IT Alliance for Public Sector
A Division of ITI

July 30, 2015

The Honorable Beth Cobert
Director (Acting)
U.S. Office of Personnel Management
Theodore Roosevelt Federal Building
1900 E Street, NW
Washington, DC 20415

The Honorable Anthony "Tony" Scott
Administrator and Federal Chief Information Officer
Office of E-Government and Information Technology
Office of Management and Budget
1650 Pennsylvania Avenue, NW
Washington, DC 20502

The Honorable J. Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator
National Security Staff
Executive Office of the President
The White House
1600 Pennsylvania Avenue, NW
First Floor, West Wing
Washington, DC 20500

Dear Director Cobert, Administrator Scott, and Special Assistant Daniel:

On behalf of ITI's IT Alliance for Public Sector[1] (ITAPS), we appreciate the opportunity to offer the attached recommendations on the recent cybersecurity challenges the federal government has faced. These recommendations address the questions: what steps industry takes to address these challenges; what priorities industry would establish, given the time left in this Administration; how industry would identify and mature for deployment technology goods and services; what protocols and practices industry uses to maximize cyber crisis response capability; and, how industry establishes clear lines of responsibility and accountability to address these challenges when they occur.

To develop these recommendations, ITAPS convened a task force comprised of 35 representatives from 20 leading technology companies. These are cybersecurity experts with deep experience in the public sector, most with stints both in government and industry. The task force identified specific elements and items and matured the recommendations we present today as the result of their deliberations.

To summarize the recommendations industry offers, we believe that the Administration should not treat the recent cyber challenges in isolation, but instead address these challenges from a government-wide posture. The government should also boldly act to alter the overall culture and approach the federal government currently uses to address cyber threats. Without such boldness, we are concerned that the challenges will persist.

Now more than ever, information and the technologies that deliver it are central to the federal government mission. This has resulted in an increase in capabilities, efficiencies, transparency, and better citizen and constituent services. Cybersecurity must be placed at the forefront of information technology in the government mission. ITAPS stands ready to assist you and others in the government to implement these recommendations. Should you have any questions, please contact Pam Walker at pwalker@itic.org.

Respectfully,

A.R. "Trey" Hodgkins, III
Senior Vice President, Public Sector

[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 @ITAlliancePS.

IT Alliance for Public Sector
A Division of ITI

ITI's IT Alliance for Public Sector Task Force Recommendations

Issue 1: Establish in Broad Terms how to do Cyber in the Federal Government

The U.S. government must make dramatic and significant changes to secure government networks and the critical information and functions they support. The federal government must declare the protection of those systems and the information residing on or traversing them a national priority and then act boldly, favoring speed and agility over adherence to legacy policies. The Federal Cybersecurity Sprint, including the activities implemented to date, manifests the sense of urgency that should be core to the cybersecurity culture and approach going forward. ITI's IT Alliance for Public Sector (ITAPS) recommends that the federal government accelerate the transformation of its approach to cybersecurity management along four primary cybersecurity management disciplines: **Security Risk Management; Governance and Accountability; People and Organizations;** and **Finance and Procurement**.

Security Risk Management:

- Determine criticality of systems and data and prioritize accordingly to achieve an effective, risk-based approach to protecting systems. For example, using current NIST directives and controls, immediately conduct an independent operational risk assessment of all U.S. government infrastructure, applications, and data to determine highest risk across the government and subsequently prioritize and appropriately resource remediation with specific completion dates, and track to expedite closure.
- Develop and execute strategies to keep systems on most up-to-date or secure versions and mitigate risk posed by those systems that cannot be immediately updated, ensuring security deployments are inherently more secure. For example, agencies should clearly define risk mitigation plans, phase-out deadlines, and justification statements.
- Modernize security approaches beyond the perimeter-focused "moats and walls" approach, transitioning from a "secure network of systems" to a "network of secured systems" to achieve security in depth and improved resilience. For example, agency security strategies should emphasize detection, identification, protection, response, supply chain transparency, security intelligence, predictive analysis, data encryption, and a "zero trust network" philosophy.
- Use industry-accepted approaches, standards, and lexicon to allow for improved, consistent understanding and communication about security, both across the organization and with vendors. For example, adopt and enforce the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST directives across the federal government.

Governance and Accountability:

- Establish an outcome-focused Governance Framework that covers all aspects of the enterprise, resulting in effective direction-setting, decision-making, oversight, transparency, and accountability. For example, fully execute and enforce the Federal Information Security Management Act (FISMA) as contemplated in the authorizing legislation and seek legislative reform where necessary.
- Escalate security from merely an IT concern to a business risk concern, providing independence and enabling security decision-making and implementation. For example, make permanent a central Administration role, with appropriate authorities and budgetary controls, to direct and oversee cyber activities across the government, including leadership of a cybersecurity "council" for interagency coordination; separate agency Chief Information Security Officer (CISO) functions from Chief Information Officer (CIO) functions; establish a mechanism to escalate agency CISO security concerns directly to the department or agency head or central cyber function for adjudication as appropriate.
- Provide for the escalation of risk-based decisions through senior leadership if critical security recommendations are rejected by owners of business lines or applications, ensuring critical security decisions are not made in isolation. For example, decisions to keep critical systems available while overriding security recommendations should no longer be routinely deferred exclusively to network, system, or application managers.
- Adopt approaches that emphasize cross-organizational collaboration, transparency, accountability, and integration; reducing costs, minimizing operational risks, and driving continuous improvement. For example, institute or adopt the security development lifecycle, NIST guidance and directives, international standards, and the DevOps method across agency operations, security, and development teams.
- Align investments of networks and security entities that often buy overlapping technology in isolation from each other, resulting in coordinated and consistent approaches across an organization. For example, implement the recently passed Federal IT Acquisition Reform Act (FITARA) and FISMA reform legislation to support the empowerment of CIOs and CISOs within agencies, and align risk management among disparate groups that purchase cybersecurity tools within agencies.

People and Organizations:

- Make information security a core part of organizational culture, ensuring greater awareness and better computing practices. For example, information security training should be mandatory for all government employees and contractors and information security performance should be an item in performance reviews.
- Optimize enterprise and workforce planning to leverage consolidation in security talent, achieving cost savings and security benefits. For example, certain functions that are not inherently governmental can be outsourced (e.g., data centers shifted to vendor-managed cloud environments) as appropriate and in accordance with the pre-defined security parameters.
- Identify the unique aspects of the operational environment as a marketing tool to improve workforce hiring and retention. For example, for recruitment and retention, the government should tout that it is a highly-attacked network posing unique security challenges and the Department of Homeland Security (DHS) should leverage the special pay incentives provided by recent legislation. Other agencies should work to identify and use similar hiring and pay incentives or exceptions.

Finance and Procurement:

- Organizational procurement programs should have clearly defined and communicated priorities, accompanied by clear direction to procurement agents on the procedures to acquire technology consistent with those priorities, resulting in a consistent, predictable, and agile acquisition approach that will result in more secure technology deployments. For example, the Director of the Office of Management and Budget (OMB), in consultation with the Administrator of the Office of Federal Procurement Policy (OFPP), as key national priorities should: (1) provide clear direction to security and acquisition officials across government that cybersecurity solutions should be acquired and implemented rapidly; (2) advise security and acquisition officials on existing authorities available for the rapid acquisition and implementation of cybersecurity solutions; and, (3) expeditiously identify impediments to the rapid acquisition and implementation of cybersecurity solutions that need to be addressed by Congress and report those impediments to the relevant committees of jurisdiction for redress.
- Tie organizational cybersecurity performance to funding, to achieve greater employee and organizational accountability and traceability. For example, OMB should withhold non-cybersecurity discretionary budget from underperforming agencies and identify and emphasize potential criminal and civil penalties for compliance failure (e.g., develop recommendations for revisions to the Anti-Deficiency Act).
- Leverage agile and transparent acquisition approaches, as appropriate, that provide security officials the flexibility to procure the technologies they need expeditiously. For example, the government should consider the use of accelerated and national security contracting authorities once identifying an appropriate technology that satisfies a defined, urgent cybersecurity requirement.
- Evaluate opportunities to achieve enhanced security using new and accepted technologies that can rapidly retire legacy systems and consolidate resources. For example, accelerate the appropriate use of shared services and the use of cloud computing, promote the right-sizing and efficient alignment of common agency systems, rapid retirement of insecure legacy systems, and consistent approaches to security.
- All emerging and existing procurement, acquisition, and development programs should be aligned and consistent with organizational risk management and governance approaches, ensuring technology deployments are secure, protected, and within a broadly understood framework. For example, any new government-provided acquisition and consulting activities offered across agencies should not proceed without the development and implementation of a security framework and plan to mitigate cyber risk consistent with the framework established pursuant to these recommendations.

IT Alliance for Public Sector
A Division of ITI

Issue 2: Identify the Focus for the Remainder of this Administration

In the remaining time for this Administration, the federal government must execute a series of initiatives and reforms to rapidly and comprehensively secure federal networks and data, urgently declaring our nation's networks a national priority. The government must move boldly with speed, transparency in action, unity of effort, and clarity in purpose. While these efforts should result in immediate enhancements, they will also set the foundation for the government's future efforts. Most importantly these efforts will begin the long process of restoring the American people's trust in the ability of the federal government to protect its networks and the information that resides in and transits those networks. The actions provided below are intended to serve as a continuation of the many good activities initiated through the Cybersecurity Sprint, and provide a roadmap to implement many of our recommendations.

Isolate Sensitive or Critical Vulnerable Systems:

- Urgently identify and prioritize protection of (including automated isolation, compartmentalization, segmentation, and/or disconnection, as appropriate) all vulnerable systems, updating to more secure configurations before reconnection.
- Develop clearly defined risk-mitigation plans, accompanied by closely managed phase-out plans for those systems that cannot be adequately secured or updated due to mission impact.
- Implement metrics through FISMA guidance that measure compartmentalization ratios to limit the number of systems or workloads a given system has access to without passing through security controls inside the network.

Define Systems, Determine Criticality, Assess Risk, and Act in a Risk-Based Manner:

- Conduct an independent operational risk assessment of the whole U.S. government enterprise, including but not limited to infrastructure, applications, data, file sharing, and related dependencies using current NIST directives and controls to determine criticality, vulnerability, and highest risk across the government; subsequently prioritize and appropriately resource remediation with specific completion dates and track to expedite closure.
- Use the results as the foundation for all future risk determinations, prioritization, and rationalized resource remediation plans based on the relevant NIST directives and controls and the NIST Cybersecurity Framework.
- Assess and improve the current state rapidly (e.g., Target and JP Morgan quickly completed after-action analyses and reengineered in months rather than years).

Develop a Comprehensive Strategy and Action Plan:

- Develop a single, unified federal civilian network cybersecurity strategy that provides clear direction, guidance, and top down governance structures to each and every federal agency.
- Inform the strategy development by the results and learning of the prevailing risk environment, the available capabilities, and the related gaps discovered through the operational risk-assessment process.

- Inventory "almost ready to deploy" technology and solutions that might be brought into service immediately to address risks. Conduct a gaps analysis between identified risks and "almost ready to deploy" solutions, operationalizing those solutions that can immediately address critical or high-priority risks.
- Engage industry and vendors in the development of the strategy, as most technologies and services the government networks rely upon are developed and delivered by industry partners.

Foster a Culture of Effective Governance and Accountability:

- Escalate security from merely an IT concern to a business risk concern, providing independence and enabling security decision-making and implementation. For example, make permanent a central Administration role, with appropriate authorities and budgetary controls, to direct and oversee cyber activities across the government, including leadership of a cybersecurity "council" for interagency coordination; separate agency CISO functions from CIO functions; establish a mechanism to escalate agency CISO security concerns directly to the department or agency head or central cyber function for adjudication as appropriate.
- Fully execute and enforce FISMA 2014 as contemplated in the authorizing legislation; seek additional legislative reform where necessary.
- Expedite implementation of the cybersecurity culture by incentivizing and holding accountable personnel to identify and bring IT security problems forward, establishing key performance indicators and security awareness training, etc.

Reform Procurement Systems to Emphasize Security, Agility, and Transparency:

- Assess the risk and financial justifications for continuing to invest operations and maintenance funding into legacy systems, particularly if those systems cannot be adequately secured.
- The Director of the OMB, in consultation with the Administrator of OFPP, as key national priorities should: (1) provide clear direction to security and acquisition officials across government that cybersecurity solutions should be acquired and implemented rapidly; (2) advise security and acquisition officials on existing authorities available for the rapid acquisition and implementation of cybersecurity solutions; and, (3) expeditiously identify impediments to the rapid acquisition and implementation of cybersecurity solutions that need to be addressed by Congress and report those impediments to the relevant committees of jurisdiction for redress.
- Any new government-provided acquisition and consulting activities offered across agencies must begin with the development and implementation of a security framework and plan to mitigate cyber risk consistent with the framework established pursuant to these recommendations.

IT Alliance for Public Sector
A Division of ITI

Issue 3: Develop a Means to Identify the Good Ideas, While Culling out the Sales Calls

In order to identify the best solution to address government cyber issues, we recommend a combination of external and internal support. To ensure that agencies have the most up-to-date information, we suggest the creation of a portal for communication between the agencies, the public, and industry. Furthermore, we recommend the addition or reevaluation of internal, government-wide groups and procedures that allow for acquisition of the best technologies to combat the newest threats. We believe that this combination will provide a well-rounded and balanced measure for finding the best solutions.

Portal for Open Communication between Agencies, the Public, and Industry:

- Create an online portal for open communication between agencies, the public, and industry.
- Provide the ability for agencies to post technology problems to the portal.
- Allow for public and industry comments and suggestions in response to these problems. These comment threads will act as brainstorming sessions to provide the agencies with a variety of solutions, similar to the National Dialogue produced by GSA.[2]
- Provide industry with the ability to submit their new technologies and cyber requirements so that the agencies always have access to the most up-to-date information.

Identifying, Evaluating and Acquiring Effective Technology:

- Inventory existing activities that identify, evaluate, implement, and deploy new technologies and propagate best practices to increase these activities across the federal civilian space.
- Establish a dedicated cybersecurity operational test and evaluation effort to identify real-world effectiveness of technologies that can better secure government networks. This should include evaluation to compare legacy technologies deployed by government, existing technologies used by industry, new technologies, and those introduced by portal.
- Provide a centralized service by allowing test and evaluation effort to learn from and span across multiple agencies. Organizations such as In-Q-Tel for the Intelligence Community, DHS Science and Technology Directorate, and the National Labs already exist to support different agencies; we support creation of a centralized organization to reduce overlap and concentrate valuable resources toward addressing the highest priority issues.

[2] "Reporting and DATA Act Open Dialogue."IdeaScale. Web. <https://cxo.dialogue2.cao.gov/>.

IT Alliance for Public Sector
A Division of ITI

Issue 4: Outline Cyber Crisis Response Best Practices

Crisis response planning is a critical component of any security operation. Combined with protection and detection capabilities, appropriate crisis response activities can minimize the impact of an incident. Effective response planning takes place well in advance of an incident and considers a range of scenarios, capabilities, conditions, and environments. Effective planning also requires education, training, and exercises for all elements of a response plan. Similarly, evaluation of response actions and effectiveness of plans is critical to improving processes going forward. Lastly, accountability and traceability are critical to ensuring that processes and plans are improved, and improvement plans should be enforced and tracked to completion. To address these issues, the federal government should consider the following best practices and actions in order to ensure effective cyber crisis response.

Incident Response Keys:

- Given the complexity of federal government networks, including the reliance on both internal and external support teams to maintain systems and respond to incidents, there are often numerous teams involved in incident response activities. Consequently, it is critical that response teams coordinate activities to enable a more effective response, but also to ensure that important forensics information is preserved. Response teams should coordinate in advance to ensure familiarity with each other's common response procedures to minimize response conflicts and overlap that may disrupt or delay incident response.
- Typically, private sector organizations place incident response teams on retainer or are able to otherwise very quickly bring in surge incident response capabilities as an incident demands. Recognizing that government agencies may not have similar contracting flexibility, agencies should nonetheless review contracting mechanisms or vehicles (such as the United States-Computer Emergency Response Team (US-CERT) fly-away teams) to enable the rapid deployment of incident response surge capabilities.

Planning:

- Agencies should complete the development and implementation of integrated, cross-business unit (e.g., IT operations, business, privacy, legal, human resources, and vendors) cyber incident response plans. It is critical that those plans be finalized, promulgated, drilled, trained, evaluated, and improved. Top-down plans like the National Cyber Incident Response Plan or National Cyber Response Framework need to be finalized and promulgated so that agencies can understand and internalize, aligning with their own bottom-up plans.
- Plans should also include appended modules or annexes that feature pre-scripted mission assignments for the most common cyber-incident scenarios. Response personnel should be trained and drilled on those scenarios, and all agency personnel should be made aware of response protocols and any response responsibilities.
- Planning efforts and scenarios should consider the impact of degraded operating environments on the ability to respond effectively, including the loss of certain capabilities due to adversary activities. For instance, in a denial of service scenario, the ability to communicate internally and externally may be degraded, affecting the ability to coordinate and execute response actions.

- As incidents may vary in complexity, severity, and impact, organizational response accountabilities and capabilities will similarly vary. Accordingly, agencies should continue to maintain basic capabilities to respond to incidents. The government, led by US-CERT, should also broadly disseminate and build awareness around the escalation protocols (including escalation points and how to escalate) for incidents that exceed the capabilities of an agency or organization. Regardless of severity, under FISMA, agencies should be required to notify US-CERT of incidents in a timely manner dependent upon the severity of the incident.
- Escalation paths should similarly clearly define criteria for incident response stand down and de-escalation, ensuring that agency incident response personnel understand and are prepared to transition from response into recovery, evaluation, lessons-learned planning, and other post-incident activities.

Communication is Critical to Managing Response:

- Throughout an incident, it is critical that an organization have clearly defined communication protocols and processes. Incident response teams must coordinate actions and discoveries, communicating with senior leadership as well as dependencies, including partners, vendors, and customers. For example, vendors should be informed of anticipated or actual impact to contractual obligations and partners should be informed of impact to participation in dependent operations or engagements.
- Most importantly, agencies should have clearly defined plans to communicate incident information with the public, particularly in incidents where citizens' information is at stake. National security information and implications should be properly protected, as necessary.

Education and Training:

- Establish a consistent, government wide, standards-based training capacity for all government employees and measure the effectiveness of that training on a regular basis. This effort should include identifying and incorporating existing government training and assessing industry best practices for security training.
- Effective planning efforts are contingent upon the ability of personnel to execute the plans as intended. Accordingly, agency plans should be exercised and tested across relevant internal, vendor, and support personnel.
- Consistent with the concept that security is the responsibility of all employees, all agency employees should be educated and trained on general incident response planning concepts and any related responsibilities, including how to notify response organizations, the information to report, and other relevant activities.

Evaluation, After Action Reports, and Root Cause Analysis:

- All incidents, exercises, and general activities offer opportunities to learn and improve planning. Accordingly, observation and evaluation should be key components of any incident response structure, including the planning cycle. All personnel should be provided the opportunity to provide feedback on plans, training, and exercises.

