ITI Promoting Innovation Worldwide

Written Testimony of

Gordon Bitko
Senior Vice President of Policy
Information Technology Industry Council (ITI)

Before the

Subcommittee on Government Operations

of the

Committee on Oversight and Reform

U.S. House of Representatives

Federal IT Modernization: How the Coronavirus Exposed Outdated Systems

July 20, 2020

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Written Testimony of
Gordon Bitko
Senior Vice President of Policy
Information Technology Industry Council (ITI)

Before the
Subcommittee on Government Operations
of the
Committee on Oversight and Reform
U.S. House of Representatives

Federal IT Modernization: How the Coronavirus Exposed Outdated Systems

July 20, 2020

Good afternoon Chairman Connolly, Ranking Member Hice, and distinguished members of the committee. Thank you for inviting me to testify today; it is a privilege to discuss federal IT modernization issues with you. My name is Gordon Bitko, and I am the Senior Vice President for Public Sector Policy at ITI, the Information Technology Industry Council. I have been in my current role since November 2019. Prior to that, I served for more than twelve years at the Federal Bureau of Investigation (FBI) and was honored to conclude my career at the FBI as that agency's Chief Information Officer (CIO); a position in which I served for three and a half years. Additionally, I have spent time as a policy fellow focused on technology policy issues at the RAND Corporation and worked as an engineer and engineering manager at both large and small technology companies. The compilation of those experiences has made me acutely aware of the challenges and opportunities confronting federal information technology (IT).

ITI works with policymakers in the United States (US) and globally, on behalf of more than 70 of the world's leading information technology and cybersecurity companies, to develop policies and regulations that promote innovation and growth. ITI believes that in an increasingly digital world, it has never been more important for the US government and our member companies to work together to promote effective government through technological leadership. The US public sector must leverage private sector innovation and leadership by adopting policies that enable government agencies to more easily use commercial products and practices that provide agility, scalability, and elasticity that support the enormous growth in demand for digital services and data.

Let me start by providing context for why I believe IT modernization is so essential, through a practical example. During the April 2013 Boston Marathon bombing investigation, the FBI collected approximately 50 Terabytes of data. Less than 5 years later, the October 2017 Las Vegas shooting investigation collected about 1 Petabyte of data, or about 20 times more than in the Boston investigation. These numbers are so big they are hard to understand, but here's another way to think about them: 1 Terabyte is about 500 hours of high definition movies, and 1 Petabyte is 500,000 hours, or 57 years, of HD movies. The FBI's systems struggled to ingest, process, and analyze information at this scale, and link it to other data in other systems. In extraordinary circumstances, such as those 2 incidents, the FBI is able to surge hundreds of people to review the evidence and case information, but doing that on a more routine basis is just not practical.

As important, what was extraordinary in 2013 is normal today. Popular mobile phones can record video at a 4k resolution. In just two months, one 4k camera on a phone, recording continuously by itself, can capture as much data as the entire Boston bombing investigation. Couple this with the proliferation of other data: cyber threats among huge volumes of Internet traffic, social media content, online transactions, as well as Internet of Things devices. It is clear that the FBI's and every federal agency's ability to accomplish its mission is inextricably linked to a technology infrastructure with the ability to manage and analyze data at speed and scale.

The imperative to modernize is true at every government agency, and the ongoing pandemic, with its vast increase in remote work, has only accelerated the need for change. The ability for federal agencies to shift to large-scale telework during COVID-19 is the result of the transformative activities of recent years, such as migration to commercial providers for at least some critical infrastructure and services.

But as I noted, government agencies cannot stand still and it is not enough to only evolve incrementally in the face of exponential change. Stressed enough, legacy systems can fail catastrophically; not gracefully like well-designed modern cloud and hybrid systems. We saw this in state unemployment systems that crashed under duress at the start of the pandemic. In the federal government, agencies are also not immune to this risk. Many still provide critical services through systems designed and built decades ago. Providing the quality of services that Americans expect and deserve means these systems must modernize to do more better and faster. Federal technological transformation can only happen if there is consistency in and dedication to

providing both funding and addressing the policies and practices that restrain innovation and modernization in government information technology.

The complexity of understanding how to compete for government business, the inherent agency and subject expertise needed, the stove-piped legacy systems, and the challenges that restrain government CIOs from planning for the long term all serve as inhibitors to innovative ideas and transformation. I'd like to highlight four areas of significant challenge that, in my experience, made it unnecessarily difficult for government to embrace and make full use of the best products and services that are available from innovative private sector companies.

1. *General bureaucratic processes, culture, and risk aversion, especially in the procurement process, still hampers government IT modernization.*

   The Department of Justice (DOJ) experience with data center consolidation offers a helpful example. The Federal Data Center Consolidation Initiative (FDCCI) dates back at least to 2011 and DOJ's efforts to centralize data centers began in earnest in 2014. DOJ's strategy entailed consolidating all legacy DOJ data centers into three core facilities, of which two would be owned and operated by the FBI. It was decided that one of the two FBI facilities was to be constructed at an existing FBI location in Pocatello, Idaho. An RFP for the project was posted in February 2016 and awarded a year later, in February 2017. Groundbreaking occurred in October of 2017, the building opened in November 2019, and full operation is currently scheduled for September 2020.

   In government, this is generally considered to be a successful program. It has delivered a new facility that will enable DOJ to close legacy data centers. As such, the department's data center metrics will improve and some applications will modernize.

   However, while this represents marginal progress, the reality is that the FBI's latest data center will never be a state-of-the-art facility. In just a few months, the FBI will be operating a data center that is considerably out-of-date. In 2018, commercial providers that were consulted about providing some services from the then-under construction data center declined to do so. The did so because by that time—a full two years prior to it being brought into regular use—the facility had already fallen short of the private sector's more advanced technical requirements. Once open, this new data center will

likely end up hosting legacy systems that were never budgeted for modernization. Meanwhile, many of the systems that had been provided with the resources to modernize will instead migrate to commercial providers with investments in innovation and resources that dwarf what the DOJ, itself, has been able to make.

Limited technical and contract expertise, risk aversion, process inefficiencies, unpredictable funding, and inflexible construction processes all contribute to timelines in government that are much longer than commercial best practices. At the same time, the lack of multi-year IT modernization funding means that legacy applications endure far longer than they would in almost any commercial environment.

2. *Federal workers in many of the programmatic disciplines central to technology—including cybersecurity, IT program management, and procurement—need to be better equipped and empowered to effectively drive government IT advancement.*

   Federal professionals in areas crucial to technology transformation are too often overworked, at risk of burning out, not as well trained and equipped as they should be, and are frequently compensated less than their peers who perform the same work in the private sector. As a result, technical knowledge in most areas today resides as much with contract staff as with government employees. Those dedicated professionals who choose to remain in government service also often become more risk averse due to the structures, norms, and rules that are in place, as well as a lack of empowerment to make bolder and more transformative decisions.

   For example, not long before I left government, procurement lawyers at the FBI advised that the Bureau would not be able to procure some commodity hardware products and services with multi-year maintenance using annual appropriations. They warned that doing so would be a violation of the Antideficiency Act. Instead they required the vendor to sell the product without the multi-year maintenance, despite the fact that it was being widely provided in that fashion as a commercially available off-the-shelf (COTS) item through a Governmentwide Acquisition Contract. Decisions like this result in significantly more overhead for vendors who must administer to the unique requirements and decisions of multiple agencies, in addition to higher prices for the government.

The Antideficiency Act was also frequently raised as potential challenge in the procurement of consumption-based cloud services, absent any new government wide guidance for how to obtain those services.

3. *True long-term and strategic planning around technology is too often difficult or impossible in the federal government.*

   Evolving priorities, frequently changing agency leadership, annual budget cycles, and IT governance processes that do not reflect the reality of agency IT challenges all create incentives that are not aligned with true and effective transformation. Rather than delivering quality services or implementing effective modernization and evolution of systems, spending a current year's appropriations before they expire frequently becomes a top priority. Similarly, federal tracking of capital investments and traditional waterfall program management processes deemphasize the importance of modern continuous software delivery leveraging best-in-class commercial products.

4. *The sheer number of monolithic and highly customized information technology systems on which government agencies depend further complicates and hinders sound approaches to federal technology.*

   Customized systems, like those found throughout the federal IT arena, place great constraints upon agency operations. These systems often implement proprietary processes that exist largely because of historical decisions and, even more concerning than their limiting effect on operations and progress, the high degree of customization means that they are often the last to see security fixes.

   The FBI system to track time and attendance uses a commercial product. However, at the time the FBI migrated to that product, rather than re-evaluating the time and attendance process and adopting commercial capabilities, the decision was made to customize the product to the FBI's specific requirements. As a result, a custom time and attendance system resides on an internal FBI network, where it is not directly accessible when out of the office. Further, because of the level of customization, nearly every major update has occurred at or past the end of life for the prior version of the product and has come uncomfortably close to an outright failure several times.

There are many excellent professionals throughout government working hard to deliver quality information technology capabilities. And all agencies each have some unique mission needs that simply cannot be solved with a COTS product. But the reality is that it is often too hard for agencies and IT professionals to get to the front lines of core problems and focus on those needs in a rational, efficient, and effective manner. They are frequently distracted or preempted by issues and needs arising from legacy systems and processes in areas where commercial capabilities could be effectively utilized, but are not.

There are specific steps that would help, in order for agencies to maximize the time on front-line challenges. Agencies and federal IT professionals should be encouraged to seek every opportunity to not reinvent the wheel, and instead leverage commercial services that can be provided at speed and scale, both within and across agencies. The government must define objectives, and then empower federal IT professionals to partner with industry to deliver and maintain those services. Where and when federal agencies have done so, the result has often been very successful. Whereas when the government has defined many complex and prescriptive requirements, particularly without first scrutinizing the underlying and often dated business processes involved, the resultant overhead of customized solutions has frequently made them late, over budget, and under-used.

Such a forward-looking, strategic approach shouldn't just apply to infrastructure computing. It can and should include services such as secure networking, identity management, help desks, and others. In each of these areas, when government leaders clearly define objectives and then place responsibility on industry to deliver and maintain those services, world class services will become far more common inside of government. It will drive competition by leveraging standards, and it will encourage innovation by opening larger government markets to companies that have not traditionally seen the federal market as worth their while, due to the complexities of agencies as well as other risks and hurdles.

At the same time, the IT budget and acquisition processes must evolve. Agencies, and particularly providers of shared services, will need to be funded appropriately and should adopt a customer service mindset. Federal professionals must be allowed and empowered to leverage commercial capabilities and approaches in a timely fashion.

Transformational change also requires long term commitments. The failure of many agencies to fully adopt Working Capital Funds, as well as the shortcomings of the annual budget cycle mean that agency IT planning staffs spend far too much time managing the budget process, and far too little ensuring that the right sorts of projects and programs are sufficiently funded and well managed.

At the same time, those IT planning staffs should more widely adopt a continuous delivery mindset. They should define and manage projects based on objectives and outcomes, on the velocity of capability delivery that improves the mission, and the consumption of those services and features by users, both within and outside the agency. IT projects should not be managed based on activity, or on waterfall project schedules. Finally, the government's processes for managing IT investments, such as the FITARA scorecard and the federal IT dashboard, should be updated to reflect the modern realities of IT development as well as sound IT policy and administration of federal technology efforts.

Thank you again for inviting me to appear before this committee. I look forward to your questions.