Michael Kans' Technology Policy Update
3 July 2019
By Michael Kans, Esq.

Federal Information Technology Acquisition Reform Act (FITARA) Oversight Hearing

Last week, the House Oversight and Reform Committee continued its ongoing, bipartisan oversight of how federal departments and agencies are securing their networks, upgrading old information technology (IT) and systems, closing and consolidating data centers, managing cyber and IT risk, and improving their acquisition and development of new IT. And yet, in their eighth Federal Information Technology Acquisition Reform Act (FITARA) scorecard, the Committee incorporated a new category by which agencies would be evaluated: compliance with the Federal Information Security Modernization Act (FISMA).

The committee heard from three agency chief information officers (CIO) after testimony from Federal CIO Suzette Kent and Government Accountability Office IT Management Issues Director Carol Harris:

- U.S. Department of Agriculture Chief Information Officer Gary Washington
- U.S. Department of Education Chief Information Officer Jason Gray
- U.S. Department of the Treasury Chief Information Officer Eric Olson

Government Operations Subcommittee Chair Gerry Connolly (D-VA), in his prepared statement, noted that when Congress enacted FITARA, it was understood that "sustained oversight" would be necessary so that agencies would understand that full implementation of the statute would lead to "cost-savings and better IT acquisition practices." He claimed that numerous hearings and briefings have resulted in agencies recognizing that "implementing FITARA is the foundation for IT acquisition and management practices that will pay dividends as agencies seek to retire costly legacy IT systems, upgrade their IT systems, and migrate to the cloud." Connolly asserted that the eighth FITARA scorecard "reflects improvements agencies have made in implementing the law" which is most notably reflected in the fact that "[f]or the second scorecard in a row, there are no agencies receiving a failing grade." He added that two agencies would have received A+ grades if they had changed the reporting structure for the CIO to report directly to the agency head of deputy head. Connolly noted the addition of FISMA compliance to the scorecard also decreased a number of agency grades but claimed that a continued focus on FISMA implementation would ultimately improve the cybersecurity posture of agencies. He said that one category of metrics is "greyed out" because draft guidance by the Office of Management and Budget (OMB) on the Data Center Optimization Initiative (DCOI) "made it difficult to evaluate progress on data center consolidation and optimization," and OMB failed to adhere to FITARA by not "establishing performance metrics and requiring public disclosure of those metrics." Connolly noted the a number of agencies are reporting to the committee that they lack the statutory authorization to transfer money in working capital funds to update legacy IT as directed by the "Modernizing Government Technology (MGT) Act." He expressed his intention and willingness to work with colleagues to address this problem.

Ranking Member Mark Meadows (R-NC) said he would be brief considering how late the hearing was in starting. He said the committee is focused on the issue of "direct reports" for CIOs, and he asserted the National Aeronautics and Space Administration (NASA) will soon be addressing this issue. Meadows said "bottom line---we paying very attention to it, and we're working in a bipartisan fashion." He said "we want everyone to understand that the scorecards are meaningful to us and eventually they're going to be meaningful to the agencies because we're working to attach dollars both as penalties and rewards." Meadows expressed his belief that if "you're getting good responses, you ought to be rewarded." He added that he visited the Office of Personnel Management and "the way we're doing federal benefits is archaic," which "has got to change." He said that as a fiscal conservative, he is willing to "spend money to get it done." Meadows declared that FITARA and FISMA compliance are critical pieces of the federal IT puzzle.

Federal CIO Suzette Kent contended that "[a]s worldwide technology capability rapidly evolves, so must Government technology, security, and IT policy." She stated that "[w]hen I took on this role, I committed to agencies that the OMB Office of the Federal Chief Information Officer (OFCIO) team will continuously update policies and metrics to remove barriers and better align agency IT resources with strategic goals." Kent claimed that "[o]ur policies must be as nimble and iterative as the emerging technology products and the evolving nature the quality service expectations of citizens." She added that "[t]his intent drove our policy updates in 2018 and 2019…[and] [s]ome of those policies were updated for the first time in over eight years." Kent added that "[w]e have also sought to update how we measure success…[and] [t]he CIO Council provided recommendation to Government Accountability Office (GAO) and to House Oversight for enhancements of the scorecard." Kent claimed that "we are focused on making metrics and measures data-driven, continuous and publicly available through websites…[and] [t]hese achievements and interactions show the Administration is committed to working with Congress and the GAO to drive stronger accountability and better outcomes government wide."

Kent added

> The Cloud Strategy and the Data Center Optimization Initiative are a few of OMB strategies and policies that are enabling agencies to modernize the Federal IT landscape. We have recently released the, guidance on High Value Assets (HVAs), Identity, Credential, and Access Management (ICAM), and the first ever Federal Data Strategy with a one year action plan. We are also working on policy to define the guideposts and controls for advancing use of automated technologies. In May, three Agencies CIOs, policy leaders from OFCIO and I met with Congressional staff team members from OGR, HSGAC and House Homeland committees and provided perspectives and details on policy updates, both finals and those in draft.

