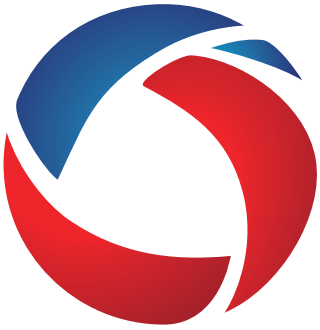


IT Alliance
for Public Sector
A Division of ITI

Tech Industry's Recommendations For Federal IT Modernization

Tech Industry Recommendations for Federal IT Modernization

Summary

The IT Alliance for Public Sector (ITAPS), a division of technology industry trade group ITI, has developed the following extensive recommendations on a wide-range of issues the White House can take to improve the United States government's information technology (IT).

Developed by a group of industry experts convened by ITAPS, the proposals are aimed at strengthening U.S. cybersecurity and national security, attracting talented IT workers needed at federal agencies, enhancing government services, improving federal efficiency and saving tax payers' money.

The recommendations were developed following meetings between White House officials and technology company executives where they discussed eight topics critical to modernizing federal IT (arranged by alphabetical order):

- **Big data/Analytics**
- **Citizen services**
- **Cloud infrastructure**
- **Cybersecurity**
- **Future trends**
- **Partnerships**
- **Purchasing**
- **Talent**

The following recommendations cover each of these topics and were developed by a task force comprised of over a hundred private sector experts from ITAPS member companies convened over a five-week period.

About ITAPS

The IT Alliance for Public Sector (ITAPS), a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies offering the latest innovations and solutions to public sector markets. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more.

Table of Contents

IT Alliance
for Public Sector
A Division of ITI

Big Data - Analytics

Topline Recommendations

1. **Establish that security of the data is paramount and responsibility for that security rests with senior executives and at the programmatic level.**

2. **Create a multi-agency data governance entity empowered to set government-wide data requirements.**

3. **Launch a Data and Analytics Center of Excellence (CoE) to achieve fast, consistent answers to business questions.**

4. **Foster a data-driven culture by requiring executives to set the tone and lead by example.**

5. **Capitalize on the granular, higher-quality, spending data that has been mandated by Congress through the Digital Accountability and Transparency Act of 2014 (DATA Act) law.**

6. **Avoid creating "bad data" by correctly managing the digitization of existing processes in government.**

7. **Expand private sector access to government data to drive additional economic growth.**

8. **Embrace the storage capabilities of cloud computing to enable data analytics.**

9. **Leverage capabilities to set real-time data and decision making as the baseline goal.**

Big Data/Analytics
Detailed Recommendations

1. **Establish that security of the data is paramount and responsibility for that security rests with senior executives and at the programmatic level.**

   The summary of the June WH CEO meeting was silent on this point. Specific actions to achieve and maintain security of data found in federal networks and systems are detailed in the cybersecurity recommendations offered in this report.

2. **Create a multi-agency data governance entity empowered to set government-wide data requirements.**

   The future capabilities and opportunities that arrive when utilizing Big Data Analytics in a governed fashion will allow our country to provide a superior experience to its citizens. To achieve these future capabilities, a data governance model, and an appropriately resourced agency or group of people to support it, needs to be created. Such an entity should be charged, at a minimum, with identifying and maintaining: a common nomenclature and terminology; standards to be used; criteria for cleansing the data and the metrics to assess successful agency utilization of the data governance model. Additionally, this entity should be empowered to offer a fast-track mechanism for problem resolution, to make determinations about the use of data.

3. **Launch a Data and Analytics Center of Excellence (CoE) to achieve fast, consistent answers to business questions.**

   More effective analytics are critical to improving agency performance and efficiency, enhancing citizen services, combating fraud, guarding against cyberattacks, and fostering increased private sector use of public data to drive economic growth. New analytic tools and techniques can empower federal agencies to meet these needs, transforming rapidly-growing caches of mission and operational data into better insights, actions, and outcomes. Inhibitors for government adoption, however, include widespread, poor data quality, a skills gap driven by growing technical complexity, and the need to provide even faster insight for agencies operating at mission speed. A Data and Analytics Center of Excellence (CoE) brings together the critical mass of expertise required to overcome these challenges. Unlike shared services centers, focused primarily on efficiency, a CoE would be charged with making more innovative uses of analytics readily accessible across agencies.

