their security assurance practices in conformance to global standards, or to their products' conformance to global assurance standards. This would focus on reasonable accountability and how companies can demonstrate accountability. For example, government procurement should more frequently leverage certifications of product conformance with the Common Criteria. In addition, the ICT industry could explore with the government if there is a way for companies to convey—in a manner acceptable to government purchasers—how ICT companies practice security assurance. To be successful, an attestation approach may need to be paired with limited liability protections. These are questions and parameters the ICT industry would welcome exploring with GSA and its interagency partners.

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

There are a number of key factors that can help to improve cybersecurity in acquisition planning and contract administration.

Make a clear delineation between COTS and custom/GOTS. For the most part, acquisitions of ICT products for federal systems rely on commercial-off-the-shelf (COTS) products, rather than

government-off-the-shelf (GOTS) and custom products. That is certainly true for non-national security systems (NSS), but it is also true for many NSS. It is important for global ICT companies to serve the federal marketplace by adopting sound security practices that make sense for the global marketplace. While certain customers may have specific functional or security needs that require them to have recourse to custom and GOTS solutions, these should be exceptional. Security requirements that apply across the board should be based on global commercial standards and best practices.

Base any requirements on risk management. Security is not an end state. Rather, it is a means to achieve and ensure continued trust in various technologies that comprise the cyber infrastructure. Cybersecurity efforts must facilitate an organization's ability to properly understand, assess, and take steps to manage ongoing risks in this environment—taking measures appropriate to the value and consequences of the information in question. Federal agencies must be able to properly assess and mitigate risk appropriate for their infrastructures and risk tolerance models, and implement policies based upon thoughtful, ongoing risk management assessments.

A risk framework should focus on properly assessing, managing, and mitigating potential security risks, which comprise threats, vulnerabilities, and consequences and can include people and processes—not just technology. A risk framework also should reflect a role for all participants in the purchasing ecosystem that can contribute to risk management, including purchasers and users.

Align any new requirements with FISMA. Industry and government have invested significant resources into FISMA. It is essential that any new requirements are harmonized with FISMA so as to avoid any conflicting requirements.

Follow a technology neutral approach. While it is acceptable for procurement policies to specify security objectives, the decisions regarding how to meet those objectives (such as what technologies to use or how or where to build them) must be left up to the vendor that would like to sell to a government entity. We urge GSA to ensure that any new requirements for cybersecurity standards be technology neutral. This will ensure that no specific technology is wrongly consecrated as a requirement, and instead that technology providers and users focus on managing risk and selecting specific security measures, including specific technologies, among a continuously evolving panoply of competing solutions. This also will preserve and promote our industry's ability to innovate, which is critical to ensuring that our industry remains globally competitive—further strengthening cybersecurity.

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.

Avoid pointing to just one standard. It is important to stress that there is no one "cybersecurity standard" or set of practices that is applicable across the board. Cybersecurity risk management

is complex, including many moving parts, responsible parties, and standards. In addition, the global ICT industry continually establishes new standardization efforts addressing emerging cybersecurity risk concerns.

Overall, the ICT industry uses a range of global standards. 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. Examples include:

- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- 3rd Generation Partnership Project (3GPP)
- World Wide Web Consortium (W3C)

In general, the most effective standards place emphasis on risk management, governance, and good ICT service management, and allow individual companies to adjust and refine the security and control objectives and implementations based on business methods, technology architectures, and risk management approach. ISO/IEC standards are particularly helpful because they offer methodological approaches to assessing and managing risk, rather than prescriptive responses or technical solutions. We caution against any approaches that prescribe specific technical implementations to apply controls.

Below we provide some examples of recognized, global security-related standards developed and used by our member companies. While not exhaustive, the standards below illustrate a range of options used or that are in development. Note that not all ITI companies use or intend to use all of these standards. The ones a particular company chooses to use depend on the company's products, services, markets, and business methods.

- ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation (CC)) is the global standard for computer security certification. The CC is based on the ISO/IEC standard and is a multi-lateral agreement – the Common Criteria Recognition Arrangement (CCRA) - among 26 countries including the United States, Japan, the United Kingdom, Australia, Germany, Korea, and India.
    - Note that 3GPP has begun to address the issue of security assurance standards and has chartered its security group, SA3, to develop a suitable methodology for mobile network security assurance. This work is still in progress, but is moving towards re-using Common Criteria methodology to define appropriate security assurance criteria for mobile networks. Once a security methodology is agreed upon, SA3 will likely begin work to produce a collaborative Protection Profile (cPP) that would be used for security compliance of mobile networks.
- ISO/IEC 27000 series is a security control framework that provides a globally recognized baseline set of control objectives and controls statements with supporting guidelines and risk management framework to provide conformity among organizations' security policies. As security automation improves, control frameworks can be used to manage

security requirements and reporting across and between organizations. This combination of consistent reporting on automated controls will only increase in importance.
    - ISO/IEC 27034 is appropriate for application security.
    - ISO/IEC 27036 is an emerging standard for supply chain security that will have four parts for information security for supplier relationships.
- ISO/IEC 28000 is the specification for security management systems for the supply chain.
- The Open Group Trusted Technology Forum (OTTF) is an industry-led global standards initiative that aims to shape global procurement strategies and best practices to help reduce threats and vulnerabilities in the global supply chain. In April 2013 OTTF released The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0 and is developing what is planned to be a global voluntary accreditation program that will assess conformance to the standard and accredit those that conform.

Avoid basing new requirements entirely on the FedRAMP model. We understand that, in its industry outreach on this work, GSA has asked if existing government acquisition processes, such as FedRAMP, could be a model for "standardized information/cyber security procurement/ supply chain/acquisition decision making." We believe aspects of FedRAMP have improved the federal government's ability to efficiently and effectively adopt cloud services. However, the FedRAMP model has significant limitations and should not be applied to ICT procurement broadly for the following reasons.

- FedRAMP currently applies to all cloud services offered to the Federal Government. Certification should not similarly be required for all ICT products made by vendors selling to the government. While a certification regime may make sense for the highest risk national security systems, a broader certification program for mid- or low-risk systems would create excessive and unnecessary costs and delays.
- FedRAMP includes third-party assessment. As we discuss in our response to Question 3, GSA should not create any new, government-specific accreditation program, including third-party assessments.
- The FedRAMP process can unnecessarily delay the deployment of effective and cost-efficient technologies.
- FedRAMP's restrictive requirements in many times raise costs and limit innovation and competition, preventing the federal government from timely procurement of leading-edge products.

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

While some of the ICT sector's products are sector-specific (i.e. an ICT solution developed specifically for the management of a power generation system), most are not. The same databases, routers or processors are used by companies in the public, retail, defense, power, transportation, tourism, and other sectors. Whether its products are sector-specific or not, a COTS ICT vendor will generally use the same design, development and manufacturing processes and practices. Therefore, these products do not comply with different and divergent product

assurance standards. Instead, they comply with and are evaluated under cross-sectoral product assurance standards. That is not to say that ICT vendors do not obtain sector-specific conformity assessments for products that have sector-specific uses. However, the corresponding standards do not prescribe the manner in which the products are developed, but rather what sector-specific technology features and functionalities they include.

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

The government should base any new requirements on global, industry-developed, consensus security standards, as we elaborate in our response to Question 33, below.

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

We understand that one of the recommendations GSA is considering putting in its report is that the government:

1) Break government IT spending into distinct categories (bands);
2) For each category, conduct a government-wide cybersecurity risk assessment in an objective way (threats, impacts), and use these assessments to rank the categories in terms of prioritization for higher security controls.
3) Overlay security for each category by defining the minimum (and maximum) security standards/controls that should be applied to that category.

We are preliminarily supportive of this approach, but have the following observations and recommendations.

- Given that each category may have its own set of standards and controls, the number of categories should not be too numerous. Rather, there should be a limited number of broad categories. This will ensure the markets remain large enough to incentivize industry to sell into them.
- At the same time, the categories should not be so broad that is impossible to apply appropriate and targeted standards/controls.
- Security for each category must truly be consistent across the federal government so that vendors can determine the ROI on pursuing business.
- For a category-type approach to be successful, GSA should focus first on setting new requirements on just one category of systems, as opposed to trying to do all categories at once.
    - GSA should first focus on agencies' mission-critical IT systems.
- Risk assessments should leverage the risk assessments already undertaken by the federal government under NIST 800-30, *Guide for Conducting Risk Assessments.*
- GSA should consider how government-wide acquisition contracts (GWACs) might be affected by the stratification of purchasing categories/application of standards to each category.

