Questions for the Record

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

Before the Hearing of the
Subcommittee on Government Operations
of the
Committee on Oversight and Reform
U.S. House of Representatives
on July 20, 2020:
Federal IT Modernization: How the Coronavirus Exposed Outdated Systems

Submitted August 13, 2020

—

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

1. Based on your experience as the former Chief Information Officer (CIO) for the Federal Bureau of Investigation (FBI), how important is it for agencies to have documented modernization plans for legacy systems?

As the former Chief Information Officer (CIO) for the Federal Bureau of Investigation (FBI), I was responsible for working with agency technical personnel responsible for system development and maintenance (i.e. "system owners") to establish modernization targets for legacy systems. These targets focused on improving both performance and security. In some cases where either the business case or security risks did not support modernizing an existing system, my office and I worked with system owners to retire and decommission those outdated legacy systems.

When doing so, it was imperative to establish and work from a defined enterprise plan. Modernizing an agency's legacy IT systems works best with a holistic rather than system-by-system approach that enables priorities to be set both across and within systems. Establishing security and performance metrics at the enterprise level that flow down to individual systems is key. For example, agencies should focus on developing a system for automated enterprise logging and monitoring of systems to identify and address security threats. Once a centralized logging methodology is established, all future system development

must include a requirement to provide logs to the centralized capability. Legacy systems that do not already share security logs are a significant security risk and, accordingly, must be modernized to do so.

By starting with an enterprise modernization plan based on well-defined requirements and standards (e.g. all systems shall be configured to share logs with an enterprise monitoring capability), agencies will be able to quickly articulate modernization requirements for legacy systems, including making data-driven retirement decisions for systems that cannot be reconfigured to comply with enterprise security and performance standards.

Without a documented plan, agency modernization efforts are likely to suffer from sporadic leadership support arising from turnover and inconsistent funding due to shifting priorities. At the same time new systems will come online in mission centers (so-called "Shadow IT"). In the absence of enterprise standards and plans those systems only exacerbate agency-wide IT challenges.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

2. What makes an IT modernization plan effective and ultimately successful?

Successful plans should approach IT modernization on an enterprise scale rather than focusing on individual needs for legacy systems. They should be based on enterprise standards and focused on continuous delivery of capabilities that strike a balance between improved business or mission performance and improved technology. If agencies do not coordinate legacy system modernization based on enterprise requirements, they risk creating a "patchwork" of systems that do not communicate well with each other and do not meet technical and security standards. This situation drains limited technical resources, increases costs, and contributes to security vulnerabilities due to siloed systems.

A successful IT modernization plan is also not simply about replacing outdated gear with new equipment. If agencies do not coordinate priorities with mission and business centers, they will certainly fail to achieve the necessary buy-in across the organization. The real value of modernization comes from working with those stakeholders and leveraging IT capabilities to improve business processes and operational capabilities. For example, modern IT infrastructure enables agencies to take advantage of artificial intelligence and machine learning tools to automate everyday tasks so government workers can focus on the cases that require human engagement. In some instances, a review of legacy systems may also indicate that the underlying programs they support could be replaced with a shared service that performs the tasks more cost-effectively than an IT modernization would.

When considering business processes, agencies must understand the individual functions performed by different systems and applications, including identifying areas of overlap. For example, while different groups within an agency may prefer to have their own applications for maintaining official records, the agency as a whole would benefit from collapsing all of these legacy systems into one streamlined, enterprise solution—ideally with or based on a COTS product.

Effective IT modernization plans prioritize the use of commercial or commercially available off-the-shelf (COTS) technologies to the greatest extent possible. Commercial technologies allow the government to leverage industry's most innovative solutions, including technical and security updates in or close to real time. In contrast, many legacy government systems are based on proprietary, customized technology.

Maintaining and upgrading these systems requires significant development work, often through costly services contracts. The latest security upgrades and patches may not be compatible with overly customized government systems, leaving these systems more vulnerable to cyber attacks. Whenever possible, agency IT modernization plans should include documented, actionable processes to retire customized legacy systems in favor of COTS solutions.

Effective and successful IT modernization plans require a robust and sustained leadership commitment. Agencies will never achieve desired technical outcomes if their modernization plans or funding levels continuously change with leadership turnover. Agencies must also build financial and contracting flexibility into their modernization plans. Contracts should be able to accommodate new and innovative technologies that may enhance modernization objectives. Financial requirements and models may also need to evolve as agencies abandon long-term contracts in favor of more agile, consumption-based spending.

To accomplish these goals, agencies should develop cross functional teams including IT system owners, contracting officers, and financial professionals dedicated to the business of modernizing IT. Additionally, agencies should engage human resource professionals to provide change management support and training to personnel impacted by system or process changes. This should include early and frequent outreach to system users to identify requirements and ensure modernization outcomes prioritize the end user experience. Finally, modernization plans should consider project goals from the perspective of oversight officials, including the ability to support oversight for agile projects.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

3. What specific advantages associated with cloud technologies did you see during your time at the FBI, in terms of both cost savings and mission fulfillment?

One of the greatest benefits of cloud technologies is scalability. By storing and processing data in the cloud, the FBI drastically improved its ability to synthesize large volumes of investigative data. Should another tragedy like the 2013 Boston Marathon bombing or 2017 Las Vegas shooting occur, cloud computing and tools such as artificial intelligence and machine learning will enable the FBI to digitally process petabytes of data in a matter of hours, versus mobilizing hundreds of agents to manually analyze data over several weeks. By replacing manual processes with cutting-edge cloud solutions, FBI agents and analysts will be more available to focus on preventing the next threat.

Additionally, moving operations to the cloud has helped the FBI become more agile. Historically, developing and deploying a new IT system could take years. By the time the system came online, much of the technology used was already outdated. In contrast, the FBI's counterterrorism division was able to design, build and deploy a new cloud-based system in a few months to review refugee cases for potential security risks. This would not have been possible on such a timeline without the cloud.

The FBI also used the cloud to improve its own continuity of operations. By storing data in the cloud versus one data center, the FBI was able to maintain connectivity without interruption even during system outages in one region.

Finally, using cloud-based email and file-sharing technologies, the FBI has successfully transitioned from an onsite to a distributed workforce during the COVID-19 pandemic. FBI agents, analysts, and professional staff now rely on cloud-based collaboration tools to continue their work remotely.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

4. Do agencies risk losing talented IT employees when they rely on legacy systems that impede effective service delivery?

Yes, agencies that rely on legacy systems that impede effective service delivery risk losing talented IT employees. In general, talented IT professionals who join government service are attracted by the opportunity to work on hard problems and challenges that may not exist in the private sector. This includes the ability to respond to unique problems using cutting-edge technologies in new and innovative ways. In most cases, recent computer science graduates, who are a primary target for professional recruiting by both public and private sector organizations, will not be interested in jobs supporting legacy systems that use arcane and outdated technologies. The skills needed for legacy system support are generally non-transferrable, not viewed as career enhancing, and not considered at the cutting edge. At the FBI, for example, talented IT professionals were generally most interested in working on investigative challenges involving complex data processing through innovative technologies. The government must modernize to effectively compete with the private sector for limited IT personnel resources.

Additionally, today's legacy computing approaches place an incredible administrative burden on the government workforce, often requiring excessive manual labor to enter and validate data, assemble data across disconnected systems, and review reams of paper forms. Outdated manual processes not only tax federal workers but increase both the likelihood of errors and the potential for waste, fraud, and abuse.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

5. How should Congress structure funding to best help government at the federal, state, and local levels modernize their IT to enable them to provide federal assistance most securely?

As amplified by the COVID-19 crisis, many IT systems at all levels of government are overburdened and under-resourced to meet increasing demands for digital services such as unemployment insurance or small business loans. Even before the COVID-19 pandemic, Government Accountability Office (GAO) audits identified multiple government IT systems in need of modernization. For example, several systems use outdated programming languages such as COBOL, run on hardware and software so old that it is no longer supported by the manufacturer, and are operating with known security vulnerabilities.[1]

Additionally, funding has not been prioritized to integrate federal agency systems with corresponding state and local systems that work together to deliver critical services to end users. Future funding streams should be dedicated toward eliminating siloed systems and promoting the use of common enterprise platforms and integrated solutions to deliver states' services, as well as federal services that are managed by states.

[1] https://www.gao.gov/products/GAO-19-471.

While the recent Coronavirus Aid, Relief, and Economic Security (CARES) Act provided significant funding for state and local governments, little funding was directed specifically toward IT modernization. As a result, states appropriately prioritized their immediate COVID-19 responses, which limited the funds available for upgrading legacy IT systems.

Congress should ensure future aid to state and local governments specifically directs funding toward modernizing legacy IT systems, including promoting cybersecurity. This includes increasing funding to states to meet greater demands for digital services. Additionally, Congress should increase funding for federal agencies to provide grants to state and local agencies that administer federal benefits at the state and local levels. Federal funds should be directly tied to improving the integration between federal systems and corresponding state and local systems. While block grants can be used, more prescriptive grants would likely accelerate modernization faster.

To the greatest extent possible, grants should incentivize the use of commercial capabilities, including commercial cloud computing and other innovative technologies. Grants should be made available to states and state agencies that adhere to modern solution and security methodologies, including establishing programs with secure, automated and continuous delivery and operation of software (DevSecOps), focusing on user experience (UX) design, and prioritizing the use of open and standards based architectures . Finally, federal agencies should be required to work closely with state and local governments to prioritize cybersecurity measures such as encryption for sensitive data shared between government systems.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

6. The National Cyber Director Act would create a cyber czar position in the White House. How should Congress design and structure the cyber czar's role so that he or she can effectively collaborate with the federal CIO as well as individual agency CIOs on cybersecurity issues and not have his or her responsibilities become siloed from the rest of the federal technology community?

The creation of a national Cyber Czar position would represent a commitment to prioritizing cybersecurity as a critical requirement for government IT systems. The technology sector looks forward to working with leaders who hold this position in the future to ensure our government's critical infrastructure is better protected from cyber attacks.

As the Cyber Czar role is defined, we recommend prioritizing integration with the government's existing cybersecurity framework to avoid unnecessary duplication of efforts and/or conflicting requirements. This includes clearly delineating roles and working relationships between the Cyber Czar, the Federal CIO, the Federal Chief Information Security Officer (CISO), and the Director of the Cybersecurity and Infrastructure Security Agency (CISA), among others. Cybersecurity must be seamlessly integrated with the government's overall IT modernization strategy and policy.

Question from Chairman Gerry Connolly for Gordon Bitko of ITI:

7. You testified that security practices and federal laws surrounding them need to be modernized, specifically citing the Federal Information Security Modernization Act (FISMA). What specific aspects of FISMA do you find are in need of updating, and what are your recommendations for doing so?

The Information Technology Industry Council (ITI) is currently working with our member companies to develop a more thorough set of recommendations for reforming the Federal Information Security Modernization Act (FISMA), including necessary complementary reforms for the Federal Information Technology Acquisition Reform Act (FITARA) and the Federal Risk and Authorization Management Program (FedRAMP). We are focused on several core areas of improvement: 1) continuing to shift FISMA implementation from paperwork and compliance-based to automated and real-time; 2) increasing consistency, thereby lowering the barriers for sharing and reuse between agencies; and 3) streamlining requirements where FISMA intersects with other policies. We look forward to collaborating with Congress to discuss more detailed recommendations as they are finalized, but provide initial recommendations here.

As a starting point, FISMA is built on the foundation of NIST 800-53 and should evolve with the planned new release of NIST 800-53 rev. 5, a significant update that provides clearer guidance on secure design and cyber resiliency and adds new controls centered on privacy and supply chain risks. FISMA requires system security plans (SSPs) for each IT system, showing how the NIST 800-53 requirements are met. SSPs must be approved by the agency CIO or Authorizing Official (AO). Although the principles of FISMA are sound, its implementation varies widely across the government, resulting in duplicative and often conflicting requirements imposed on federal IT contractors.

The definition of FISMA-reportable systems is somewhat ambiguous and has been interpreted differently across the government. This results in an inconsistent application of FISMA security requirements and controls, which weakens agencies' security posture. FISMA should be reformed to include a more precise definition of reportable systems.

One of the most significant challenges with FISMA, however, is the lack of reciprocity and information-sharing across the federal government. For example, contractors providing the same product or service to multiple agencies must currently support multiple SSPs and receive multiple Authorizations to Operate (ATOs). ATO requirements may differ based on the preference or experience of each agency's AO, which leads to confusion for contractors.

Additionally, there is no formal mechanism for agencies to share SSPs and risk determinations with each other, leading to duplicative efforts and a significant resource drain. Information System Security Officers (ISSOs), one of the key federal government positions required for ensuring agency cybersecurity, spend their time drafting new SSPs from scratch rather than building on the prior work done by other agency colleagues. For systems containing Personally Identifiable Information (PII), ISSOs participate in separate Privacy Impact Assessments (PIAs) based on requirements in the Privacy Act and the E-Government Act. Many privacy controls are already documented in the SSP, resulting in unnecessary and duplicative paperwork.

This situation could be improved by streamlining SSP and PIA requirements, including standardizing SSPs across the government. SSPs currently vary in quality, which contributes to a reluctance by agency AOs and/or CIOs to accept security evaluations done by other agencies. Standard quality assurance requirements and audits will help address this issue. As agencies shift to category management procurement frameworks such as Government-wide Acquisition Contracts (GWACS) and Best-in-Class (BIC) contract vehicles, agencies should consider greater vetting and security reviews at the master

contract level, which can be shared with agencies at the task order level. This limits the universe of security controls that must be considered by individual ordering agencies.

Additionally, FISMA should be reformed to mandate the sharing of SSP information and security controls within the federal government, which will require agencies to shift from manual documentation of controls to automated, machine-readable formats. Today, security controls and control baselines are often represented in proprietary formats, requiring data conversion and manual effort to describe their implementation. FISMA should be reformed to require a standardized, data-centric framework that can be applied to information systems government-wide to document and assess security controls. By moving security controls and control baselines from a text-based and manual approach (using word processors or spreadsheets) to a set of standardized and machine-readable formats, security professionals will be able to automate security assessment, auditing, and continuous monitoring processes. This will free up scarce personnel resources to better monitor, detect, and prevent cyber attacks against government systems.

Finally, the FISMA audit process should be reformed. Currently, agency Inspectors General (IGs) perform annual audits of a small sample of systems. This does not accurately reflect the full cybersecurity profile of an agency. True compliance must be assessed through continuous monitoring and evaluation of agency IT systems on a large scale.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

1. What are the top IT modernization priorities that Congress should act on?

In the wake of the COVID-19 pandemic, the importance of a well-funded, modernized, and secure IT infrastructure to support government operations cannot be overstated. As federal, state, and local agencies are still trying to reconstitute operations remotely while managing an unprecedented need for government services, Congress should immediately prioritize emergency funding and support for all levels of government in areas that include:

- IT infrastructure to enable, secure, and ensure continuity of remote work and operations;
- Technology and business process modernization so that we can transform and modernize labor intensive processes while increasing operational resiliency and scalability;
- Adoption of secure cloud computing tools;
- Increased delivery of digital services to citizens; and
- Policies and processes necessary for seamless work from home and distributed operations.

At the same time, Congress and the federal government should ensure commensurate investments in cybersecurity that expand and improve secure remote connectivity and access, leverage secure cloud capabilities, accelerate modernization of critical cybersecurity protocols, and improve training and readiness of IT executives and professionals who serve within and work alongside government.

Going forward, Congress must ensure adequate resources for agencies to provide critical citizen services in compliance with the 21st Century Integrated Digital Experience Act (IDEA). This Act requires all government-produced digital products, including websites and applications, to be consistent, modern, and mobile-friendly. Its implementation is an important step in ensuring modern delivery of services to citizens, which will become even more important as the United States moves into the post-pandemic era when mobile devices will play an even more integral role in accessing governmental services. The IDEA law has a set of criteria for new and redesigned websites and digital services including: accessibility for individuals with disabilities (as required by section 508 of the Rehabilitation Act of 1973), consistency in appearance, provision of services through industry standard secure connections, the presence of a search function, and full functionality on mobile devices. Congress should include sufficient funding for effective implementation of the Act, including funding for oversight mechanisms to assess the percentage of existing public facing websites that comply with the requirements of the law.

Congress should also ensure the funding flexibilities of the Modernizing Government Technology (MGT) Act are implemented in a meaningful way across the government. The MGT Act authorizes agencies to establish working capital funds (WCFs) to support the modernization of and reinvestment in government IT. While the WCF is a useful tool to enable agencies to conduct longer term and more strategic planning around IT investments, agencies have largely struggled to implement WCFs or have insufficiently funded WCFs based on a percentage of overall IT spending.

The MGT Act also created the centralized Technology Modernization Fund (TMF), 'housed' at the General Services Administration (GSA) and overseen by a board that is led by the Federal CIO and Administrator of GSA, to fund large government IT modernization projects. However, the TMF is insufficiently funded to meaningfully contribute to large-scale IT modernization projects. Additionally, agencies are reluctant to accept TMF disbursements because they are structured as loans; not grants. Congress should reconsider

the TMF's structure and possible agency barriers to establishing WCFs as part of a larger assessment of the MGT Act's success in modernizing government IT.

Finally, Congress should provide additional funding toward federal, state, and local data modernization and automation efforts. Government agencies struggle to process, store, and secure the ever-increasing volumes of data they ingest. Some of the greatest technical challenges facing agencies are actually data challenges. Agencies must modernize and leverage data as an asset.

At the federal level, Congress should ensure Chief Data Officers (CDOs) receive adequate funding to perform their work and execute effective data management strategies, including automating manual data processing functions. For example, the COVID-19 pandemic has highlighted the critical need for the Centers for Disease Control and Prevention's (CDC's) public health data modernization initiative.[2] Currently, COVID-19 case reporting is entered by hand by health officials using a paper form, which is then scanned and submitted to the CDC. This creates delays in processing data, making it more difficult for the CDC to analyze aggregated public health data to identify COVID-19 trends and hot spots. While the CARES Act provided $500 million for CDC data modernization, Congress should continue to fund data modernization and pursue oversight mechanisms to improve how all federal agencies use data to turn insights into action. Congress should also consider policies and legislation promoting secure data interoperability across government IT systems. This will better-equip government agencies to make informed, data-driven decisions.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

2. How can the federal government better articulate its technology needs to industry?

The federal government generally struggles with defining contract requirements that accomplish program objectives while still allowing for innovation and contractor expertise. While competition concerns may limit open dialogue opportunities with industry experts, many agencies simply do not take advantage of available market research opportunities and techniques.

Some of the most successful acquisitions provide multiple rounds of early engagement between the government and industry regarding commercial best practices, long before final proposals are due. For example, the government should consider incorporating best practices which can help understand industry capabilities and better define true mission needs, such as industry days, one-on-one meetings with vendors, and Requests for Information (RFI) as standard activities for major procurements. Additionally, agencies should consider sharing draft documents for industry review and comment before issuing a final solicitation. Preliminary industry feedback on system requirements documents, statements of work/objectives, draft solicitations/evaluation criteria, etc. can prove invaluable for ensuring the government and industry are in lockstep regarding commercial best practices.

To the maximum extent practicable, agencies should define requirements based on Statements of Objectives (SOOs) rather than prescriptive solicitations. This practice allows agencies to fully leverage contractor expertise without inhibiting innovation. Additionally, agencies should take advantage of existing flexibilities in the Federal Acquisition Regulation (FAR) including iterative, flexible instruments

[2] https://www.cdc.gov/surveillance/surveillance-data-strategies/data-IT-transformation.html.

such as Broad Agency Announcements (BAAs). BAAs provide greater opportunities for agencies to understand industry's innovative capabilities without investing upfront in long-term, expensive contractual arrangements.

When available, agencies should consider using Other Transaction Authorities (OTAs) and other non-FAR instruments to support the acquisition of cutting-edge, developmental technologies. The government should also utilize programs like Challenge.gov, which allows agencies to sponsor prize competitions for top ideas and concepts as well as breakthrough software, scientific, and technology solutions to help achieve their agency missions. These types of arrangements may be appealing to non-traditional government contractors.

Congress should also consider expanding Commercial Solutions Opening (CSO) Procedures authority to multiple agencies. CSO is a relatively new, non-FAR based acquisition mechanism that provides a streamlined acquisition process and simplified contract terms, all designed to open up the field of competition so that the government and taxpayers benefit from a large pool of solutions, with lower costs and better performance. The General Services Administration (GSA), Department of Homeland Security (DHS), and Department of Defense (DoD) have successfully used CSO Procedures to acquire innovative commercial solutions, including solutions supporting the United States' COVID-19 response.

Finally, as part of acquisition planning, agencies should consider the total cost of ownership for legacy, proprietary systems versus modernized, commercial systems. This includes considering downstream operations and maintenance (O&M) costs associated with supporting legacy applications, often through expensive service contracts. While the upfront costs of transitioning to a new manufacturer's hardware and O&M may appear to exceed the cost of maintaining the status quo, this may not be the case long-term. In most instances, adopting modern solutions based on open standards promotes competition by avoiding long-term vendor "lock in," which results in total cost savings for the government. Government contract solicitations and price evaluations that do not consider the total cost of ownership do not accurately account for potential cost savings through IT modernization.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

3. What changes would you make to the structure and process for awarding projects funds from the TMF?

While the Technology Modernization Fund (TMF) provides an important funding stream for IT modernization projects, the current total amounts involved remain too small to effect large-scale IT modernization in federal agencies. Additionally, the required pay back provision discourages many agencies from accepting funds. The TMF should be reformed to provide grants instead of repayable loans. Additionally, in doing so, Congress should consider relaxing pay-back provisions tied to previous TMF disbursements.

To improve the federal government's ability to provide secure digital services to citizens, TMF grants should be conditioned on agencies' use of commercial capabilities, including innovative technologies such as commercial cloud computing infrastructure. Additionally, TMF grants should be made to federal programs implementing modern solution and security methodologies, including DevSecOps, UX design, open architecture, and global security standards. Finally, TMF grants should prioritize improving the

integration between federal systems and corresponding state and local systems, with an emphasis on commercial solutions and cybersecurity.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

4. How can this Committee help improve the delivery of Federal assistance, grant, and mission related programs at the State agency level? What policies does Congress need to examine in order to assure that the downstream delivery and citizen engagement at the State and local level is an effective and positive experience?

The COVID-19 shortfalls regarding digital services delivery have made it abundantly clear that government IT systems will only meet program objectives if they keep the citizen at the center. The 21st Century Integrated Digital Experience Act (IDEA) represents an important effort at the federal level to ensure Executive agency websites provide an accessible, streamlined user experience; however, the Act currently does not apply to state and local government websites.

The delivery of federal assistance, grant, and mission related programs at the state agency level should include requirements for prioritizing end user experience and accessibility. When federal agencies act as a pass-through for administering benefits at the state and local levels, federal funds should be directly tied to developing digital services and products based on requirements and standards in the Act. All state and local websites and applications should be consistent, modern, mobile-friendly, and compliant with the latest commercial best practices and global security standards.

Additional federal funding should be allocated toward integrating federal agency systems and corresponding state and local systems that work together to deliver critical services to end users. Future funding streams should also be tied to the use of commercial products, including open, standards-based technologies and integrated solutions to deliver digital services.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

5. The FITARA scorecard currently captures the MGT Act requirement for an agency that has set up a working capital fund to transition away from legacy IT systems. However, the federal government continues to spend a majority of its IT budget on operating and managing of these older systems. What other metrics could the committee track to ensure we incentivize this transition away from legacy IT?

While the working capital fund (WCF) is a good tool to enable agencies to conduct longer term and more strategic planning around IT investments, the FITARA measure of WCFs could be improved by factoring in the percentage of total agency spend included in the WCF, or agency sub-components involved. For example, the Department of Justice (DOJ) has a WCF and the FBI contributes to it. However, the FBI's contribution only represents a small fraction of the FBI's overall IT spending. As a result, the WCF does not provide necessary funding stability to enable long-term IT investment planning. Alternatively, an improved measure could compare the size of an organization to the recommended amount for its IT budget. WCF contributions should be a meaningful percentage relative to the size of the agency at large.