   Designed to work in conjunction with the data governance entity created above, the CoE would encompass cross-disciplinary teams with diverse skills, working in a highly collaborative environment to quickly evaluate and implement new approaches to problem solving. Working iteratively in an agile manner, the CoE can rapidly test and refine a variety of techniques to produce the optimal approach and outcome. Finally, a CoE can help federal agencies attract scarce, in-demand talent to public service by offering the unique opportunity to work on groundbreaking challenges in the government and train other staff on emerging practices.

4. **Foster a data-driven culture by requiring executives to set the tone and lead by example.**

   The Administration should ensure – through the application of Big Data Analytics to operational data – that actions within the federal government should be based upon, and substantiated with, data and evidence-based decision making, including the identification of measurable objectives and anticipated outcomes. Agency business leaders should be given a larger role in analytics, including ownership and accountability for areas like finance – with corresponding requirements to align analytics and business requirements – to ensure that there is a clear understanding of the question(s) to be answered.

5. **Capitalize on the granular, higher-quality, spending data that has been mandated by Congress through the Digital Accountability and Transparency Act of 2014 (DATA Act) law.**

   Federal agencies and the public have begun to benefit from these data practices for financial data and the Administration should ensure that these initiatives are leveraged to identify cost savings, combat fraud, waste, and abuse, enhance accountability and improve citizen services.

6. **Avoid creating "bad data" by correctly managing the digitization of existing processes in government.**

   "Bad Data" is information that can be erroneous, misleading, or poorly formatted that systematically impacts decision makers, managers, and workers. The digitization of paper-based and other processes in the federal government should be effectively managed to ensure that the outcome can contribute clean, machine-readable data that can further empower agency decision making and mission activities. We should not just digitize existing processes but first, assess the reason for the process and, second, determine whether that need is still valid. Once that validity is established, the governance model requirements should be applied.

7. **Expand private sector access to government data to drive additional economic growth.**

   OMB's Open Data Policy – Managing Information as an Asset (M-13-13) established approaches for making government data more open and accessible to the private sector and machine-readable. The new Administration should leverage existing programs, like Project Open Data, to identify and prioritize the disclosure of high-value government data sets to incentivize entrepreneurs and innovators to invest in new products and capabilities.

8. **Embrace the storage capabilities of cloud computing to enable data analytics.**

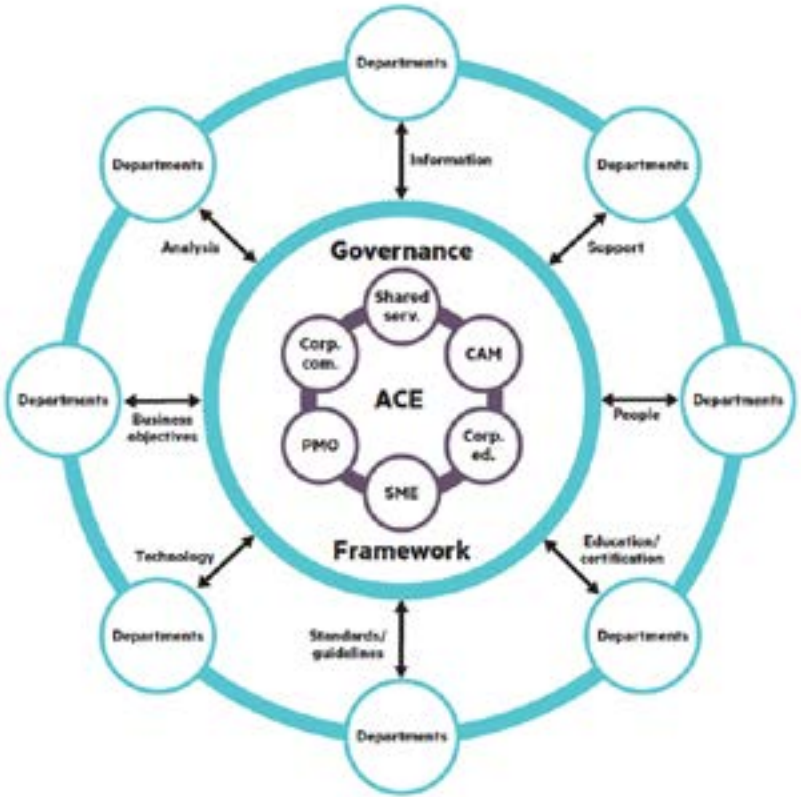
   The lack of inexpensive, reliable, secure, and fast storage is a major inhibitor to consolidating and utilizing Big Data in the federal government. By using cloud-based delivery models, federal agencies can address these constraints, while establishing third-party access to data and limiting the exposure of the underlying systems.