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?

We understand that, in its industry outreach on this work, GSA has asked "Current government practice dictates that acquisition officers often make acquisition decisions, rather than risk owners. 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? If you were to centralize the cyber security acquisition decision-making across the government enterprise, would what it look like?" Further, GSA has stated that its draft report may recommend that U.S. Government cybersecurity experts be engaged throughout procurements, including pre-solicitation (to make sure security needs are included in RFP requirements) and prior to award (to ensure the apparent winner adequately meets the security requirements in the RFP), and possibly post-award engagement.

We support the involvement of cybersecurity experts more fully in government procurement in this regard. We would appreciate clarification of where the experts would sit (if each agency would have its own individual or cadre of individuals, or if there would be an interagency group that advises all agencies).

Regardless of structure, we have the following recommendations:

- Any security-related input these experts provide into procurements must be consistent government-wide, and be harmonized with the training and agency comparison requirements of the Clinger-Cohen Act. Experts also should receive standardized training, apply consistent assessments, and provide consistent input across agencies to contracts, awards, and post-award engagement. This should include coordination between the Administrator for Federal Procurement Policy, the Chief Information Officers Council, and the Federal Acquisition Institute. If GSA ultimately decides, as it is considering, to recommend breaking federal IT acquisitions into segments that have different risk levels and thus different security control overlays, then there should be consistency within each segment.
- One option is for agencies' chief information security officer (CISO) staff to work more closely with contracting officers.
- Cybersecurity experts should be a layer of oversight in addition to—not instead of—adding security as a parameter in contracts.

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

We would like to take this opportunity to advise against a certain approach that we have seen in some federal policies, namely excluding vendors or their products from procurements for perceived security risks without informing vendors of their exclusions or allowing them to address the perceived risks.

Recent laws, such as Section 310 of the FY2012 Intelligence Authorization Act and Section 806 of the FY2011 National Defense Authorization Act (NDAA), included such provisions that

provided the federal intelligence community new powers to exclude from procurement those IT products in the supply chain that the community believes would endanger national security. Further, these provisions enable the intelligence community to blacklist companies without any notification to such companies of their designation.

This approach can unintentionally but negatively impact affected companies, could preclude suppliers from being able to mitigate supply chain risks (because they may not know what they are) and could, if the proposals are emulated by other governments, then impede U.S.-based IT companies' ability to compete in the global marketplace.[1]

If the federal government believes that a vendor or its products would introduce unacceptable risks so that the vendor should be disqualified from a procurement, the vendor should be:

1) Given notice of disqualification;
2) Provided information as to why they were disqualified;
3) Given the opportunity to remediate the issue or take corrective action and;
4) Be given the opportunity to re-apply.

Commercial practices

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

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

Commonly used commercial standards are sometimes specified as part of federal requirements for specific technologies, or they may serve as models or proxies for federal standards or processes. Open standards, which are developed by recognized industry bodies and widely available for commercial use, are the most common requirements. For example, the Trusted Platform Module, a cryptographic technology standard developed and maintained by the Trusted Computing Group, is an open standard required by many federal agencies as part of their secure computing operations. ISO and IEC develop and maintain an extensive series of standards, such as the ISO/IEC 27000 series related to information security, that serve as models for federal requirements and policies. In some cases, these standards are developed and maintained in close coordination with officials from NIST, DOD, and other agencies.

We think that commonly used commercial standards do and should fulfill federal procurement requirements in all cases that are under examination by this RFI (we understand GSA's report does not intend to make recommendations related to national security systems).

[1] Also, in the case of the intelligence community, this provision was unnecessary. Existing powers allow the federal intelligence community to exclude a source for the purpose of reducing supply chain risk. Specifically, 10 USC 2304(c)(6) allows an agency to limit the number of sources from which it solicits bids or proposals due to national security concerns.

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?

ISO/IEC 27005 ("Information technology -- Security techniques -- Information security risk management") as well as elements of the ISO/IEC 27000 series related to information security, are examples of ISO/IEC information security management system (ISMS) standards that provide a framework and best practices for risk assessment and management. It is important to note that the standards do not specify specific risk analysis methods, but rather the process from analyzing risks to creating a risk management program. These standards, as well as others in the ISO/IEC family such as the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), are widely used and therefore would be preferable to a separate and duplicative framework for the federal government. That said, the federal acquisitions community should approach the development and adoption of any risk analysis framework in close coordination with the ICT industry to prevent faulty or ineffective risk assessment frameworks.