- Exercise evaluation activities should be managed independently of the response organization, as there is a potential conflict of interest if the reviewing entity resides within or is subordinate to the operational entity. For example, US-CERT should not self-evaluate participation in exercises like Cyber-Storm. Instead, independent evaluation personnel with the appropriate expertise, like those available from the Federal Emergency Management Agency (FEMA) National Exercise Division, should be used.
- Agency evaluation and reporting protocols should include both quick-look evaluations compiled within the first several hours of an incident, in addition to comprehensive after action reports issued after a careful and thorough examination of an incident. Quick-look reports should be institutionalized, as they are valuable for stemming or mitigating the propagation of further incidents.
- After action reports should be accompanied by improvement plans that clearly identify the responsible implementer of improvement actions, and a clearly defined action plan should be put into place that tracks status of implementation. As evaluation programs mature and organizational planning processes increasingly integrate disciplines and functions (e.g., response, development, operations, business units, etc.), evaluation and learning should take place on a continual, parallel basis with regular opportunities to improve processes and protocols, rather than as a step or phase in a process or sequence.

Accountability:

- Any incident or breach with the possibility of a personally identifiable information (PII) disclosure should have an assigned privacy officer. The privacy officer should coordinate with the incident response, providing regular updates in synch with other elements of the response effort.

IT Alliance for Public Sector
A Division of ITI

Issue 5: Determining Responsibility and Accountability

The federal government too often has vague lines of responsibility and accountability. Understanding how business establishes clear lines of responsibility and whom to hold accountable in a cyber crisis would be beneficial to establishing better cybersecurity accountability in the federal government. The current lines of responsibility and accountability are not getting the desired results across the federal government as demonstrated through recent incidences occurring at federal agencies. Exact lines are blurred and in some cases may even present a potential conflict of interest, such as the CISO reporting to the CIO. There are some key actions that must be taken to improve the responsibilities and accountability for cybersecurity in the federal government. ITAPS recommends addressing cyber responsibility and accountability through people, governance, and the following next steps:

People:

- Ensure that federal government employees understand that information security is everyone's job and a condition of employment, understand their specific roles, and that information security will be an essential part of their performance reviews.
- Increase information security training and awareness at all levels and in all areas in the government (e.g., elected officials, appointed officials, senior executives, IT personnel, users, contractors) and the number of information security professionals.
- Establish protocols for, and encourage and incent federal government employees to use, a reporting mechanism for information security concerns or weakness within their department and agency first and then outside the standard chain of command (e.g., risk executive, IG, computer incidence response team) without fear of reprisal when normal processes are not providing necessary results.
- Increase the professionalism and provide additional incentives to the government cyber workforce by creating a separate career path and job series demonstrating the criticality and importance of cybersecurity throughout the government.

Governance:

- Require the establishment of an outcome-based Cyber Governance Framework to set direction, make decisions, provide oversight, and ensure transparency of management planning and execution of a cohesive, integrated cyber program for the federal government[3] as a whole; use the Framework to guide the development and implementation of frameworks for each department and agency.
- Establish for the federal government as a whole and at each department and agency an enterprise level review process by key stakeholders (e.g., executive committee, audit committee, steering committee, risk committee, enterprise IT governance committee) to review and approve policy, associated direction, requirements, and risk for IT and information security.
- The governance review process should ensure: 1) that the Cyber Governance Framework is established and maintained; 2) benefits and value are delivered; 3) risks are minimized; 4) resources (e.g., people, funds, tools, processes) are optimized; and, 5) stakeholder and management transparency.

[3] The overall federal governance entity should have very senior representatives and decision-makers with IT, risk, and cyber knowledge from the White House, OMB, DHS, DoD, OPM, IC, NIST, Cyber Command, and the IG community.

- Hold all personnel at all levels accountable for complying with security policies and fulfilling assigned cybersecurity roles and responsibilities; ensure this accountability is in job descriptions, personnel evaluations, vendor contracts, performance objectives, etc., with appropriate incentives and dis-incentives.