9. **Leverage capabilities to set real-time data and decision making as the baseline goal.**

   Imagine being able to stop fraudulent transactions from going through Medicaid payment processing as fast as your credit card can be frozen when the card-issuer's systems identify abnormal spending behavior. Instead of someone finding fraudulent activity weeks, months or even years after it has occurred, utilizing real-time data analytics and processing applications can identify such activity and prevent the expenditure of government funds in the first place.

   Automation is a process that is more frequently being seen in a variety of industries. Removing human interaction, decision, or error from a particular process normally indicates business will see better outcomes. With government processes, there is hesitation to allow machines and programs to make decisions. But to truly deliver effective data analytics, the federal government should let the data be aggregated and analyzed, but continue to have a designated official in charge of executing decisions. As technology continues to advance, machine learning and artificial intelligence will become impossible to ignore if we expect the federal government to keep advancing at a similar pace of innovation that is being driven by the private sector.

Analytics Center of Excellence Model Structure



ACE benefits

1. Improves business outcome
   a) Builds analytic competencies
   b) Provides consistent answers to questions
2. Maximizes assets to meet information requirements
   a) Reduces time to get answers
   b) Increases information access efficiencies
3. Incorporates certification and education program
4. Uses standards and guidelines
5. Meets regulatory and confidentiality commitments
6. Provides a workplace that attracts and retains industry-leading resources

Government Framework for Analytics Center of Excellence

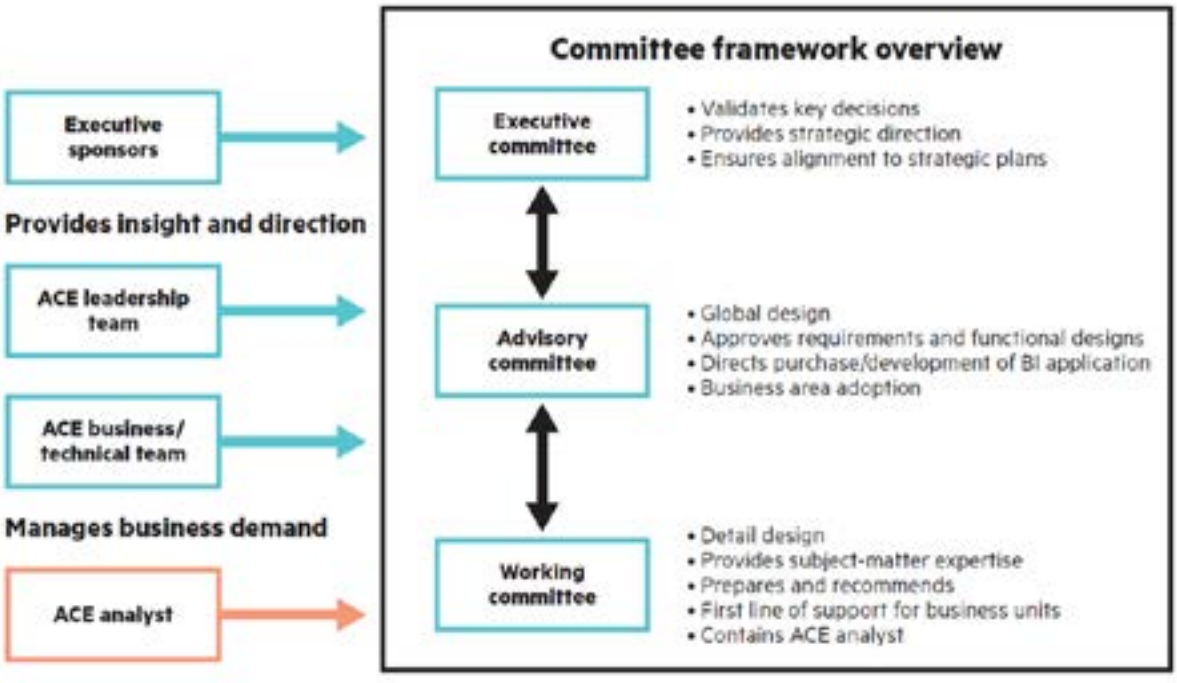


Figure 4. Governance Framework

Big Data/Analytics
Additional Resources

Analytic Use Cases – Hewlett Packard Enterprise

Better Decisions, Better Government: Effective Data Management Through a Coordinated Approach – National Association of State Chief Information Officers

Citizen Insight Dashboard – Hewlett Packard Enterprise

Data Analytics for Payment Accuracy, Program Integrity, and Efficiency - SAS

Data.Oregon.gov – The First Citizen Social Interactive State Data Portal

Enhancing Postal Efficiency - Intel

Transitioning to Digital Government Primer for 2017 - Gartner

Inspiring Innovation with Next-generation Analytics - Intel

Insights Platform for Government - Accenture

Launching an Insights-Driven Transformation - Accenture

Social Media Analytics – Hewlett Packard Enterprise

The 5As of Analytics Transformation - Accenture

Voice of the Citizen: The Path to Future Citizens – Hewlett Packard Enterprise

Transform Federal Government Services - Microsoft

Microsoft in Government: Federal Government Solutions

Government Connected Field Service Solutions - Microsoft

Connected Field Service Solution by Microsoft

Big Data and Advance Analytics Solutions | Microsoft Azure

IT Alliance
for Public Sector
A Division of ITI

Citizen Services

Topline Recommendations

1. **Establish senior executive accountability at the Office of Management and Budget (OMB) and in the departments and agencies at the Undersecretary or Deputy Secretary of Management-level for the citizen or customer experience (additional refinement as needed) with appropriate funding and authorities.**

2. **Require agile and human centered design to start acquisition or project development.**

3. **Utilize shared services, where appropriate, to establish consistent citizen experiences across the government enterprise.**

4. **To the greatest extent practicable, citizen services should have the following attributes:**
   - **Use human/citizen-based design**
   - **Offer transparency**
   - **Provide self-service options**
   - **Offer immediate customer service**
   - **Secure payment processing**
   - **Embrace a digital baseline**
   - **Deliver a consistent and personalized experience**

5. **Identify and inventory the highest-impact citizen facing services by agency and establish cost baseline data around the provision of those services.**

6. **Create incentives for cultural change by modifying Executive/Senior Executive Service (SES) level and government personnel agreements to include citizen experience improvement and tie evaluations and bonuses to metrics showing improvements.**

7. **Establish mechanisms to collect and analyze customer feedback for government/citizens services on a real-time basis and exempt voluntary provision of customer feedback from PRA information collection clearance approvals at OMB.**

8. **Deliver and manage services, to the maximum extent practicable, through an omnichannel approach. Citizen experiences should be consistent and agnostic of the channel they use to access a service.**

9. **Expand and Improve General Services Administration (GSA) Digital Analytics Program (DAP) to measure customer experience to improve government websites.**

Citizen Services
Detailed Recommendations

1. **Establish Senior executive accountability at OMB and at the Undersecretary or Deputy Secretary of Management-level in the agencies and departments for the citizen or customer experience with appropriate funding and authorities.**

    - In the private sector, the Chief Experience Officer is the individual responsible for delivering better customer experience and superior service. In the federal government, no single individual has that responsibility and, citizen service often falls through the cracks.
    - OMB should establish accountability at the Secretary-level to promote and deliver a 21st century digital experience to citizens.
    - Agencies should be required to establish citizen experience metrics and strategies within 6 months that includes a customer experience baseline, consistent and measurable data that is based on qualitative and quantitative voice of the customer and customer experience feedback. The strategy should prioritize the implementation of customer services that eliminate the need for a citizen to physically visit a federal building by providing the same customer service online.

2. **Require human centered design, along with agile, to start acquisition or project development.**

    There is broad consensus that information technology (IT) projects should be developed and delivered using leading commercial practices, including agile and human centered design, to speed time to value, reduce risk, lower costs, and better meet the needs of users, as recommended in the Digital Services Playbook (see plays #1 and 4). To fully achieve these objectives, agencies should use human centered design, starting in acquisition planning, to ensure IT initiatives are designed around the needs of users and customers, including both employees and/or citizens, and desired mission outcomes, rather than around government organizations, policy, process, or technology. Just as agencies are starting to require use of agile, major modernization and other significant IT investments should require human centered design, including use of immersive user and stakeholder research, to increase mission impact, accelerate adoption, and achieve lasting success.

3. **Utilize shared services, where appropriate, to establish consistent citizen experiences across the government enterprise.**

    Certain administrative functions are similar within government agencies regardless of mission, including financial management (FM), human resources (HR), acquisition, IT, grants management, and travel, which are all support service areas common across federal government agencies. By removing redundant internal services and adopting interagency shared services for administrative functions, government agencies can dedicate more time, energy, and resources to their core missions, thereby providing government the opportunity to improve interaction with its customers.

    "The drive to embark on this transformational journey is fueled by the need for a higher performing, more responsive government, emerging technologies that enable agencies to securely leverage common systems, services and data in ways they never have, the benefits of reduced duplication, more resilient cyber-security strategies, and opportunities to optimize operations and improve quality based on process and system standardization. The status quo, where 80% of the $80 billion Federal IT budget is dedicated to maintaining legacy systems, is simply not sustainable or beneficial in the future." (Unified Shared Services Management (USSM) Mission-Support Services—Concept of Operations Roles and Responsibilities)

Some examples of state citizen services done well that can be leveraged through shared services to create enterprise-wide availability in the federal government include:

- Licensing and permitting solutions
- Contact call centers
- Common points of entry/shared data for like-services
- Financial transparency solutions
- Grants management
- Loan processing
- Claims processing
- Case management solutions

4. To the greatest extent practicable, citizen services should have the following attributes:

- Use human/citizen-based design
- Offer transparency
- Offer self-service options
- Offer multi-platform, on-demand customer service
- Secure payment processing
- Embrace a digital baseline
- Provide a common look and feel in standardized interfaces for all government services

Citizens expect a consistent, cohesive experience across channels which today requires agencies have a 360-degree view of their customer. To that end, citizen services should embrace digital government transformation and online transactions. Each government transaction should offer an accessible digital experience option with the promise of improved digital service delivery by government to its citizens. Not only does a digital service offer expanded experience options, it also offers cost savings considering the average in-person government transaction costs $16.90, compared to the average online government transaction of $0.40 (40 cents) and in doing so can allow in-person transactions to address complex issues more efficiently by moving common functions online. [1]

Citizen services are most successful when they incorporate key attributes that align with citizen expectations.

For government agencies and organizations to provide effective services, they should create and execute on solutions that rely on a human/citizen-based design. The most successful services are ones that understand human behavior and accessibility issues and consider trends in user experience. For example, increasingly citizens are receiving information on-the-go, so it has become increasingly important that they have access to mobile-friendly content. This means ensuring that digital materials (blogs, event sign ups, emails and alerts) are accessible via all personal devices and utilize services like interactive text messaging.

This also means that in general, human attention spans have decreased. To get and keep a citizen's attention, government agencies need to create content that is short and to the point. Citizen services should also be transparent. Government information must be communicated in a way that is accessible and easy to understand. This means it is crucial to communicate with citizens using plain language guidelines to prevent messages from getting lost in translation.

Finally, citizen services should meet the customer where and when they need it while providing the same level of service and experience they have come to expect from their interactions with the private sector. To

1 Deloitte Access Economics study; data regarding digitizing transactions in Australia

the greatest extent possible, self-service options that facilitate fast, easy, multi-channel transactions should be offered. Citizen services must also provide on-demand customer service for users and secure payment processing to ensure privacy of personal data.

5. **Identify and inventory the highest-impact citizen facing services by agency and establish cost baseline data around the provision of those services.**

   The administration should build on the existing OMB data that identifies the highest impact citizen facing service, and should prioritize and focus improvement efforts on those services. An inventory of services should be conducted to build out the existing data and to establish a thorough baseline that captures end-to-end cost of service delivery, as well as available customer experience data. Setting such a baseline is critical to understanding current cost and quality of services. The baseline should be used to define measurable, meaningful targets for improvements, to track results and identify opportunities for greater efficiency, better service and to meet gaps in customer experience. Given that citizen services often cross program and agency organizational boundaries, it is especially important to collect, analyze and share standardized data on the end to end experience rather than in program specific silos. This approach will also foster cross agency collaboration and sharing of best practices that show proven results.

6. **Create incentives for cultural changes by modifying Executive/SES level and government personnel agreements to include citizen experience improvement and tie evaluations and bonuses to metrics showing improvements.**

   Government personnel today, at all levels, are evaluated using outdated metrics and are not incentivized through the evaluation, career advancement, compensation, and bonus processes to evolve or change practices or the culture of their organization to achieve improvements, like the delivery of citizen services.

   OMB, working with the Office of Personnel Management (OPM), should develop new evaluation criteria within 6 months that can be applied for personnel evaluations at all levels for 2018. These new criteria should be relevant for government personnel, no matter if they are senior political appointees, SES members, senior career, or general services government personnel and should focus on outcomes, not work volume, or output. The new criteria should include metrics for measuring the improvement of citizen experiences with government services and directly tie qualitative and quantitative improvements in those experiences to the achievement of career advancement and additional compensation in any form.

7. **Establish mechanisms to collect and analyze customer feedback for government/citizens services on a real-time basis and exempt voluntary provision of customer feedback from Paperwork Reduction Act (PRA) information collection clearance approvals at OMB.**

   Technology has enabled a variety of means to collect, in a real-time basis, feedback and satisfaction measurements from users and customers in a variety of settings. For government customers, agencies should be required to immediately deploy means of understanding and measuring customer experience for all citizen services offered at that agency. Customer experience feedback should measure both qualitative and quantitative experiences by agency customers and that feedback should inform metrics for further measurement and programmatic or customer service improvements that the agency can implement.

   Customer experience and satisfaction measurement is currently constrained by requirements in the PRA that all information collection conducted by an agency must either comply with the law or receive a waiver from OMB. While the PRA restrictions are well-meaning, they have hobbled the ability for government entities to solicit voluntary feedback and prohibit the collection of customer satisfaction and experience feedback from more than 9 people without OMB approval. The Administration should determine what

authorities it has to establish an exception to the PRA requirements when agencies are seeking voluntary feedback regarding customer experience with the provision of government services. Such an exception should be put in place as quickly as possible. Additionally, the administration should assess the Federal Citizen Services Reform Act of 2017 to determine what support could be afforded to permanently provide statutory authority for agencies to measure customer experiences for the purpose of improving government services.

8. **Deliver and manage services, to the maximum extent practicable, through an omni channel approach. Citizen experiences should be consistent and agnostic of the channel they use to access a service.**

Omni-channel is a synchronized operating model in which all communications channels are aligned and present a single face to the customer. In an omni-channel approach, the service provider effectively operates as a single channel, orchestrating high-value customer experiences across all touch points.

Omni-channel should deliver a customer experience that is seamless, consistent, and personalized through the integration of agent-assisted channels with digital channels, such as a website or social media platforms, so that customers can easily interact with agencies and obtain needed services and information, when, where, and how they choose.