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

Many technology companies use authorized suppliers and resellers as a best practice. Authorized and/or licensed suppliers and resellers usually have agreed to stringent contractual obligations and other protections and quality assurance measures that protect both the buyer and seller of specified technologies. These measures often include protections that improve product assurance; protections that restrict or limit access to product development, intellectual property, and other product elements; and accountability with regard to distribution practices, custodial record keeping, and other provisions. Products that are purchased from unauthorized dealers, gray market outlets, and other unauthorized channels do not offer these assurances and protections, thus greatly increasing the risk of counterfeits, tampering, or otherwise compromised products.

Federal purchasers and their contractors should procure ICT equipment directly from OEMs or their authorized resellers and service partners except when the item is discontinued or otherwise unavailable. This can help to minimize the chances that counterfeit products will be unintentionally acquired. If the government uses non-authorized sources of supply, OEMs should be relieved of any liability from counterfeit parts or software that create cybersecurity risks. Further, manufacturers should be indemnified from any cybersecurity or supply chain liability for software or hardware configuration changes conducted by government personnel or an authorized third-party (i.e. integrator) unless the changes are conducted by OEM-authorized servicers.

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

ITI companies take a responsible approach to disclosure of vulnerabilities to protect our customers as well as the integrity of our own systems. Reckless disclosure of unpatched vulnerabilities puts our customers at risk and reduces the effectiveness of security patches. ITI

companies have robust processes and procedures in place for timely detection, patching of vulnerabilities, and notification as appropriate.

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.

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

Global standards should have preeminence. Globally developed security standards form the foundation of cybersecurity risk management. We are committed to global standards because standardized security technologies, practices, and products deployed across the global digital infrastructure enable interoperability and assurance of security policies and controls, security innovation, efficient and effective use of private sector resources, and rapid response to cybersecurity challenges. Global standardization also restrains the emergence of multiple, conflicting security requirements in multiple jurisdictions, which could compromise cybersecurity. Global ICT standards respond broadly to the needs of global markets, demonstrate relevance through voluntary worldwide adoption and implementation, and are products of standardization processes that are consensus-based, transparent, and industry-led with participation open to any interested party. They also reflect the realities of cyberspace and the ICT marketplace and reduce barriers to trade.

We urge GSA to take an approach consistent with NIST's approach to standards and best practices in the development of the Cybersecurity Framework. NIST, on p. 1 of its recent RFI on the Framework, stated:

> The Cybersecurity Framework will incorporate existing consensus-based standards to the fullest extent possible, consistent with requirements of the National Technology Transfer and Advancement Act of 1995, and guidance provided by Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities." Principles articulated in the Executive Office of the President memorandum M-12-08 "Principles for Federal Engagement in Standards Activities to Address National Priorities" will be followed. The Framework should also be consistent with, and support the broad policy goals of, the Administration's 2010 "National Security Strategy," 2011 "Cyberspace Policy Review," "International Strategy for Cyberspace" of May 2011 and HSPD-7 "Critical Infrastructure Identification, Prioritization, and Protection."

Guidance provided by the NTTAA of 1995 and OMB Circular A-119 directs agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical. This approach is also in line with the statement made by President Obama upon the 2009 release of the Administration's Cyberspace Policy Review: "Let me be very clear: my administration will not dictate security standards for private companies. On

the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity."

However, in referencing/using global standards, the government should not make U.S.-specific modifications to the standards. No matter how slight, this will result in a U.S.-centric approach, balkanize the global marketplace, and could encourage other governments to adopt their own country-specific standards (see our answer to Question 34, below), and ultimately, lead to less secure acquisition options for the U.S. government buyer. Simple mappings of U.S. federal standards to global standards for government agencies may improve understanding for agencies,[2] but global ICT providers will be focused on global standards.

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?

We are using our response to this question not to point out specific conflicts and recommend how they can best be harmonized or de-conflicted, but to make two key recommendations related to the other governments' approaches- the need for the U.S. Government to lead by example, and to proactively do outreach to ensure that other governments do not misunderstand GSA's work in implementing the EO.

