SIIA Accelerating Innovation in Technology, Data & Media

202.289.7442
www.siia.net

1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905

18F and U.S. Digital Service Oversight

David LeDuc
Senior Director, Public Policy
Software and Information Industry Association

Statement before the Subcommittees on Information Technology and Government Operations of the House Committee on Oversight and Government Reform

June 10, 2016

Chairman Hurd and Chairman Meadows, Ranking Members Kelly and Connolly, and members of the Subcommittee, on behalf of the Software and Information Industry Association (SIIA), thank you for this opportunity to testify before you today to discuss 18F and U.S. Digital Service (USDS) Oversight.

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital information industries. The more than 700 software companies, data and analytics firms, information service companies, and digital publishers that make up our membership serve nearly every segment of society, including business, education, government, healthcare and consumers. As leaders in the global market for software and information products and services, they are drivers of innovation and economic strength—software alone contributes $425 billion to the U.S. economy and directly employs 2.5 million workers and supports millions of other jobs.

Introduction

SIIA Commends the Obama Administration for its work to update and enhance the Federal Government IT Framework, which has strived to evolve federal IT to a more modular, agile, cloud-focused approach, and we support much of the core mission of both the USDS and 18F.

For many years, SIIA has been a strong supporter of the Obama Administration's efforts to modernize federal IT. From early initiatives to open Federal data, to having federal agencies use, buy and share cutting-edge solutions, and continue the significant progress we have seen over recent years to enhance the way government uses technology to serve the American public.

SIIA supports the goals of 18F to help agencies buy, and share efficient and easy-to-use digital services. For instance, SIIA supports 18F's core objectives and efforts to take a flexible, customer-centric approach, where federal IT acquisitions can be faster, cheaper, and produce better results. 18F is potentially well suited to help agency customers identify and use innovative technology, where they can apply technical advice to help agencies develop new requests for quotation for IT services.

For instance, 18F is well served to work with federal agencies to help write agile, modular, and user-centered design into agency requests for quotations, the development of a marketplace for Federal agencies to buy IT services using modern techniques, as well as their work with agencies to provide data sets for the public to search, understand, and share government data.

These are just a few examples of how 18F is able to help federal agencies through its innovative, customer-centric approach. However, we also have several questions and concerns about 18F, such as 18F's "build custom" IT approach, their ability to operate outside of the traditional procurement process, the lack of transparency surrounding cost coverage and the recent reorganization of 18F within the Technology Transformation Service (TTS). These questions and concerns are highlighted below, along with recommendations to help guide 18F towards the well-intended goals of the organization.

1. **18F's focus on "build custom" departs from the longstanding reliance on a "buy, not build" IT procurement policy, presenting both unnecessary competition with the private sector and the risk of a legacy of "government-off-the-shelf solutions."**

   At the May 25th hearing before this Committee on Legacy IT, Federal CIO Tony Scott reiterated the Administration's commitment to rely on the "buy, not build" approach, saying, "we're encouraging the buying of services rather than developing them themselves."

   This "buy, not build," or COTS-first approach is a long-standing, critical component of Federal IT policy. For instance, the Administration's Shared Services Strategy emphasized the key role of commercial organizations in providing the actual IT shared service to agencies, in the context of growing use of commodity IT, modularity, and "open solutions," while reducing duplicative support. The issue goes deeper than that one policy, however. As the update to Circular A-130 clearly puts it to agencies, "All IT systems and services operate only vendor-supported solutions, and planning budgeting activities incorporate migration planning and resourcing to accomplish this requirement."[1] Why? As OMB has said consistently, choosing a vendor-supported solution avoids the risk of agencies pursuing "government-off-the-shelf" solutions, and recognizes that agencies often lack (and are challenged to maintain) consistent and necessary IT management staff. They also benefit from economies of scale, among other advantages, when choosing vendor-supported commercial-off-the-shelf solutions. Vendors—whether the IT product is proprietary or open source—are in the best position, working with their agencies customers, to provide relevant updates, assurances of security, and performance.

   However, 18F has taken a different fork in the path, focusing on a "build custom" approach to develop new solutions that are likely to require sustained, meaningful and experienced support plans, which are not necessarily available as part of solutions provided by 18F. The importance of ongoing support for agency solutions cannot be overstated, and agencies cannot afford for it to be overlooked.