GAO IT Management Issues Director Carol Harris said the OMB and federal agencies have taken steps to improve the management of IT acquisitions and operations and ensure federal cybersecurity through a series of initiatives." She said that "[a]s of June 2019, federal agencies had fully implemented 60 percent of the 1,277 IT management-related recommendations that GAO has made to them since fiscal year 2010." Harris stated that "[l]ikewise, agencies had implemented 78 percent of the 3,058 security-related recommendations that GAO has made since 2010." She added that "[e]ven with this progress, significant actions remain to be completed" and highlighted the following categories of GAO recommendations:

- **Chief Information Officer (CIO) responsibilities.** Laws such as the Federal Information Technology Acquisition Reform Act (FITARA) and related guidance assigned 35 key IT management responsibilities to CIOs to help address longstanding challenges. In August 2018, GAO reported that none of the 24 selected agencies had established policies that fully addressed the role of their CIO, as called for by laws and guidance. GAO recommended that OMB and each of the 24 agencies take actions to improve the effectiveness of CIOs' implementation of their responsibilities. As of June 2019, none of the 27 recommendations had been implemented.

- **CIO IT acquisition review.** According to FITARA, covered agencies' CIOs are required to review and approve IT contracts. Nevertheless, in January 2018, GAO reported that most of the CIOs at 22 covered agencies were not adequately involved in reviewing billions of dollars of IT acquisitions. Consequently, GAO made 39 recommendations to improve CIO oversight for these acquisitions. As of June 2019, 23 of the recommendations had not been implemented.
- **Consolidating data centers.** OMB launched an initiative in 2010 to reduce data centers. According to 24 agencies, data center consolidation and optimization efforts had resulted in approximately $4.7 billion in cost savings through August 2018. Even so, additional work remains. GAO has made 196 recommendations to OMB and agencies to improve the reporting of related cost savings and to achieve optimization targets. As of June 2019, 79 of the recommendations had not been implemented.
- **Managing software licenses.** Effective management of software licenses can help avoid purchasing too many licenses that result in unused software. In May 2014, GAO reported that better management of licenses was needed to achieve savings, and made 136 recommendations to improve such management. As of June 2019, 27 of the recommendations had not been implemented.
- **Ensuring the nation's cybersecurity.** While the government has acted to protect federal information systems, GAO has consistently identified shortcomings in the federal government's approach to cybersecurity. The 3,058 recommendations that GAO made to agencies since 2010 have been aimed at addressing cybersecurity challenges. These recommendations have identified actions for agencies to take to fully implement aspects of their information security programs and strengthen technical security controls over their computer networks and systems. As of June 2019, 674 of the recommendations had not been implemented.

How State and Local Governments Cybersecurity Might Be Helped By The Federal Government

The House Homeland Security Committee's Cybersecurity, Infrastructure Protection, & Innovation Subcommittee held a hearing to examine the recent spate of ransomware and cyber attacks on states, cities, and towns. In May, Baltimore, Maryland paid about $100,000 in bitcoin to hackers that caused the city an estimated $18 million in damages, and in June two Florida cities, Riviera Beach and Lake City, paid out a reported $1 million in ransom to hackers. In May, a cybersecurity firm "was able to catalog 169 ransomware incidents affecting state and local governments since 2013" with the caveat that "[r]ansomware attacks are not always publicly reported by state and local governments and there is no centralized reporting authority…[consequently] the number of incidents is most likely underreported."

The committee heard from these witnesses:

- Atlanta Mayor Keisha Lance Bottoms
- Center for Internet Security Senior Vice President of Operations and Chair of Multi-State ISAC Thomas Duffy
- The Center for Long Term Cybersecurity Affiliated Researcher Ahmad Sultan
- The McCrary Institute for Cyber and Critical Infrastructure Security Director Frank J. Cilluffo

Subcommittee Chair Cedric Richmond (D-LA) said "I want to spend some time looking at how cybersecurity impacts real people–like the ones I represent in the 2nd District of Louisiana." He said "[m]any of them are not thinking about phishing emails or ransomware or whether a hostile foreign government has gained access to the networks that control their drinking water, transportation, or medical care." Richmond stated that "while the Federal government has an important role to play in securing these networks, state and local governments own them." He stated that "[t]he staffing, structure, and resources available to state and local agencies vary across the country–but many of them are operating with a shoestring budget…[a]nd, like Federal agencies, they are increasingly being targeted with sophisticated cyber attacks." Richmond said that "[u]ltimately, we cannot expect under-resourced, under-staffed state and local governments to defend their networks from state-sponsored hackers from Russia, China, and Iran." He explained that "[t]oward that end, I am working on a comprehensive package to improve the cybersecurity posture of our state and local governments…[and] I look forward to hearing from our witnesses today about opportunities to address this important national security issue."

Subcommittee Ranking Member John Katko (R-NY) said "[o]ur State and local governments are prime targets for cyberattacks…[a]nd in the first four months of 2019 alone, there have already been 21 attacks, including in my home state of New York." He claimed that "[i]n 2018, the National Association of State Chief Information Officers found that many states typically spend only one to two percent of their budget on cybersecurity…[and] [m]ost employ fewer than fifteen full-time cyber professionals." Katko said that "[t]his is not surprising, given the budgeting challenges many State and local governments face and the talent pipeline issues we have discussed in previous hearings." He declared that "[i]t will take work from Federal, State and local governments, as well as outside stakeholders, to improve this situation, but it is clear that action is needed." Katko proposed the following policy response:

- I will introduce a bill, the State and Local Cybersecurity Improvement Act, which directs the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security, to develop a resource guide for State and local officials to navigate the challenges of protecting their networks.
- My bill also will create two new grant programs. The first is a one-time grant for State and local governments to identify their High Value Assets and system critical architecture. To protect something, you must know what is worth protecting.
- The second grant program helps State and local governments conduct exercises to train, prepare and evaluate their ability to respond to an attack. Working through an exercise allows a government to identify weaknesses in their current plan and establishes protocols and procedures to be prepared in case the worst happens.

Sultan stated that "the interconnected nature of online networks means that poor cybersecurity outcomes for underserved populations can affect countless others." He said that "[i]t not only deepens inequalities for those already most vulnerable to existing economic and social forces, but reduces trust in online services for all." Sultan stated that "[w]ith 5G networks and Artificial Intelligence systems promising smarter cities where key government services are powered by strong mobile connections and trained machine learning algorithms, the risk of ignoring poor cybersecurity outcomes are at an all-time high." He said that "[i]t is imperative that we work diligently towards raising awareness and educating underserved populations about cybersecurity." He said that "[s]olutions exist but they require close coordination between Federal, state, and local governments…[and] some ways that the Federal government can assist state and local governments include:

- Direct funds towards local cybersecurity awareness trainings: Local governments can partner with nonprofits to roll out trainings aimed at improving the cybersecurity knowledge and outcomes for underserved residents. These trainings can be expensive as they require devices and equipment, qualified trainers, monetary or other incentives for participants, and fixed locations scattered throughout the city. Local government budget might not be able to justify prioritizing these expenses.

- Design baseline training programs: Not all state and local governments have the capacity or expertise to design a cybersecurity training program. The Federal government should work with local governments to design a baseline training program which details the core topics that all training programs should address. While the Federal government should design the baseline topics and curriculum, the programs should be informed by and tailored to the ground realities of each city and should not limit any government from going further than its selected baseline topics.
- Develop and rollout public awareness campaigns: Public awareness campaigns are more cost-effective and can scale better to reach larger audiences when developed centrally. This streamlines the process of disseminating content to schools, broadcast TV, online and physical publications, social media platforms, and radio.
- Coordinate public-private partnerships: The Federal government is uniquely positioned to work with private technology companies to create advice resources, cross-company collaborations in areas like phishing scams and coordinated disinformation campaigns, and technological solutions like cybersecurity chat bots and apps for smart-phones that no longer receive security updates. As I will explain later in this testimony, underserved populations tend to place a high level of trust on advice resources provided by private technology companies. It would be highly inefficient for every state and local government to individually approach technology companies for their own respective solutions.

Cilluffo asserted that "[t]here are examples and pockets of State and Local Government cybersecurity excellence to be sure; but there are also significant gaps and seams where the Federal Government can help and can do so without subverting the principle that the level of government that is closest to the people knows best how to serve them." He said that "[c]yber needs at the State and Local level are many: more money, more experts, more tools, more information/awareness and more collaboration (between government and industry, and among governments and regions) – to name just a few." Cilluffo laid out a few ideas on how the federal government might help state and local governments:

- A dedicated Federal grant program should have built-in safeguards to ensure that there is return on Federal investment in the form of measurable State/Local and by extension national capabilities. Simply throwing Federal money at the problem is not the answer. Instead, there must be a thoughtful strategy and accompanying metrics to support the request for funds and any subsequent grant. The program would therefore be risk-based and tailored to particular context. Among the purposes that such a program could and should support would be both State-level and regional exercises. Notably momentum for directed Federal funding is building as evidenced for example by the recommendations in the May 2019 Interim Report of the Homeland Security Advisory Council's State, Local, Tribal and Territorial Cybersecurity Subcommittee.
- The Federal Government could further assist by providing opportunities for State and Local officials to gain and hone cybersecurity skills, as well as how to identify and counter foreign influence. While education and training programs certainly do exist they are neither as numerous nor as evenly available across the country as would be ideal.
- Over the past twenty years, the country has learned many lessons about preparing for, responding to and bouncing back from major incidents such as terrorist attacks and natural disasters. These experiences have ultimately made us smarter, stronger and more resilient

as a nation, though we still have a ways to go. Among these lessons is the value of taking a regional approach to capacity-building and mutual assistance, which builds upon existing relationships and arrangements, and follows logically and naturally from proximity and geography, rather than duplicating efforts and according formal borders/boundaries undue influence.

- One of the most significant cybersecurity challenges to State Governments relates to the 2020 election and in particular preparing to administer the vote and ultimately doing so. Protecting the integrity of the process from beginning to end is of paramount importance as this exercise provides the bedrock for our democracy; trust and faith in the process is the glue that binds us together. The Federal Government can and should share more widely and actively its unique informational and other assets with State-level counterparts for the targeted purposes of identifying and mitigating threats in this context.

OMB Revises Data Center Consolidation Policy

In a new memorandum, the Office of Management and Budget (OMB) acting through the Chief Information Officer (CIO) has updated the Data Center Optimization Initiative (DCOI) and rescinded the Obama Administration's controlling authority on data center consolidation. OMB declared that "[a]s a result of work that has occurred over the past years there will be continuous improvements, but the Federal Government should not expect to see continued dramatic savings or large-scale closures from ongoing data center consolidation and optimization efforts as agency needs grow." Nonetheless, OMB will prioritize "the effort to consolidate and optimize data centers in the following hierarchy, to maximize the return on investment and based on the level of impact for the effort." Agencies are directed to "consider their mission goals first, and this prioritization second, in the following descending order of importance" "[w]hen considering the allocation of limited resources or conflicting priorities:

1) Consolidation and Closure
2) Optimization
   i) Virtualization
   ii) Availability
   iii) Energy Metering
   iv) Server Utilization Reporting"

The federal government has a statutory obligation to close, consolidate, and optimize data centers as enshrined in the "Federal Information Technology Acquisition Reform Act" (FITARA) and then extended until October 1, 2020 under the "FITARA Enhancement Act of 2017." In April 2019, the Government Accountability Office (GAO) found that the DCOI had achieved "mixed" progress at best as a number of agencies had failed to close the data centers as planned and had also failed to optimize the operations of data centers despite clear and transparent OMB metrics. However, the GAO found that six agencies had largely complied with the DCOI through "gathering leadership support, effective communication, and alignment with the core tenets of DCOI," providing a possible roadmap to drive other agencies to do the same.

OMB noted

> As agencies gain greater IT spending transparency through Capital Planning and Investment Control (CPIC) and Technology Business Management (TBM), the resulting data will support and enable their ability to rationalize their application portfolios to find greater return on investment, in alignment with the 2018 Federal Cloud Computing Strategy ("Cloud Smart").

> (***See below article***) Rather than focusing on infrastructure alone, agencies must consider what applications are running in their data centers to facilitate further consolidation and optimization. This will frequently require updating legacy applications to take advantage of modem technologies such as APIs, microservices, and cloud, as well as replacing bespoke systems with commercial offerings when cost-effective. Agencies should consider carefully the Total Cost of Ownership (TCO) when making such determinations, not just licensing and hosting costs.

Overall, in the memorandum, OMB asserted that the easy gains of consolidation have long been realized and the DCOI "will focus on targeted improvements in key areas where agencies can make meaningful improvements and achieve further cost savings through optimization and closures, as well as driving further maturity in IT modernization." OMB then outlined a number of DCOI policy changes to realize this new focus:

- OMB extended the current freeze on budgeting "any funds or resources toward initiating a new agency-owned data center or significantly expanding an existing agency-owned data center without approval from OMB." However, agencies may request this approval in writing and the freeze will not apply to "critical agency facilities as described under the "Key Mission Facilities for Data Management" section" of the memorandum.
- OMB recognized that how agencies were defining "tiered" data centers resulted in legitimate data centers being characterized as "server closets" because they did not have "a backup generator or other hardware but that operated as a data center in all other regards." Consequently, "agencies shall report purpose-built physically separate and dedicated spaces as tiered data centers when they appropriately meet key criteria." OMB further claimed that "agencies have seen little real savings from the consolidation of non-tiered facilities, small server closets, telecom closets, individual print and file servers, and single computers acting as servers." As a result, OMB "will no longer require agencies to consolidate these server closets, meet optimization targets, or include them in their inventory submissions." Yet, OMB did direct that "agencies should consolidate any business applications hosted in non-tiered data centers and closets when cost-effective and as appropriate for accomplishing the agency mission and enhancing system security or information privacy." OMB added that
- Private sector-provided cloud services are not data centers for the purposes of this Memorandum. Agencies are no longer required to report their cloud investments as part of their data center inventories, as this information is already collected through the Capital Planning and Investment Control (CPIC) process.
- OMB also advised agencies they "should consider opportunities for investments that may yield long-term savings through energy efficiency" possibly through "refreshing inefficient hardware may lead to long-term savings, especially where legacy systems past their end-of-life incur large costs for support."
- OMB explained "[a]gencies should continue to replace manual collections and reporting of operational data as well as systems, software, and hardware inventory housed within data centers with automated monitoring, inventory, and management tools...[and] [t]o the extent permissible under the Federal Acquisition Regulation (FAR), agencies must include standard automated infrastructure management requirements for all new data center service contracts or procurement vehicles."
- OMB stated that "[t]o obtain more accurate measure of data centers performance, 0MB will avoid using averages for metrics whenever possible and will instead identify metrics where agencies can demonstrate continuous improvement beyond the performance period of this memorandum...[and] will recommend guidelines for reasonable performance on these

> metrics, when appropriate, across the entire Federal enterprise, based on real, collected data baselines."

New Federal Cloud Policy Finalized

The Chief Information Officer (CIO) Suzette Kent and the Chief Information Officers Council (CIO Council) have released a revised "Federal Cloud Computing Strategy" (Cloud Smart) that replaces the Obama Administration's Cloud First Strategy that will be "executed over an eighteen-month period." The CIO noted that "[s]ince the release of the original draft of this strategy [in September 2018], the Office of Management and Budget (OMB) has worked with its partners – both Government agencies and in the private sector - to update policy guidance and create new resources for aiding cloud adoption." In terms of salient takeaways, the CIO and CIO Council are defining cloud in very broad terms and are purposely "provider-agnostic," meaning neither commercial entities nor federal agencies would be preferred in the provision of cloud services under this iteration of federal cloud policy. Moreover, the CIO and CIO Council are making the case that a culture shift is needed across the federal government with respect to modernization that entails regular review and reform of cloud practices.

The CIO Council "developed a list of action items to execute the Cloud Smart strategy...[that] constitute a work plan aimed at creating and updating programs, policies, and resources that the whole of Government will use to advance the Cloud Smart agenda." The CIO added that "all Federal agencies will rationalize their application portfolios to drive Federal cloud adoption...[and] [t]he rationalization process will involve reducing an application portfolio by

1) assessing the need for and usage of applications; and
2) discarding obsolete, redundant, or overly resource-intensive applications.

The CIO and CIO Council stated "[t]o support these rationalization efforts, the CIO Council will develop best practices and other resources…[and] while the initial Cloud Smart work plan will be executed over an eighteen-month period, its actions will be refreshed continuously as needed to keep up with the changing cloud market and emerging technologies."

The CIO claimed that "[d]ecreased application management responsibilities will free agencies to focus on improving service delivery by optimizing their remaining applications." To this end, the CIO Council recently released this Application Rationalization Playbook, "a practical guide for application rationalization and IT portfolio management under Cloud Smart...intended to help Portfolio Managers think through their agency's approach to IT modernization."

As noted, the CIO uses the "cloud" definition developed by NIST Special Publication (SP) 800-145 and refined in SP 500-322: "those solutions that exhibit five essential characteristics of cloud computing, as defined by NIST: on-demand service, broad network access, resource pooling, rapid elasticity, and measured service." The CIO stressed that "[t]hese characteristics and the solutions that exhibit them are provider-agnostic – meaning anyone can develop and deploy a cloud solution, whether an outside vendor or a Federal agency." The CIO added that "[c]loud adoption strategies that successfully meet the intent of Cloud Smart should not be developed around the question of who owns which resources or what anticipated cost savings exist." The CIO stated that "agencies should assess their requirements and seek the environments and solutions, cloud or otherwise, that best enable them to achieve their mission goals while being good stewards of taxpayer resources."

The CIO is calling on agencies to "cultivate an organizational mindset of constant improvement and learning" in order "[t]o realize the full benefit of cloud technology." The CIO explained that "modernization is a constant state of change and part of the day-to-day business of technology at every agency...[and] agencies will need to iteratively improve policies, technical guidance, and business requirements to match changing needs, drive positive outcomes, and prevent their IT portfolio from becoming obsolete."

The CIO and CIO Council discussed the following topics as part of the Cloud Smart strategy:

- Security
  - Trusted Internet Connections
  - Continuous Data Protection and Awareness
  - FedRAMP
- Procurement
  - Category Management
  - Service Level Agreements
  - Security Requirements for Contracts
- Workforce
  - Identifying Skill Gaps for Current and Future Work Roles
  - Reskilling and Retaining Current Federal Employees
  - Recruiting and Hiring to Address Skill Gaps
  - Employee Communication, Engagement, and Transition Strategies
  - Removing Bureaucratic Barriers to Hiring Talent Expeditiously

PSI Reports Highlights Federal Cybersecurity Failings

The Senate Homeland Security Committee's Permanent Subcommittee on Investigations (PSI) released a staff report on federal cybersecurity and found in the four years since the enactment of the "Federal Information Security Modernization Act of 2014" (FISMA), "federal agencies have failed to substantially improve their information security posture." PSI further asserted that "[t]he vast majority of the federal government has failed to implement basic and effective data security controls—leaving PII and other sensitive information vulnerable to exploitation." In making these determinations, PSI examined the annual Inspector General reports on FISMA for seven agencies "cited by OMB as having the lowest ratings with regard to cybersecurity practices based on NIST's cybersecurity framework in fiscal year 2017."

PSI reviewed the past ten years of audits for the Department of Homeland Security (DHS) and seven other agencies:

(1) the Department of State ("State");
(2) the Department of Transportation ("DOT");
(3) the Department of Housing and Urban Development ("HUD");
(4) the Department of Agriculture ("USDA");
(5) the Department of Health and Human Services ("HHS");
(6) the Department of Education ("Education"); and
(7) the Social Security Administration ("SSA").

PSI turned up these common problems from IG reports for the eight agencies in question:

- *Protection of PII*. Several agencies failed to properly protect the PII entrusted to their care. These agencies included State, DOT, HUD, Education, and SSA. The HUD IG has noted this issue in *nine* of the last eleven audits.

- *Comprehensive list of IT assets*. The IGs identified a persistent issue with agencies failing to maintain an accurate and comprehensive inventory of its IT assets. In the last decade, IGs identified this as a recurrent problem for State, DOT, HUD, HHS, and SSA.
- *Remediation of cyber vulnerabilities*. Over the past decade, IGs for all eight agencies reviewed by the Subcommittee found each agency failed to timely remediate cyber vulnerabilities and apply security patches. For example, the HUD and State IGs identified the failure to patch security vulnerabilities *seven* of the last ten annual audits. HHS and Education cybersecurity audits highlighted failures to apply security patches *eight* out of ten years. For the last *nine* years, USDA failed to timely apply patches. Both DHS and DOT failed to properly apply security patches for the last *ten* consecutive years.
- *Authority to operate*. The IGs identified multiple agencies that failed to ensure systems had valid authorities to operate. These included DHS, DOT, HUD, USDA, HHS, and Education. For example, HHS systems lacked valid authorities to operate for the last *nine* consecutive audits. Additionally, the DHS IG determined that DHS operated systems without valid authorities in *seven* of the last ten audits. As stated, DHS is the agency in charge of securing the networks of all other government agencies.
- *Overreliance on legacy systems*. The extensive use of legacy systems was also a common issue identified by IGs. All eight agencies examined by the Subcommittee relied on legacy systems. For example, the DHS IG noted the use of unsupported operating systems for at least the last four years, including Windows XP and Windows 2003.
- *Chief Information Officer*. In an effort to prioritize agency cybersecurity, Congress established the position of Chief Information Officer ("CIO") in 1996. Since then, Congress has increased the responsibilities of agency CIOs several times. The most recent attempts were included in FISMA and the Federal Information Technology Acquisition Reform Act, which gave CIOs plenary governance over an agency's IT budget and priorities. Despite these authorities, agencies still struggle with empowering the CIO. In August 2018, GAO found that none of the 24 major agencies—including the eight examined by the Subcommittee—properly addressed the role of CIO as Congress directed. These 24 agencies included the eight agencies reviewed by the Subcommittee in this report.

PSI made the following recommendations:

1. **OMB should require agencies to adopt its risk-based budgeting model addressing blind IT spending.** This process links agency IT spending to FISMA metrics to help agencies identify cybersecurity weaknesses that place the security of agency information at risk. Agencies currently use their limited IT funds on capabilities for perceived security weaknesses instead of using those funds on the security risks most likely to be exploited by hostile actors. OMB should report to Congress whether legislation is needed.
2. **Federal agencies should consolidate security processes and capabilities commonly referred to as Security Operations Centers ("SOCs").** This would provide agencies with better visibility across their networks. With this visibility, agencies could better detect cybersecurity incidents and exfiltration attempts.
3. **OMB should ensure that CIOs have the authority to make organization-wide decisions regarding cybersecurity.** This authority was provided to CIOs in 2014 with the enactment of FISMA, but the Subcommittee discovered that this is not being implemented as Congress intended. Without this authority, agencies have no senior officer to hold personnel accountable to security standards and implement policies that strengthen the agency's information security program. Congress should consider whether legislation is needed.
4. **OMB should ensure that CIOs are reporting to agency heads on the status of its information security program as mandated by FISMA.** Agency heads often exclusively

rely upon CIOs and Chief Information Security Officers ("CISO") for matters of information security. This complete delegation detracts from the leadership accountability necessary for agency-wide improvements. To ensure this line of communication, CIOs should submit quarterly reports to agency heads detailing agency performance against FISMA metrics and return on investment for existing cybersecurity capabilities.

5. **Federal agencies should prioritize cyber hiring to fill CIO vacancies and other IT positions critical to agency cybersecurity efforts.** To facilitate this prioritization, OMB should determine if additional flexibility is needed across the government for cyber hiring and suggest any legislation necessary to Congress.
6. **OMB should consider reestablishing CyberStat or regular in- person reviews with agency leadership to focus on cybersecurity issues and generate actionable recommendations to accelerate the fortification of government networks.** OMB should include a summary of the value added by these reviews in its annual FISMA report to Congress.
7. **In developing shared services for cybersecurity, DHS should consult agency CIOs to ensure that the proposed service will be widely utilized.** When DHS launches a shared service, it should consider piloting the service with a small number of agencies to confirm operability and functionality. As the Quality Service Management Office for cybersecurity, DHS should include a summary of the five-year services implementation plan required by OMB in its annual FISMA report to Congress.
8. **All federal agencies should include progress reports on cybersecurity audit remediation in their annual budget justification submission to Congress.** Agencies should also include a description of the OMB approved business case in the budget justification for modernized technology or services for which OMB designated a Quality Service Management Office to demonstrate that a separate procurement results in better value.
9. **Federal agencies should create open cybersecurity recommendation dashboards.** Once created, each agency should submit to Congress every six months metrics on audit recommendation closure rates and accomplishments. Each agency head should also be briefed and approve the agency's plan for addressing open cyber recommendations.

What PSI or the full Committee does on the basis of this report is not clear. It should be noted that most of the recommendations are steps the Administration and agencies could take under their existing authorities, which would be a less directive approach than legislating new requirements. Additionally, in March, PSI released a report on the failures of Equifax in leading to one of the largest breaches in U.S. history but no legislation has been introduced based on the recommendations made to address data security. Of course, both PSI Chair Rob Portman (R-OH) and Ranking Member Tom Carper (D-DE) are fluent in IT and cybersecurity issues given the former's tenure as OMB Director and the latter's involvement as a cosponsor with the "E-Government Act of 2002" and a sponsor of the "Federal Information Security Modernization Act of 2014" during his tenure as chair of the Senate Homeland Security Committee. They may well hold hearings but it is not as if Congress has not held hearings on inadequate federal cybersecurity. Moreover, whether this results in follow on legislation is questionable given full Committee Chair Ron Johnson's (R-WI) reputation as being the roadblock that kills bipartisan House cybersecurity legislation. Conceivably, a bill like the "Federal CIO Authorization Act of 2019" (H.R. 247), which easily passed the House in January, could be enacted to address some of the problems PSI turned up. However, despite the bipartisan support in the House as this bill was passed by voice vote, the bill has not been acted on in the Senate Homeland Security Committee.

House Intelligence Reauthorization Marked Up

The House Intelligence Committee marked up and reported out a three-year intelligence reauthorization six weeks after the Senate Intelligence Committee finished work on its bill. On June 27, the Committee met in a closed session and considered the "Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act (IAA) for Fiscal Years 2018, 2019, and 2020" after adopting an amendment in the nature of a substitute by unanimous voice vote. In their press release, the Committee explained "[t]he combined bill for the fiscal years 2018, 2019, and 2020 includes provisions:

- Prioritizing the IC's collection and analytic capabilities against hard target countries, namely China, Russia, Iran, and North Korea, while sustaining critical intelligence capabilities that support counterterrorism and counterproliferation efforts;
- Adapting the IC to operate in a strategic environment of rapid technological change, while posturing it to better leverage commercial innovation;
- Securing the IC itself, through provisions intended to insulate it from supply chain risks and to mitigate insider threats, among many other things;
- Reinforcing existing hiring pipelines, broadening engagement with nontraditional communities, and reducing barriers to onboarding, such as security clearance backlogs, to ensure the IC consistently recruits, hires, retains and promotes the most highly qualified, and most highly diverse possible workforce;"

CISA Issues Warning About Iranian Cyber Attacks; Administration Leaks Word Of U.S. Reprisals

The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued a statement and warnings in light of "a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies." CISA Christopher Krebs explained "[w]e will continue to work with our intelligence community and cybersecurity partners to monitor Iranian cyber activity, share information, and take steps to keep America and our allies safe." He added that "Iranian regime actors and proxies are increasingly using destructive 'wiper' attacks, looking to do much more than just steal data and money." Krebs added that "[t]hese efforts are often enabled through common tactics like spear phishing, password spraying, and credential stuffing…[and] [w]hat might start as an account compromise, where you think you might just lose data, can quickly become a situation where you've lost your whole network."

The warning from CISA comes a week after increasing tensions between the U.S. and Iran spilled over in the cyber realm as multiple media reports indicate Iran launched attacks against U.S. agencies and oil and gas companies. Other reports suggest the U.S. retaliated against an organization with ties to Iran's Revolutionary Guard. These reports quoted "two former intelligence officials" who claim Cyber Command targeted an organization that has been tracking U.S. Navy vessels and other ships in and out of the Persian Gulf. In light of other recent media reports that Cyber Command successfully penetrated and planted malware deep in Russian utilities as part of its campaign during the 2018 mid-term election, the forays against Iranian entities may signal an ongoing and possibly escalating use of cyber operations by the U.S.

PCLOB Has Full Membership and Details Its Oversight Agenda

The Senate confirmed three nominees to the Privacy and Civil Liberties Oversight Board (PCLOB) by voice vote this week: Aditya Bamzai, Travis LeBlanc and Edward Felten. However, Felten was technically confirmed to serve his own term as he has been serving out the remainder of someone else's term. These new members join Chair Adam Klein and Board Member Jane Nitze who were confirmed last year.

This week, before the confirmation of the three new members, the PCOLB voted to "initiate three new oversight projects:"

- The aviation-security project will examine how facial recognition and other biometric technologies are used to verify identity at each phase of a journey, from booking to baggage claim. The project will consider both operational benefits and privacy and civil liberties concerns arising from the use of biometric technologies in the aviation-security context.
- The Board has voted to review the FBI's "querying" (or searching) of data obtained pursuant to Section 702 of the Foreign Intelligence Surveillance Act. The review will also examine the procedures and technology used to record queries and ensure compliance with applicable rules.
- The Board has voted to conduct an oversight project related to the use of airline Passenger Name Records.

PCLOB has been a point of contention between the U.S. and the E.U. During the annual reviews of the Privacy Shield agreement that governs the flow of personal data of E.U. citizens transferred to the U.S. for processing, European authorities have expressed their concerns that the PCLOB was not functional and then operating without a full complement of Board Members. In the last annual report, the European Data Protection Board (EDPB) stated it

> can only encourage the PCLOB to issue further reports, on Presidential Policy Directive 28 (PPD-28), to follow up on the first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a follow-up report on Section 702 FISA. The EDPB recalls that the WP29 considered a report on Section 702 important for assessing whether the collection of data under section 702 is not indiscriminate and access is not conducted on a generalized basis under the UPSTREAM program, and for assessing the necessity and proportionality of the definition of "targets", the tasking of selectors under section 702 (including in the context of the UPSTREAM program), as well as the concrete process of application of selectors in the context of the UPSTREAM program to clarify whether massive access to data occurs in this context.

NIST Refines Thinking On Forthcoming Privacy Framework

In advance of the third public meeting on its forthcoming Privacy Framework next week, the National Institute of Standards and Technology (NIST) released Supplemental Materials to the Privacy Framework Discussion Draft on which NIST is accepting comment. NIST explained that it "developed the following documents based on stakeholder input received since the release of the Privacy Framework Discussion Draft (Discussion Draft)." NIST stated that "[w]hile the Discussion Draft is still the current complete working draft of the framework, these materials are intended to drive additional feedback about aspects of the Discussion Draft that generated significant dialogue." NIST said it "will use feedback on these materials to develop a preliminary draft of the framework."

Here are the Supplemental Materials:

- **Two Proposed Cores: Integrated and Separated Versions.** The two proposed Cores offer different levels of alignment with the Cybersecurity Framework. In the Separated Core, NIST has removed the overlapping Cybersecurity Framework Functions, Categories, Subcategories that pertain to data security. In contrast, the Integrated Core maintains data security Functions, Categories, and Subcategories that overlap with the Cybersecurity Framework. In addition, each Core contains the same updates based on specific feedback on the Discussion Draft Core. A summary of material changes can be found in each document.

- **Draft Executive Summary**. This extended summary is intended to clarify issues about the scope and purpose of the Privacy Framework that generated significant dialogue, including privacy risk to individuals and the relationship to organizational risk, privacy risk assessment terminology, the relationship of privacy risk and cybersecurity risk, and organizational roles.
- **Hypothetical Use Case Profiles**. Two hypothetical use cases to improve understanding of the Core and demonstrate how the development of Profiles can increase collaboration and dialogue across organizations and support risk-based decisions.
- **Proposed Roadmap Topic Areas**. This document proposes priority areas that pose challenges to organizations in achieving their privacy objectives for inclusion in a companion roadmap to the Privacy Framework.
- **Glossary**. This document contains updated terms and definitions.

In the Draft Executive Summary, NIST offers this summary of what the agency hopes the Privacy Framework will be:

> The Privacy Framework provides a shared lexicon and is a practical tool that can assist organizations—even those fully compliant with relevant laws or regulations—in making ethical decisions when designing or deploying their products and services and avoiding losses of trust that damage their reputations and can slow adoption or cause abandonment of these products and services.

NIST added "[t]he Privacy Framework is intended to be widely usable by organizations of all sizes and agnostic to any particular technology, sector, law,or jurisdiction...[and] [d]ifferent parts of an organization's workforce, including executives, legal, and IT may take responsibility for different outcomes and activities." NIST explained that "[w]hile privacy is often discussed in compliance terms, the Privacy Framework highlights that regulatory compliance is only one piece of the puzzle, and often should be viewed as the floor instead of the ceiling."