Lead by example. ITI's members are global companies located in various countries. Most service the global market (including foreign governments) and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, we acutely understand the impact of international policies on security innovation and the need for governments' policies to be globally compatible. Cybersecurity approaches that differ dramatically by country—a policy patchwork—not only present potentially negative consequences for security, but also disrupt global commerce and ignore the borderless nature of the Internet.

A growing number of governments around the world are enacting cybersecurity-related laws, regulations, certification systems and other requirements, covering their government markets.[3] In some of these cases, these include country-specific requirements that do not improve security but instead erect market access barriers to U.S. ICT companies conducting business in those markets. The Administration (USTR, the Departments of Commerce, State, and others) has actively worked with the U.S. technology industry to try to convince these governments to drop some of these requirements. We are very thankful for the Administration's efforts.

[2] For example, NIST 800-53 includes mapping to Common Criteria (which is based on ISO/IEC 15408) and also to the general information security management standard ISO/IEC 27001.

[3] We are not focused on requirements for security technologies sold into intelligence and military networks (which may in some cases demand country-specific approaches). We refer to discriminatory and unnecessarily trade-restrictive and burdensome requirements that apply to non-military or intelligence government IT systems.

However, this reality indicates that some governments are eager to take restrictive approaches in the procurement space related to security that diverge from the best practices we recommend in our response. This highlights the critical need for the U.S. Government to take the right approach and lead by example. Any new procurement regulations adopted in the U.S. will perhaps be emulated by other governments around the world in their policy environments. This is one among the many reasons we advocate GSA take an approach that highlights the essential role that the global, consensus-based standards play for government security; that eschews new government-run certification schemes; that is technology-neutral; and that is transparent and developed with extensive, ongoing stakeholder input. The U.S. Government has a strong responsibility to set a positive example and make sure any regulations we develop would be equally beneficial if deployed globally. If the United States follows this path, we hope it will lead to greater global consensus for government cybersecurity policymaking and send a signal to our trading partners about the most appropriate way to improve cybersecurity.

Conduct outreach to other governments. We appreciate the outreach to U.S. industry that GSA is conducting regarding its work. Outreach should not solely be domestic, however. The U.S. Government should conduct extensive global outreach to educate other governments about the development, purpose, and role of any requirements GSA develops—what they are and what they are not—and encourage those governments to similarly take approaches to procurement based on voluntary, global, industry-led standards and a transparent process involving industry input.

This will minimize the chances that some governments might misunderstand GSA's work under the EO and assume the U.S. Government is developing new U.S.-specific standards or planning to make acquisition decisions based on country of origin. The latter possibility is one about which we are acutely sensitive. Especially given the recent, unfortunate language in Section 516 of the Continuing Resolution, it is imperative the Administration make clear it does not intend to discriminate based on country of origin. Outreach to foreign governments explaining exactly what the Administration intends to do will help mitigate any chances foreign governments will develop their own policies based on a misunderstanding of ours.

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

There are some key additional ways that the Federal Government should improve the acquisition process to achieve better cybersecurity.

Rationalize and streamline acquisition procedures and checklists related to security.

Weight security appropriately in contracting. Currently, many federal procurements give disproportionate weight to factors such as cost, schedule, supplier diversity, or other factors. In fact, some procurement officials are rewarded based on how much money they save their agency, not on whether the ICT procurements increase the agency's security. If contracting officers are making decisions based on getting the lowest price, there is a chance the products they procure will not have the security features or functions needed for the system or application in which

they will be used. Security should be adequately weighted as a factor in a "successful" procurement so that decisions are not driven by other factors at the security's expense.

Conclusion

ITI would like to again thank GSA for its outreach to industry as it works through the complex topics in this RFI. ITI also would like to commend the Administration for having integrated so much of the input it has received from industry over the past few years on this topic, and for its willingness and eagerness to consistently engage with our companies and the ICT industry generally on how government and industry can work together to improve cybersecurity. The commitment to industry outreach in this regard is an excellent example of the effective public-private partnerships that are essential to improving cybersecurity.

We hope that our responses to the important questions raised in the RFI are helpful and will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. ITI and its members look forward to continuing to work with GSA and the Administration generally to improve America's cybersecurity posture. Please continue to consider ITI a resource on cybersecurity issues moving forward. Do not hesitate to contact me at any time with any questions at dkriz@itic.org or 202-626-5731.

Thank you very much for your consideration.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy