IT Alliance for Public Sector
A Division of ITI

10 September 2015

The Honorable Anne Rung
Administrator
Office of Federal Procurement Policy
Office of Management & Budget
1650 Pennsylvania Avenue, NW
Eisenhower Executive Office Building
Washington, DC 20503

The Honorable Tony Scott
Federal Chief Information Officer and
Administrator for E-Government and Information Technology
Office of the Federal Chief Information Officer
Office of Management & Budget
1650 Pennsylvania Avenue, NW
Eisenhower Executive Office Building
Washington, DC 20503

RE: OMB Proposed Guidance on Improving Cybersecurity Protections in Federal Acquisitions

Dear Administrators Rung and Scott:

On behalf of the Information Technology Alliance for Public Sector (ITAPS)[1], we are responding to the request for comments regarding the Office of Management and Budget (OMB) Guidance on Improving Cybersecurity Protections in Federal Acquisition published on the policy.cio.gov The proposal is intended to provide guidance to federal agencies on implementing strengthened cybersecurity protections through federal acquisitions for products or services that generate, collect, maintain, disseminate, store, or provide access to controlled unclassified information (CUI) on behalf of the federal government. ITAPS 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. ITAPS appreciate this opportunity to share our perspectives and comment on these draft guidelines.

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 customers, brands, and intellectual property – which are essential components of our members' businesses – are 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 acquisitions of goods and services.

Overview

[1] **About ITAPS**. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS 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. Follow us on Twitter @ITAllliancePS.

As ITAPS stated in our more expansive recommendations to this Administration, [2] security is essential to the federal government mission and should no longer be treated and addressed in a patchwork, uncoordinated fashion. Allowing the furtherance of uncoordinated security approaches will simply continue the current model and perpetuate a security regime that is only as strong as the weakest link. This draft guidance raises many concerns and questions, as it does not firmly establish lines of responsibility and create clear lines of authority for the security of acquisitions across the entire federal government enterprise. The guidance is written in sweeping terms, is overly broad, and fails to explain key terms of art or adequately align the technical frameworks with standard acquisition practices.

Over the last couple of years, the federal government has issued two Cybersecurity Executive Orders (EO) 13636 and 13691 and several regulatory measures to enhance cyber resiliency within the federal government and critical infrastructure controlled by the private sector. This draft fails to recognize the need for greater control over federal network security and instead authorizes too much discretion for agencies to create their own unique cyber-security acquisition systems. Such a lack of coordination and management will perpetuate and further the existing federal agency patchwork of requirements for contractors, since it encourages each agency to develop their own cyber requirements for acquisition purposes.

The Introduction to the guidance states that OMB plans to review and incorporate public feedback, "as appropriate", to develop final guidance, but this guidance does not carry the weight of regulatory authority for either agency personnel or contractors and appears to order agencies to "immediately begin" to apply the guidance. We believe OMB should revise this guidance as stated herein to provide clarity and impose uniformity of applicable rules to clearly establish lines of authority and responsibility, create clarity for agencies and define consistent requirements so contractors providing products and services to the federal government have one regime to adopt for compliance. In the alternative, OMB should recall or withdraw the proposed guidance and coordinate with executive agencies to implement an acquisition framework using the standard notice and comment rulemaking process.

To illustrate the number of overlapping and potentially conflicting requirements contractors currently face, we share the following inventory of regulatory actions ongoing at the time of this writing:

- Department of Defense (DoD) rule on the safeguarding of unclassified controlled technical information and reporting of associated cyber incidents.
- DoD interim rule on the safeguarding of covered defense information and reporting of incidents
- DoD interim rule on cloud computing and the reporting of incidents
- National Institute of Standards and Technology (NIST) guidance on cybersecurity and the management of controlled unclassified information
- OMB's proposed guidance on cybersecurity protections
- Department of Homeland Security (DHS) Class Deviation 15-01 Safeguarding of Sensitive Information
- OMB's impending issuance of security revisions to Circular A-130
- Anticipated Federal Acquisition Regulations (FAR) clauses on these topics (along with the fact that the FAR does not currently address the existing regime)
- Future NIST cybersecurity guidance, such as NIST Special Publication (SP 800-160) "Systems Security Engineering An Integrated Approach to Building Trustworthy Resilient Systems"

[2] ITAPS letter to OPM, OMB, and National Security Staff dated 30 July 2015, Cyber-Security Task Force Recommendations

If the point of the OMB guidance is to develop an efficient and effective cyber-security acquisition infrastructure, OMB should harmonize their guidance with these other federal efforts and ensure that they are applied consistently across the entire federal enterprise. Without such management, this array of new requirements, regulation and guidance will add further confusion for the acquisition community, increase the compliance burden for both the government customer and the vendor community and significantly increase costs for the taxpayer for the technology goods and services the government mission requires.

