



December 15, 2016

President-elect Donald J. Trump  
Office of the Presidential Transition  
1800 G Street, NW  
Washington, D.C. 20006

Dear Mr. President-elect:

Congratulations on your election as the 45<sup>th</sup> President of the United States.

The IT Alliance for Public Sector (ITAPS)<sup>1</sup>, a division of ITI, is composed of the leading technology hardware, software, services, and solutions companies offering the latest innovations to the federal government marketplace. We are committed to working with you to improve government operations and efficiency and commend you for setting cybersecurity as a top priority for your Administration.

Our organization has worked diligently in the past few weeks to convene our experienced and talented member companies to develop the following recommendations. These address a short and long-term, multi-pronged effort to address the information technology challenges in the federal government during your Administration. We look forward to the opportunity to discuss these recommendations in greater detail with you and your team.

### **Background**

Information technology (IT) is the platform for the daily functions of every civilian agency and the armed forces in order to complete their missions on behalf of the American people. Several high-profile and damaging incidents of cyber-attacks on the federal government have, however, revealed the serious risks cybersecurity vulnerabilities in older IT systems pose to government operations and the security of our country. We believe that achieving government-wide cybersecurity is interdependent upon two other imperatives: IT modernization and acquisition overhaul. Without them, “cybersecurity” can be no more than a tagline.

Last year, the federal government spent \$80 billion on IT. Shockingly, 80% of that funding is spent on maintaining costly, vulnerable legacy IT systems<sup>2</sup>. Rather than investing in new technologies to maintain U.S. supremacy, the federal government is caught in a destructive cycle of spending tens of billions of dollars to only sustain IT systems - effectively and consistently missing the opportunity to modernize.

Further exacerbating the current federal IT condition are technology cycles that are measured in years, while business and tech sector cycles are measured in days and weeks. The lifecycle of federal IT initiatives frequently take so long to realize that by the time they are complete, the government has

---

<sup>1</sup> **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](http://itaps.itic.org) to learn more. Follow us on Twitter [@ITAlliancePS](#).

<sup>2</sup> <https://hurd.house.gov/media-center/press-releases/rep-hurd-connelly-sens-moran-udall-introduce-move-it-act>

purchased outdated technology. Government procurement and appropriations processes make these cycles even longer, delivering some capabilities years after they are envisioned. This dynamic must change and government must adopt rapid prototyping and development operations like those in industry and migrate capabilities to the cloud where appropriate.

To move the federal government away from employees searching for spare parts to keep these systems operational, and to achieve your goal of cybersecurity and a modern government which best serves and protects the American people, we must recognize that: perpetual maintenance of federal legacy IT systems is suboptimal and inefficient; that appropriations and procurement processes hobble effective IT investment; and, achieving greater cybersecurity is interdependent with solving these other challenges, as well. To achieve these goals, we would recommend the following:

### Cybersecurity Through IT Modernization

Cybersecurity isn't a standalone goal; it cuts across IT programs as an embedded element. Too frequently, however, cybersecurity has been approached in the federal space as a standalone goal, addressed as an after-thought or a bolt-on solution in efforts to better protect legacy IT systems. The tech sector does not consider or use such options as best practices, except temporarily in extreme or urgent vulnerabilities, and instead we would recommend a focus on achieving cybersecurity as one of several advancements that can be derived from IT modernization.

What we know of the inventory of information systems operated by the federal government is that they are typically old, expensive to maintain and repair, and represent a substantial cyber vulnerability. These systems also require unnecessarily high staffing and funding levels, and leave vital government operations open to cyber-attack. Budget dollars that could be invested in IT modernization, cloud migration, or cybersecurity are instead overwhelmingly directed into the operation and maintenance of these antiquated systems.

*Get a clear picture of the hardware and software assets the federal government uses.*

**Recommendation: Direct agencies to create within 90 days a complete inventory of IT systems, hardware, and software and identify those systems that are subject to increased vulnerability.** Such an inventory should include an assessment of the cyber-risk each system poses, the cost of operating such a system, including legacy cost drivers and a value assessment of the system in the context of the agency mission. Such a starting point would afford the new Administration the ability to prioritize systems most in need of modernization.

*Government personnel must become more tech-savvy.*

**Recommendation: Make agency cybersecurity a personal responsibility for government personnel, provide more robust training opportunities for cybersecurity, and create a more tech-savvy workforce.** President-elect Trump has said changes are needed in the federal workforce and we must ensure that the personnel in public service are better able to obtain the skills and knowledge necessary to identify, acquire, deploy, operate, and protect modernized IT systems. Personnel must be held accountable when cyber failures occur, but they should also be regularly trained as industry personnel are in regards to best practices about how to manage this risk. They must also be provided ongoing opportunities to learn about technology and innovation. An effective means for such an objective that industry would support is more robust personnel exchanges, where industry personnel and government employees switch places to better understand and appreciate the operations of their counterparts, the technologies, and the

technical needs of the agency mission. Such an exchange can be made a career requirement for anyone involved in the procurement, acquisition, operation, or cybersecurity of government IT systems.

### **IT Modernization Through Reform**

To achieve greater security and maintain the United States' technological superiority, policymakers must take steps to address dysfunctions in the government acquisition and procurement system and the appropriations process. Simply put, both are antiquated and designed to acquire goods and services in a time that predates the advanced capabilities now widely available, like mobile and cloud computing, the internet of things, and artificial intelligence, and neither can match the pace of innovation. While we recognize true reforms will also require Congressional action—and we encourage you to work with lawmakers to do so—your Administration can also take needed actions as well.

A key symptom of dysfunction in the acquisition and procurement process and the appropriations process is the extended lifecycle they create in the federal government. The disconnect in timing impedes the government's ability to gain timely access to innovation readily available in the IT industrial base. It is also imperative because our adversaries do not have such impediments to their ability to access the same technologies and capabilities.

*Acquire improved technological capabilities with better requirements that deliver outcome based solutions.*

**Recommendation: Use existing authority to better manage desired outcomes in IT acquisition and management.** Authorities are already in place to better manage how government should evolve to see IT: as a central mission capability enabler and not as a back-office system or an information deliverer. Agencies should assess their needs and enable industry to identify and deliver solutions-based capabilities. And, agencies should be encouraged to collaborate with industry on prototyping, co-development, and testing so industry and government can work together to deliver the desired capability based outcomes.

*Leverage existing acquisition and procurement reviews to make changes in the process for IT.*

**Recommendation: Work with Congress to expand the authorization and support for the Section 809 Panel.** Congress has already begun the work of assessing the state of acquisition and procurement, but only for the Department of Defense. The panel's authority should be made government-wide and adequate resources should be provided to develop recommendations for action. Such a top to bottom review of statutes and regulations, with an eye toward enabling government acquisition and procurement for the information age, are critical to assessing what changes are necessary.

*Rapidly adopt new funding options for IT investment that can be used this fiscal year.*

**Recommendation: Work with Congress to quickly adopt proposals to create greater IT funding flexibility.** Our dysfunctional appropriations process contributes to the unacceptable state of cybersecurity and information technology in the federal government. Because of budget cycles and Continuing Resolutions, agencies are hobbled in their ability to effectively plan for modernization and obligate funding when it is needed to acquire and deploy capabilities. The disconnect impedes the government's ability to gain timely access to innovation readily available in the IT industrial base. Congress has already worked to advance proposals that will create funding flexibility through incentives for agencies and the reinvestment of savings and we would encourage your Administration to move quickly for passage of these initiatives to make funding efficiencies available to agencies in this fiscal year.

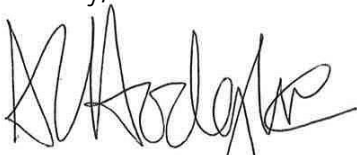
*Improve the regulatory compliance regime for all in the industrial base.*

**Recommendation: Conduct a top to bottom review of procurement regulations that impose government unique requirements, while suspending work-around programs designed to deliver technology through circumvention of the acquisition and procurement process.**

Such an assessment should seek to identify and make recommendations to revise or remove government unique requirements that distort or create barriers to entry and sustainment in the market. These should include imbalanced set-aside policies, contract flow down clauses, and other artificial market distortions away from commercial item preferences and practices. Instead of addressing these systemic challenges and root causes, government has instead begun to focus on ways to work around existing procurement and acquisition requirements still imposed on traditional vendors with the creation of small scale programs (Digital Services, 18F, DIUx, etc.) to develop technology for government consumption. Some of these initiatives have also used waivers and exceptions to requirements for technology providers that are new entrants to the market. This work around tactic does not address the underlying problems, and, if some regulations and compliance requirements make delivering innovation or cybersecurity a challenge or even a barrier, then they should be treated as barriers to all in the industrial base and should be marked for revision or repeal. By addressing these root causes and removing the barriers and burdens they create, acquiring technology should become easier and be more efficient for federal agencies.

Mr. President-elect, we are fully aware that any one of these – Cybersecurity, IT Modernization, or Procurement and Acquisition Reform – is a substantial effort by themselves. But, we believe that these elements are closely intertwined, and without addressing all three, we cannot position the federal government or its' IT capabilities where they need to be in the 21<sup>st</sup> Century. Thank you for your attention to our recommendations. We would welcome the opportunity to discuss these recommendations in greater detail with the appropriate members of your transition team and to work with your Administration on achieving these outcomes going forward.

Sincerely,



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