   As a result, U.S. technology companies face direct competition from a government-backed entity. Private sector providers, who in many cases may be capable of providing a better, more secure product at a cheaper price, run the risk of being effectively excluded from 18F initiatives. Competition from 18F can only be expected to grow stronger over time, and this particularly affects small businesses.

[1] OMB. Proposed update to Circular No. A-130, *Managing Information as a Strategic Resource.* Oct. 21, 2015.

Additionally, 18F expanded its consulting and acquisition services earlier this year to assist federal agencies that provide grants to state and local programs, essentially offering the same consulting and acquisition services to states and local governments as it does to federal agencies. This expansion of services beyond the Federal Government raises a serious question about the role of the Federal Government in picking technology winners and losers, and in some cases is likely to present competition with private sector vendors who already invest heavily in the state and local market.

2. **18F has the ability to operate outside of the traditional procurement process, with a dual role to design agency procurements, and to compete for the opportunity to provide agency solutions, without sufficient transparency and oversight.**

   18f has largely been marketed as a solution to agencies looking to update and modernize their outdated IT, particularly where agencies are hamstrung by outdated procurement policies. In their own terms, 18F has been characterized as "passionate about 'hacking' bureaucracy to drive efficiency, transparency, and savings for government agencies."[2]

   As I said at the outset, the objectives to modernize IT to more modular, citizen-centric solutions, are widely shared. But in many cases it is the policies themselves that are in need of fixing, rather than a new federal consulting entity with the ability to sidestep (or interpret as convenient) the regulations and policies that IT vendors are forced to comply with.

   Perhaps most concerning, 18F combines policy-making functions, operations and promotion of their own product and service sales. As currently structured, 18F has a unique role working alongside agencies to help them craft RFPs and purchase agreements. This is an area where there are many questions about the operation of 18F and not many answers due to the lack of transparency around 18F to date.

   Indeed, it appears that 18F could be deployed to design acquisition plans and RFP's, and then have an opportunity to respond, often before the RFP's may even be announced. There appear to be no restrictions on 18F from being engaged by agencies to address specific problems with IT projects, essentially a sole source consultancy.

   This multi-purpose structure enables 18F to both influence the expansion of their own services while charging the agency who is paying for these 18F implementation services, ultimately eliminating competition by self-selecting their own people and

[2] 18F. "*Hello, world! We are 18F*." March 19, 2014.

mapping their own capabilities and technology preferences to an agency's digital delivery goals. The end result is not likely to achieve the best value for agencies, and it ignores innovate ideas from outside government.

Private sector IT solutions providers doing business with federal agencies must demonstrate their compliance with critical security requirements, such as FISMA security certifications or the often onerous FedRAMP approval process. For instance, the Federal Government has moved to ensure that federal cloud service providers are required to obtain FedRAMP certification in order to compete for government business. The FedRAMP certification process is long and expensive for cloud service providers (CSPs) averaging more than 12 months and costing millions of dollars.

But there is a lack of clarity, and potential oversight, around 18F's development and offering of cloud services as a CSP. Their Platform as a Service (PaaS) solution, Cloud.gov, was recently announced as "FedRAMP Ready," a step that indicates a CSP is ready for agency or FedRAMP Program Management Office (PMO) detailed reviews required to become "FedRAMP Compliant" and gives agencies the confidence that the SSP documentation meets the FedRAMP PMO's quality and security standards that are necessary to initiate the assessment and authorization process with the Joint Authorization Board (JAB).[3] Given the substantial challenge the FedRAMP approval process poses to private sector CSPs, the review of Cloud.gov should be an independent process, no less rigorous and not be prioritized over private offerings because of the proximity and close working relationship of 18F and FedRAMP within GSA.

There is also the broader question of why 18F chose to create Cloud.gov when there are already other commercial-off-the-shelf platforms available? According to the Cloud.gov project lead, "18F is going to be a model CSP in the federal space," and "Cloud.gov is only part of the equation."[4]

Additionally, of particular concern for this Committee is the risk that 18F could negate the steps taken to establish appropriate agency CIO oversight established in the Federal Information Technology Acquisition Reform Act (FITARA). As directed by OMB, FITARA seeks to "Strengthen the agency CIO's accountability for the agency's IT cost, schedule, performance, and security" and establish "common baselines" for roles, responsibilities and authorities of agency CIOs.[5] Yet, in many respects, it appears that 18F operates outside these parameters, ones which this Committee spent years defining and establishing through statute.