As a threshold matter, Section 8(e) of EO 13636 "directed GSA and DoD to make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration." ITAPS and its members have been participating since EO issuance in the General Services Administration (GSA) and DoD Joint Working Group efforts on "Improving Cybersecurity and Resilience Through Acquisition" as required for government-wide implementation of EO 13636. Throughout the efforts of the agency 8(e) working group to socialize their policy approach, industry has clearly stated that any recommendations must: (a) be based upon the use of a risk-based approach, (b) develop common definitions and terms of art and, (c) harmonize any resultant regulatory requirements. That deliberate approach has been guiding the federal cyber-security effort since its inception, but OMB's proposed guidance will lead to inconsistency in agency cyber acquisition policy, does not use a risk-based approach and does not harmonize the assorted agency efforts that will lead to better security and help contractors implement the rules with which they must comply.

Security Controls

The security controls in the draft guidance are based on the requirements of the Federal Information Security Management Act (FISMA), OMB policy and NIST standards and require all systems to meet NIST SP 800-53, instead of using a risk-based approach. The guidance does not differentiate between the specific agency missions, the type of systems necessary for those missions or the level of security needed for the system as determined prior to acquisition by a risk assessment of the missions and how the network or system will be used. Furthermore, the draft guidance does not adequately demarcate the line between controls needed for contractor systems operated on behalf of the government (800-53) and contractor internal systems where CUI is "incidental" to the contract's requirements (800-171), depending on whether contracting personnel consider information "incidental" or not. The lack of any definition of incidental could create added risk for contractors whose systems are already in place, but which may not fulfill all the requirements of 800-53.

The OMB Guidance is also intertwined with, and may be dependent upon, the actions of National Archives and Records Administration (NARA) to consolidate agency CUI marking and handling schemes into a single CUI FAR clause. The OMB guidance is thus premature to the development and completion of other joint industry and government efforts to define the scope of CUI. A policy approach that generates multiple CUI instructions will only result in divergent and ineffective policies being implemented by the government if the OMB guidance moves forward, since NARA has not yet finalized the CUI rules nor developed the FAR clauses and NIST is currently developing more requirements in a supplemental to SP 800-171 for data that needs even greater protection. We are also concerned that the proposed CUI regulation needs stronger language to prohibit federal agencies from taking unilateral action by issuing their own regulations to safeguard CUI, such as the DHS Class Deviation 15-01 on Safeguarding of Sensitive Information. This deviation is onerous and goes beyond NARA's CUI to impact any contractor that has access to DHS data through nonfederal information systems, but under this proposed guidance,

that approach could be adopted as a standard procurement policy should all agencies be authorized to act individually.

Furthermore, the existing guidance does not discuss or mention Federal Risk and Authorization Management Program (FedRAMP). Given the enormous resources contractors have devoted to achieving FedRAMP Authority to Operate (ATO), the guidance should explain how it relates to FedRAMP ATO status. Controls in SP 800-171 are met through FedRAMP Revision 4 for securing government sensitive data, but the guidance does not provide any acknowledgement of the program. We recommend that the guidance address FedRAMP and how it will work with FedRAMP for government cloud acquisition.

We further recommend that contractors should be able to propose alternative IT security controls than those required by NIST if they demonstrably provide the same or higher levels of security. ITAPS members are global companies that use international standards to secure their products and services. Under the DoD's Unclassified Controlled Technical Information (UCTI) Defense Federal Acquisition Regulation Supplement (DFARS), a contractor can offer ISO 27002 certification in lieu of conforming to NIST SP 800-53 or NIST SP 800-171. Such flexibility should be emphasized in the OMB Guidance to allow IT companies to use alternative IT security controls.

Cyber Incident Reporting

This section is vague and broad. We believe that OMB needs to define "cyber incident" and CUI so agencies are working from a consistent definition. Currently NIST and the DoD interim guidance on the safeguarding of covered defense information and reporting of incidents are using inconsistent, potentially conflicting definitions, including vague requirements to report on incidents with "potentially adverse effect(s)." Furthermore, this guideline is extending SP 800-171 beyond its original intentions to cyber incidences. OMB needs to utilize this guidance to address existing inconsistencies and establish uniform and harmonized cyber incident reporting across the entire government enterprise. Without such uniformity and harmonization, questions left to agencies to answer will likely result in further differentiation between contractor requirements and increase the cost of compliance and the goods and services the government seeks to acquire. Instead, we recommend that OMB follow the security model in the NIST Cybersecurity Framework, which encourages entities to select those security controls best tailored to their environment.

We agree that single reporting for an incident could lead to more efficient and timely communication about breaches, but recommend to OMB that where incident reporting is required, that safe harbors be erected to prevent erroneous good faith reporting from third party liability. OMB should also recognize in the policy that the incident reporting regime should be different for systems operated for the government and for contractor internal systems with incidental levels of CUI. Authority to invent specific agency remedies for reporting failures should also not venture outside the current contract remedies structure and the OMB guidance should establish protective mechanisms for information included in an incident report that is otherwise proprietary, business confidential or competition sensitive.

As the guidance suggests, reporting requirements could be idiosyncratic to each agency or type of requirement or any number of varying elements of performance. Reporting timelines should thus become part of an open dialogue between government and industry since contractors may not be able to meet some agency deadlines if those become a negotiation element subject to contract forces.

Information System Security Assessments

ITAPS members are global companies that sell their products and services in an integrated global market. We have strong concerns about this guidance requiring contractors to give the federal government access to their facilities and data anytime. In this post-Snowden environment, this has huge economic implications. ITAPS parent association, the Information Technology Industry Council (ITI) has been consistent in our opposition to efforts around the globe to establish government access to IT company's backend systems.

Many IT companies are custodians of sensitive customer information from around the globe. These companies cannot allow for these inspections to compromise other customers' (particularly foreign government) data privacy. Such a requirement has implications for many of the latest technological capabilities, including cloud services. The technical construct of multi-tenant clouds, where the government is but one of many customers, would prevent the type of access the proposal suggests for assessments of systems. If companies allowed the government to access their systems, they could be violating other customer's, including other U.S. government agency customers, contractual requirements. We are also concerned that the government could expose and have access to our intellectual property and data systems when using private vendors to do assessments or the government requiring entering our facility. This could have the net effect of requiring any global commercial company that does business with the government to have a segregated IT system to ensure customer data privacy, thereby forcing it to incur significant additional costs and raise prices for the federal government to do business.

To the extent that contractors are handling Personally Identifiable Information (PII), the guidance only speaks to SAOP review and certification. We recommend that OMB addresses in a separate section of the guidance how PII should be handled. This would be helpful to include safeguards, notice, breach response and reporting.
Without latitude, this proposal risks critical supplier relationships. Even in larger organizations, there will be a roadmap to full compliance and successful Authority to Operate (ATO) for all programs. Phased integration can support continued progress to OMB objectives and acquisition goals. Possible alternatives include developing a maturity model, initially focused on foundational elements and including additional components over time. For example, the first release of the requirement could establish an ATO component, focused on Security Control compliance. Future releases could add Incident Reporting, Continuous Monitoring and Due Diligence requirements to the ATO scope.

A reconsideration of the ATO process and timelines would support both supplier maturity and availability. For instance, Interim Authority to Operate (IATO) durations could be longer, based on an accepted Plan of Action & Milestones (POA&M), with periodic status reports to confirm progress to remediate gaps. Finally, continued optimization of ATO deliverables will be key to productivity and compliance cost. Clear agreement on expectations during the acquisition cycle will ensure appropriate allocation of resources.

Information Security Continuous Monitoring

We have strong concerns with the draft language in the guidance requiring DHS Continuous Diagnostics and Monitoring (CDM) capabilities to be placed on contractor operating information systems on behalf of the government. If the agency determines that providing DHS CDM capabilities to a contractor is not feasible, then the agency may elect to perform information security continuous monitoring and IT security scanning of contractor systems with tools and infrastructure of its choosing. Our understanding is that DHS CDM capabilities are not fully functional at this point. We have concerns about both the mandating of CDM as well as of other scanning tools operated by the government if CDM is not feasible.