An additional FITARA metric could assess the extent to which agencies adopt incremental development approaches, versus wholesale changeovers. Incremental development plays an essential role in improving

and expanding IT systems and has been increasingly embraced by the private sector as it drives rapid IT innovation. While the frequency of delivering new functionality varies by system, some high speed DevSecOps models deploy new capabilities daily, if not more frequently. The U.S. Government should aim to increase the frequency of incremental deliveries, pushing code to production monthly or at least every six weeks. This is a significant improvement beyond the current government standard of delivering code every six months, which is not agile development. Further, the FITARA scorecard could be augmented to require reporting the number of contracts awarded requiring agile development methodology, as well as the extent to which agencies are migrating from formal change control boards toward DevSecOps.

The FITARA scorecard should also be modified to measure the authority of Agency CIOs and AOs to leverage the Federal Risk and Authorization Management Program (FedRAMP), the government's standardized approach for adopting secure cloud services. Despite agencies' increasing migration from legacy systems to cloud-based applications, not all agencies are relying on FedRAMP accreditations as part of their own system security assessments. The result is that individual agencies spend more time accrediting new technologies. The FITARA scorecard should track the number of FedRAMP authorizations sponsored by CIOs and AOs, to highlight the value of delivering shared services. Additionally, this metric should evaluate the number of existing authorized FedRAMP products and services used, and/or the number of agency Authorizations to Operate (ATOs) leveraging FedRAMP products and services to inherit security controls, thereby reducing agency-specific control requirements and time to accreditation. This will incentivize CIOs and AOs to evaluate and accept risk based on the work of other agencies, which accelerates the adoption of innovative technologies.

Finally, FITARA's metrics for tracking transparency and risk management should be improved to incentivize migrating from end of life technology to secure, modern systems. Current scorecard methodology suggests that a higher percentage of reported risk is more transparent and is therefore appropriate. However, this practice does nothing to account for existing risk mitigation efforts, nor does it do a good job of encouraging better risk management and mitigation which should be the goal. Instead, it creates an incentive for agencies to label projects as high risk, for the sole purpose of achieving a higher score on this FITARA metric. The FITARA measure can be improved by accounting for mitigation options put in place, starting with the highest risk mission critical projects. Additionally, the FITARA scorecard could incentivize IT modernization by accounting for retirement and disposal rates for high-risk systems that are not mission critical or use obsolete/end of life technology. Finally, this metric could be improved by including a compound measure accounting for both risks recognized and subsequently adopted mitigation strategies in response to those risks.

Question from Ranking Member Jody Hice for Gordon Bitko of ITI:

6. The FITARA scorecard currently has a FISMA component to assess if agencies have met their cybersecurity goals. How can this metric be improved upon?

The current FITARA scorecard methodology for assessing agency performance on cybersecurity goals relies on Agency Inspectors General FISMA assessments against the NIST Cyber Security Framework (CSF). In general, this is a sound approach, but the FITARA measurement is somewhat limited due to the small sample of systems that Agency IGs typically audit to inform the assessment against the CSF. The current cybersecurity methodology can be improved by adopting the following recommendations:

- NIST 800-53 rev 5 supply chain and privacy should be incorporated into future FISMA scores in line with the overall planned schedule for 800-53 rev 5;
- IG staffs should audit a larger sample of agency systems; and
- IG audit staffs should be cross trained from different agencies to ensure consistency of assessments across the federal government.

The FITARA scorecard should be updated to include metrics assessing whether agencies have implemented continuous monitoring programs for IT systems. Additionally, metrics should be added to evaluate actual incident response (e.g. by having an independent monitor for exercises like Cyber Storm/Ice Storm, or through real penetration testing of agency networks, if such a program can be established). Finally, an evaluation of agency Supply Chain Risk Management (SCRM) should be included within this dimension. An initial measure would be to track if agencies have established SCRM plans as described in NIST 800-161.