---

[3] Fretwell. "Cloud.gov gets FedRAMP ready." *Govfresh*. June 5th, 2016

[4] Ibid.

[5] OMB. "Memorandum for Heads of Executive Derpatments and Agencies." *Management and Oversight of Federal Information*. June, 2015

3. **18F must be required to cover its costs in offering agencies IT services, but transparency is currently lacking in this area.**

   Services provided by 18F, which are provided on a fee-for-service basis, charged to agency customers, not only pose direct competition with existing private sector services, but they are currently lacking transparency on whether costs are fully recovered. In the absence of transparency in this area, 18F is operating outside of parameters that are required for private sector vendors doing business with federal agencies. 18F should be required to provide detailed assessment of services provided, as well as revenues and expenses to demonstrate whether they are covering costs—and if not, they should be required to provide a plan for cost recovery in the near future. The private sector IT providers with which 18F competes with are forced to document their cost and expenses and ultimately must cover their costs.

   Without sufficient transparency in this area, it is difficult to make an apples-to-apples comparison between 18F's services and private sector entities who provide similar solutions.

4. **The unanswered questions and lack of transparency are particularly concerning given the expansion and recent GSA reorganization of 18F.**

   18F launched in March 2014 as a 15-person team of innovators, designers and developers recruited from the private sector to improve the government's digital services. Since then, the unit has grown to a total of 183 personnel across four offices nationwide.

   The Administration is moving to embed and make permanent the 18F program quickly, without seeking input from Congress or working with other agencies, and without addressing the issues identified above. Just last month, GSA announced the creation of the TTS, a new unit composed of 18F, the Office of Citizen Services and Innovative Technologies and the Presidential Innovation Fellows program.[6] The new organization was described by GSA Administrator Denise Turner Roth as a "launchpad to set us up for the next big expedition for the federal government in technology."

   This is highly concerning given the unanswered questions about process, cost and competition. 18F should undergo the traditional oversight and scrutiny by both Congress and the Administration to ensure that 18F will stay within a well-defined, designated lane as an internal government IT consulting service.

   Further — 18F, the Office of Citizen Services, USDS & PIF — are serving as a model for agencies throughout the government. There is an opportunity to provide oversight,

[6] Moore. "GSA Announces New Governmentwide Tech Unit that will House 18F." *Nextgov*. May, 2016

and perhaps give direction to how these organizations should be implemented and managed.

Conclusion

There is no question the federal government needs to update and modernize systems, and there is value for the Government to maintain a cadre of technical experts who can assist agencies in developing their plans and 'common baselines', but these objectives should not come at the cost of competing with private sector providers who operate in a competitive environment. Nor should 18F be able to operate without adequate transparency and oversight.

The establishment of a federal digitization team is a good idea for agencies, but there is an open question about the boundaries and the necessary oversight and the ability to ensure that 18F does not in fact raise costs to the Government or result in products that lack sufficient support. GSA should be able to better explain the value of an internal government consulting service and product sales function that operates through a competitive fee-for-service business model.

In closing, following are three key requirements to help guide 18F towards the well-intended goals of the organization:

- Greater transparency on cost and process,
- Adherence to the current "buy first" approach of commercial-off-the-shelf products, consistent with Federal government IT policy,
- Requirement to function by the same rules as other IT vendors, needing to provide for the same level of scrutiny and completion on costs.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: David LeDuc

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

N/A

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

Software and Information Industry Association (SIIA)
Senior Director, Public Policy

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

N/A

I certify that the above information is true and correct.
Signature: Date: June 10th, 2016

David LeDuc
Senior Director, Public Policy

David is a veteran of public policy and the technology industry, and a leading industry strategist. As SIIA's Senior Director for Public Policy, he leads SIIA's Technology Policy Committee, where he is responsible for working closely with member companies to develop and promote SIIA's public policy priorities across a wide range of information technology issues, including privacy, cyber security, cloud computing, open standards, e-commerce, e-government and information policy. David represents the Association before Congress, the Administration, and he advises member companies on policy outcomes, political strategy and best practices. He recently authored public policy white papers on Data-Driven Innovation and Cloud Computing.

David has been instrumental in the development of policies to promote the software and digital content industries dating back to the late 1990s. He began representing the technology industry as a government affairs manager for the Software Publishers Association. Prior to that, David worked on Capitol Hill implementing political public affairs campaigns.