NIST launched its "Privacy Framework: An Enterprise Risk Management Tool" through the release of a request for information (RFI) in November 2018 that led to the development and release for comment of the Discussion Draft. NIST's effort started two months after the National Telecommunications and Information Administration (NTIA), another Department of Commerce component agency, requested comments "on ways to advance consumer privacy while protecting prosperity and innovation" and more specifically on "a proposed approach to this task that lays out a set of user-centric privacy outcomes that underpin the protections that should be produced by any Federal actions on consumer-privacy policy, and a set of high-level goals that describe the outlines of the ecosystem that should be created to provide those protections." This was intended to guide the Trump Administration's approach to the differing requirements of the EU's GDPR, the California Consumer Privacy Act, and other regimes that have come into effect or will soon come into effect. However, the abrupt departure of former NTIA head David Redl in May may set NTIA back in this effort and may have signaled turbulence at the agency.

NIST Paper Focus on Cybersecurity and Privacy of IoT

The National Institute of Standards and Technology (NIST) has released a publication designed "to help organizations better understand and manage the cybersecurity and privacy risks associated with individual Internet of Things (IoT) devices throughout the devices' lifecycles." Although the recommendations in this document are not binding on federal agencies, federal contractors, or other private entities, it is quite likely that NIST's cachet could result in this and other IoT documents setting a de facto standard for IoT security and possibly be folded into federal legislation. Nonetheless, the agency claims the publication "provides insights to inform organizations' risk management processes" and "[a]fter reading this publication, an organization should be able to improve the quality of its risk assessments for IoT devices and its response to the identified risk through the lens of cybersecurity and privacy." It bears note that from the onset of tackling IoT standards that NIST is pairing cybersecurity and privacy unlike its Cybersecurity Framework which addresses privacy as an important but ancillary concern to cybersecurity. This reflects the agency's growing awareness of privacy risks and how they correlate to cybersecurity. This coupling may foretell a sea change in how policymakers in Washington view the two issues.

NIST explained that NIST Interagency or Internal Report 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks is aimed at "personnel at federal agencies with responsibilities related to managing cybersecurity and privacy risks for IoT devices, although personnel at other organizations may also find value in the content." NIST stated that "[t]his publication emphasizes what makes managing these risks different for IoT devices in general, including consumer, enterprise, and industrial IoT devices, than conventional information technology (IT) devices...[and] omits all aspects of risk management that are largely the same for IoT and conventional IT, including all aspects of risk management beyond the IoT devices themselves, because these are already addressed by many other risk management publications."

NIST explained that "[t]his publication identifies three high-level considerations that may affect the management of cybersecurity and privacy risks for IoT devices as compared to conventional IT devices:

1. Many IoT devices interact with the physical world in ways conventional IT devices usually do not. The potential impact of some IoT devices making changes to physical systems and thus affecting the physical world needs to be explicitly recognized and addressed from cybersecurity and privacy perspectives. Also, operational requirements for performance, reliability, resilience, and safety may be at odds with common cybersecurity and privacy practices for conventional IT devices.
2. Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can. This can necessitate doing tasks manually for large numbers of IoT devices, expanding staff knowledge and tools to include a much wider variety of IoT device software, and addressing risks with manufacturers and other third parties having remote access or control over IoT devices.
3. The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices. This means organizations may have to select, implement, and manage additional controls, as well as determine how to respond to risk when sufficient controls for mitigating risk are not available.

NIST lays out "[c]ybersecurity and privacy risks for IoT devices can be thought of in terms of three high-level risk mitigation goals:

1. Protect device security. In other words, prevent a device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other

organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.
2. Protect data security. Protect the confidentiality, integrity, and/or availability of data (including personally identifiable information [PII]) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device except those without any data that needs protection.
3. Protect individuals' privacy. Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection. This goal applies to all IoT devices that process PII or that directly or indirectly impact individuals.

Incidentally, the "Internet of Things Cybersecurity Improvement Act of 2019" (H.R. 1668/S. 734) all but references the completion of this NIST initiative by name as being a condition antecedent to the development of recommendations and guidelines the agency must provide the Office of Management and Budget (OMB). And, of course, this bill was marked up and reported out of committee last month by both House Oversight and Reform and Senate Homeland Security. The other NIST effort referenced in the bill, the draft document "Considerations for a Core IoT Cybersecurity Capabilities Baseline," was released for comment in February and NIST will hold a workshop next month "gather feedback on NIST's approach to the IoT Cybersecurity Baseline and related taxonomy as well as discuss current status and future directions of this work." NIST also released a white paper last year, the "Internet of Things (IoT) Trust Concerns," that "identifies seventeen technical trust-related issues that may negatively impact the adoption of IoT products and services…[and] offers recommendations for mitigating or reducing the effects of these concerns while also suggesting additional areas of research regarding the subject of 'IoT trust.'"

Further Reading

"The Culture War Has Finally Come For Wikipedia" – *BuzzFeed News*
"IG: DHS needs more election tech help, IT patching" – *FCW*
"Inside the West's failed fight against China's 'Cloud Hopper' hackers" – *Reuters*
"NSA Improperly Collected U.S. Phone Records a Second Time" – *Wall Street Journal*
"Huawei Telecom Gear Much More Vulnerable to Hackers Than Rivals' Equipment, Report Says" – *Wall Street Journal*
"U.S. Tech Companies Sidestep a Trump Ban, to Keep Selling to Huawei" – *New York Times*