TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

September 10, 2015

Tony Scott
United States Chief Information Officer
Administrator, Office of Electronic Government and Information Technology
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Administrator Scott:

The Telecommunications Industry Association (TIA), the leading trade association for global manufacturers, vendors, and suppliers of information and communications technology (ICT), writes to convey its input to the Office of Management and Budget's (OMB) on draft guidance on implementing strengthened cybersecurity protections in Federal acquisitions towards mitigating the risk of potential incidents in the future. TIA and our member companies are committed to enhancing the national security in both the public and private sectors. Appended to this letter are TIA's consensus views on the proposed OMB guidance.

TIA appreciates OMB's efforts to improve cybersecurity in Federal acquisitions. Generally, we urge that OMB be guided by the following principles:

- Successful efforts to improve cybersecurity will leverage public-private partnerships to effectively collaborate on addressing current and emerging threats;
- The U.S. government should enable and stimulate greater cyber threat information sharing between the public and private sector;
- Policymakers and regulators should ensure that they address economic barriers for owners and operators of critical infrastructure in efforts to secure cyberspace;
- The global nature of the ICT industry necessarily requires a global approach to address cybersecurity concerns; and
- A global supply chain can only be secured through an industry-driven adoption of best practices and global standards.

TIA represents approximately 300 ICT manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the the public sector and are directly impacted by OMB's proposed guidance. Representing our membership's commitments in this area, we also hold membership and are actively engaged in key public-private efforts that contribute to secure information systems, including the Communications Sector and Information Technology Coordinating Councils and the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC), among other successful public-private partnerships.

Thank you for your continuing hard work on this important national and economic security issue, and TIA looks forward to working with you moving forward. For more information, please contact Brian Scarpelli at (703)-907-7714 or by email at bscarpelli@tiaonline.org.

Sincerely,

___/s/_____

Brian Scarpelli
Director, Government Affairs
Telecommunications Industry Association (TIA)
d: 703.907.7714 | m: 517.507.1446 | BScarpelli@tiaonline.org
TIAonline.org

TIA Views on OMB's draft Improving Cybersecurity Protections in Federal Acquisitions

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Introduction	While OMB notes that its goal is to "allow for a better understanding of the perspectives of the broader community and to identify areas for improvement to make this guidance even more meaningful and effective," TIA notes that this guidance was not published in the Federal Register, and recommends that OMB ensure that it's development of guidance meets governmental transparency requirements, such as the Administrative Procedure Act. We appreciate the unique GitHub platform, but believe that publication in the Federal Register will help improve participation in OMB's important efforts towards improving cybersecurity protections in Federal acquisitions.	N/A
Cyber Incident Reporting section	TIA appreciates OMB's effort to develop guidance for contractor reporting of cyber incidents. In order to ensure that "reporting will promote timely and meaningful information sharing that allows both the contractor and the agency to work closely together to investigate the incident, identify affected individuals, quickly respond to the incident and take other appropriate actions as necessary," TIA urges OMB to ensure that it minimizes the burdens on contractors by ensuring a simplified and clear reporting procedure.	In the Cyber Incident Reporting section, we recommend that OMB specifically recommend in its guidance that agencies shall make efforts to create straightforward and clear guidance on cyber incident reporting.

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Cyber Incident Reporting section	Incident reporting should not include "potentially adverse effects." This is far too broad and not risk-based. It will result in over-reporting. It will divert resources from responding to events that cause actual harm without yielding significant security benefits. The section on contract language requires inclusion of "Specific government remedies if a contractor fails to report according to the agreed upon contractual language." Any such remedies should be defined by law or regulation, be proportionate to the actual harm suffered by the relevant agency, and take into account whether notification was briefly delayed, delayed by weeks or months, or never provided. At the end of the section, it states that contractors "shall" report incidents not only to the SOC, but also to four other officials. Contractor reports should be made only to the SOC, which should then report to other agency officials. SOC personnel are in a better position to identify the current officials and provide notification in the most secure manner.	TIA urges OMB to eliminate "or potentially adverse effects" from the first paragraph of the Cyber Incident Reporting section. TIA urges OMB to include that "…specific government remedies if a contractor fails to report according to the agreed upon contractual language" may be defined by law or regulation, should be proportionate to the actual harm suffered by the relevant agency, and should take into account whether notification was briefly delayed, delayed by weeks or months, or never provided. TIA urges OMB to eliminate the proposed requirement on contactors to report incidents to officials other than the SOC.

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Information System Security Assessments	In the context of demonstrating/attesting to adequate levels of security before entering an arrangement with the government, TIA believes that audit and inspection rights should be limited to reviewing documents demonstrating that a certification or attestation has been made on the front end by the vendor or a third party. Direct inspection of physical facilities, databases, IT systems, and devices by the government is not appropriate. Heightened complexity occurs where the government is using a shared, multi-tenant cloud environment, whether other tenants may have sensitive data or trade secrets and object to government officials being able to inspect the hardware holding that data. As another example in the post-incident context, in an incident response and sanitization exercise, if a government official happens to misuse a shared multitenant cloud service (*e.g.*, by inserting controlled or even classified information) other tenants will object to the government seizing or analyzing physical hardware for sanitization purposes. Per discussion above, in this scenario, the right to physical inspection is again not reasonable.	TIA urges OMB to limit audit and inspection rights in this section's context to reviewing documents demonstrating that a certification or attestation has been made on the front end by the vendor or a third party, and not to include direct inspection of physical facilities.
Information Security Continuous Monitoring section	TIA supports the proposal that agencies and contractors must work together to determine and implement an appropriate solution that fulfills the ISCM requirements; that agencies should work with DHS to ensure that the proposed solution fulfills the ISCM requirements identified in FISMA; and that, for systems not operated on behalf of the Government that continuous monitoring is part of the security assessment requirement in NIST SP 800-171.	N/A

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Business Due Diligence section	For companies which contract with and vend to the Federal government, attaining and maintaining the proper level of trust is of the upmost importance. We urge that any actions by OMB towards improving cybersecurity reinforce the need for reasonable assessments along with a fair opportunity for concerns to be addressed by the contractor or vendor at issue. For example, the document explicitly says that third party validation is acceptable depending on the risk assessment, though a self-assessment may also often be an appropriate mechanism depending on the risks of the system.	TIA believes that OMB's guidance on due diligence process should include the following fairness and due process elements: • Right to see what is in the record relating to your company • Clear rules about what types / sources of information can and cannot be included in that record (e.g., to eliminate unsubstantiated rumors) • Freshness requirements so that information beyond a certain age does not stick in the file forever • Right to request corrections or deletions of inaccurate data • Right to comment on data that you believe to be inaccurate, which the government refuses to correct or delete • OMB should clarify what information, if any, will be subject to FOIA requests.

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Coordination of OMB's efforts with other Federal efforts	OMB does not mention ongoing Federal acquisition efforts to address cyber-based threats in its draft save for one reference to the FAR, giving rise to questions on TIA's part around, for example, the interplay of this effort and Department of Defense Interim Rules. OMB should ensure close coordination with all other Federal entities when adopting rules for improving cybersecurity acquisition. For example, on August 26, 2015, the Department of Defense (DoD) issued an interim rule that expands the obligations imposed on defense contractors and subcontractors to safeguard "covered defense information" and for reporting cyber incidents on unclassified information systems that contain such information.[1] The interim rule revises the Defense Federal Acquisition Regulation Supplement (DFARS) to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 and section 1632 of the NDAA for FY 2015. In addition, the interim rule implements DoD policies and procedures for safeguarding data and reporting cyber incidents when contracting for cloud computing services. DoD's interim rules go into effect as of their publication (Aug 26), and comments are being accepted until Oct 26). TIA is unclear about why this draft OMB policy is moving forward, apparently in parallel, when DOD has initiated the rule changes described above. Duplicative and/or redundant Federal policies, particularly in the information security space, needlessly increase complexity for contractors and vendors, and disincent investment and innovation in this space. We strongly urge OMB to ensure that its efforts to improve cybersecurity in Federal acquisitions, and to specifically clarify this draft OMB guidance's relationship to the DoD rulemaking.	OMB should acknowledge the related DoD rulemaking (and other related Federal efforts), and provide a description of the relationship of this effort to them. OMB should also summarize it's efforts to ensure that its guidance is not duplicative or conflicting with other related Federal efforts.

[1] *See* http://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf.

Area of Draft Guidance/Issue	TIA View/Recommendation	Line Edit
Federal education	TIA has long noted that a large challenge for reform in the acquisition process will be to ensure that cybersecurity concerns are fully appreciated and understood throughout that process, and that this will require adequate workforce training across the Federal government. In addition, TIA believes that end-user education is also a crucial aspect to improving cyber threat ecosystem response capabilities, as many cyber vulnerabilities are already known and related attacks are relatively easily preventable. Numerous efforts exist across sectors to inform end users of proper steps to take to ensure that proper cyber "hygiene." For example, TIA supports that network operators and service providers generally educate the customers on important steps that should be taken, from the use of adequate passwords to encryption of data. TIA notes its supports providing federal Chief Information Officers ("CIOs") with increased authority over IT expenditures. We believe that this is consistent Clinger-Cohen Act. However, concentrating budget authority with department level CIOs can also limit innovation and needed flexibility at operational level where much of the IT purchasing occurs, and can slow the acquisition process. Agency CIOs should be trained to develop enhanced acquisition skills that also encourage the consideration of necessary cyber security concerns.	TIA urges OMB to include a new section addressing cybersecurity in relevant training for Federal employees. While it has been suggested in a related effort to improve Federal acquisition per EO 13636,[2] this section should not focus on requiring more from industry relative to cybersecurity in certain types of acquisition, but should instead ensure accountability for those making acquisition decisions. While industry has a role in increasing education on ways to improve resiliency to cyber-based vulnerabilities, the role of the Federal workforce training process is also very important and OMB's guidance should reflect this reality.

[2] *See* DoD and GSA, *Improving Cybersecurity Resiliency Through Acquisition: Final Report of the Department of Defense and General Services Administration* (rel. Nov. 2013) at 14-15. TIA submitted views on this report that include recommendations on education and awareness recommendations, which are available at http://bit.ly/S2Wsxz.