Next Steps:

- The immediate focus should be on establishing the Cyber Governance Framework for the federal government as a whole, with compliant department and agency-level frameworks to follow, ensuring objective assessments of current cyber risks, set direction across the government, prioritize remediation efforts and resource allocation, assign management responsibilities for execution, and establish tracking and oversight.
- Establish a RACI-type (responsible, accountable, consulted, informed) chart for the overall federal government and each department and agency that clearly identifies roles, responsibilities, and accountabilities for cybersecurity; publish and communicate with all shareholders (see people recommendation above) across the organizations; and maintain and enforce the RACI assignments (title and name where possible encourages ownership).
- Escalate security from merely an IT concern to a business risk concern, providing independence and enabling security decision-making and implementation. For example, make permanent a central Administration role with appropriate authorities and budgetary controls to direct and oversee cyber activities across the government, including leadership of a cybersecurity "council" for interagency coordination; separate agency CISO functions from CIO functions; establish a mechanism to escalate agency CISO security concerns directly to the department and agency head or central cyber function for adjudication as appropriate.
- Longer-term focus must include improvements in the five previously mentioned governance areas, as well as transitioning of the overall cyber program from one of detection and reaction to one of proactive prevention through continuous real-time monitoring, and adaptation of new tools, security intelligence, behavior, and predictive analysis.
- Adopt approaches that emphasize cross-organizational collaboration, transparency, accountability, and integration, reducing costs, minimizing operational risks, and driving continuous improvement (e.g., institute or adopt the security development lifecycle, NIST guidance and directives, international standards, and the DevOps method across agency operations, security, and development teams).

IT Alliance for Public Sector
A Division of ITI

ITAPS OPM-OMB-NSC Cybersecurity Task Force

Adobe
Steve Gottwals, Technical Director, Security Solutions
Matthew Schrader, Senior Manager, Government Relations & Public Policy

AT&T Gov. Solutions
Chris Smith, CTO

BlackBerry
Ed Hearst, VP, Government Affairs

CenturyLink
Brian Adkins, Senior Director, Legislative Affairs
Kathryn Condello, Director, National Security and Emergency Preparedness

CGI
Michael Lucero, Director, Cybersecurity

Fujitsu
Neil Jarvis, CIO
Mike Clauser, Government Relations

IBM
Jim Golden, Associate Partner, IT Governance & Cybersecurity
John Lainhart, Global Business Services US Public Sector Cybersecurity & Privacy Service Area Leader

Lenovo
Gerald Fralick, CSO
Tim Olson, Solutions Architect and Sales Specialist
Mario Rebello, Managing Director, US Government Relations

Lockheed Martin
Steve Hull, CIO
Sandee Throneberry, Defense Industrial Base Integration Lead
Jennifer Warren, VP, Technology Policy & Regulation

Microsoft
Pat Arnold, CTP, Consulting Services
Chris Krebs, Director, Cybersecurity Policy and Strategy

NCR
Tom Verbeck, Public Sector Strategy VP and CTO
Marija Zivanovic-Smith, VP, Global Government Programs

Oracle
Geoff Green, VP, Business Development Executive

Palo Alto Networks
Ryan Gillis, VP, Cybersecurity Strategy and Global Policy

EMC/RSA
Matt McCormack, CTO, Global Public Sector
David Colberg, Director, Government Affairs & Public Policy

SAIC
Jonathan Jowers, CISO
Amy Childers, VP, Government Affairs

SAP
Greg Chapman, Senior VP, Federal, Aerospace & Defense
Mark Whittington, VP, Channels and Alliances
Tom Sisti, Senior Director & Chief Legislative Counsel

Schneider Electric
Jay Taylor, Director, Global Standards, Codes, and Environment
George Wrenn, CSO

Symantec
Jeff Greene, Senior Policy Counsel, Cybersecurity and Identity

VMware
Steve Coles, VP, Public Sector
Dennis Moreau, Senior Engineering Architect
Charles Saroka, Staff Systems Engineer
Patty Stolnacker-Koch, Director, Government Relations