While we are strong supporters of the CDM program and believe that it gives federal government agencies a great deal of benefit, we want to better understand what the proposed obligation really means from an operational point of view relative to contractors. Does it mean that the government would give the CDM capability to contractors? Or does it mean that contractors would be obligated to comply with CDM and thus would grow the size of the effective CDM market? While the idea of growing the size of the CDM market has some appeal, if this is what the proposed rule would do, the idea that the government could be in the business of giving away CDM solutions to the private sector would be troubling for us.

As mentioned in the information security assessment, we are concerned about placing CDM on our information systems because IT companies are custodians of sensitive customer information from around the globe. These companies cannot allow for these inspections to compromise other customers' (particularly foreign government) data privacy.

Business Due Diligence

OMB's proposed guidance anticipates the creation of a database that will permit agencies to conduct cyber related due diligence. OMB's proposed guidance does not provide any details or standards as to how this database will be used or maintained by agencies in procurements, nor any detail on how the government will stand up such capability, or collect, sort or differentiate the data once put into a system of records, notwithstanding providing contracting officials the discretion and authority to exclude any given source within the supply chain based on questionable or suspect information sources.

OMB also proposes to produce "risk indicators" for agencies to use in making determinations as to how a contractor assures information integrity and security. The guidance does not provide any direction as to how these risk indicators will be used by agencies in their acquisition activity. Concerns include whether these risk indicators will be uniformly and consistently evaluated, what criteria will be used and who will be performing the evaluations, and how disagreement with the evaluations will be adjudicated by contractors and acquisition staff.

We are concerned about GSA maintaining a database of "bad actors" – contractors that fail to live up to OMB cyber standards. What is the protocol or adjudication for companies' recourse against the classification and/or removal from the list? Will companies be able to review the information contained in this database. Will contractor officials use this information to exclude you from a competition without you knowing? We urge OMB to work with the 8(e) working group to establish accurate and transparent vetting protocols on any open source data acquired by the government as part of this process.

It's premature for OMB to include business due diligence when GSA has not worked out many of the details for agencies to use when there is currently nothing in place for agencies to use and the risk of a de facto debarment is greatest where companies cannot or are not able to discover the reasons why they are on the bad actor list.

Others Concerns:

Requirements in this guidance and the regulatory cyber regime will limit competition for small and emerging companies. Smaller businesses will need the technical resources to meet these requirements such as implementing SP 800-171 that they may not have today. This could cause some primes or integrators to have to eliminate these smaller businesses from their supply chains. Furthermore, many of the leading commercial IT companies are the

global innovative leaders in providing IT security systems. Recently, the Department of Defense and the Department of Homeland Security has initiated efforts to reach out to Silicon Valley to get more untraditional IT companies to sell their products and services to the federal government. Setting so many rules can provide an impediment for small business and access to non-traditional players.

The draft guidance does not address whether and how contracts and contractors should incorporate actions being taken in response to the ongoing OMB "cyber-security sprints", including the role contractors should play in addressing such sprints.

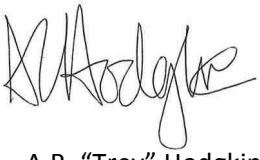
We also recommend that OMB address NIST's ongoing work with international standards development organizations to map NIST controls with international information security standards. Since much of this would ultimately result in new FAR provisions, we are concerned there is virtually no information about what exactly would fall under the scope of the guidance. Is it all IT procurements? A portion thereof? Or a small subset of acquisitions that represent the greatest potential risk? Without any of that further information, it's difficult to assess the severity of concerns.

As a process matter, the OMB effort to elicit industry comments is laudable but the method used (GitHub) and the time allotted (30 days) is insufficient to address so weighty and important a topic. We recommend that before any final guidance to agencies is promulgated, OMB publish the next iteration of the guidance for public comment and allow for an appropriately scaled comment period for greater transparency.

In conclusion, we strongly urge OMB to (1) modify the guidance dramatically to align with the many other agency cyber efforts per the recommendations in the letter, or (2) withdraw the guidance and go through a standard regulatory comment process. This guidance needs to create a risk-based process. ITAPS recommends that an approach built around a capability maturity model that factors in varying levels of company capability based on size, type of business model, flexibility and that is risk based would be a vast improvement to the prescriptive model being fostered in the proposed OMB guidance. We urge OMB to prominently feature more of the NIST Framework in this guidance and should be much more integral to this guidance. The Framework should be used government-wide to help determine agencies cyber risk.

Thank you again for the opportunity to respond to this request and share our viewpoints. We look forward to working with OMB as you refine this guidance, and we are available at any time to elaborate on our response. Should you have any questions regarding these comments, please 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