Agencies should develop and implement a sustainable, scalable omni-channel approach for major citizen services, with a well-coordinated, enterprise level strategy that includes a central, common technology platform and toolset to ensure consistent, accurate information and services for employees and customers, independent of channel.

9. **Expand and improve the General Services Administration (GSA) Digital Analytics Program (DAP) to measure customer experience to improve government websites.**

- Establish agreed upon metrics to determine the effectiveness of and customer satisfaction with government federal websites. These should include:
  - Overall customer experience
  - Completion rate of intended task
  - Percentage of visitors, likely to recommend the website
  - Ensure all agencies better utilize DAP data to make performance improvements
  - Leverage government-wide use of web analytics data libraries
  - Consider the issuance of a government-wide policy timeline to implement the DAP per the November 8, 2016 OMB Policies for Federal Agency Public Websites and Digital Services guidance.

The Digital Analytics Program (DAP) offers advanced Web analytics to federal agencies so they can assess website performance and use it to drive improvements in on-line content and service delivery. The program is a hosted shared service provided by GSA's Technology Transformation Service. On November 8, 2016, the Office of Management and Budget (OMB) released a memorandum on Policies for Federal Agency Public Websites and Digital Services, which requires federal agencies to implement the DAP JavaScript code on all public facing federal websites. OMB should ensure agencies are complying with this requirement, and using DAP and similar web analytics data to improve and manage website performance.

While DAP's web analytics and the public facing analytics.usa.gov site provide valuable, actionable insight on website performance and gaps, it should be expanded to include customer satisfaction measurement, as intended when the 2012 Digital Strategy established it. This data can provide valuable "voice of the customer" data that will enable further understanding of customer experience with government website and services.

Citizen Services
Additional Resources

Citizen Experience (CX) Check List - Highpoint

Connected Government: The Innovation Dimension - Telstra

Creating An Infrastructure And Machinery For Exceptional Customer Experience

Customer Experience – Partnership for Public Service/Accenture

Government for the People – Partnership for Public Service/Accenture

Leading in the New - Accenture

Transforming Government Customer Service - Highpoint

Enriched Citizen Services Through Service Design - Accenture

Montana's eGovernment Services: Assessing the Last Decade

The Most Important Customer: Improving the Citizen Experience with Government – Partnership for Public Service/Accenture

The Power of Personalization - Accenture

The University of Utah eGovernance
- Smarter eGovernment: The Benefits of Online Services for Utah Businesses
- Smarter eGovernment: Multi-State Report 2013
- Utah.gov: Connecting Residents and Government

The Voice of the Citizen – Hewlett Packard Enterprises

Citizen Services Solutions - Microsoft

Reinvest Productivity for Citizen Engagement - Microsoft

Government Connected Field Service Solutions - Microsoft

Accessibility

IT Alliance
for Public Sector
A Division of ITI

Cloud/Infrastructure

Topline Recommendations

1. **Establish an automation first goal for information technology (IT) modernization efforts:**
   a. **Automation of existing applications and infrastructure;**
   b. **Establish interoperability standards;**
   c. **Automating cloud deployments and migrations;**
   d. **Integrating the automation of application development, operations, and security (DevOpsSec);**
   e. **Automating security assessment processes.**

2. **Facilitate access to a cloud marketplace.**

3. **Cloud migration and transformation – a recommended process:**
   a. **Establish a cloud strategy;**
   b. **Proper planning;**
   c. **Assess the applications for suitability to the cloud;**
   d. **Identify the target platforms:**
   e. **Modernization of the applications and associated process;**
   f. **Build the roadmap.**

4. **Accelerating cloud adoption in the federal government:**
   a. **Evaluate the current accreditation process;**
   b. **Enablement/transparency;**
   c. **Evolution.**

Cloud/Infrastructure
Detailed Recommendations

The industrial revolution is replete with examples of American ingenuity, converting bespoke craftsmanship into automated processes. Henry Ford capitalized on the intersection of the moving assembly line, standardized parts, and workflows to bring affordable transportation to the world. Due to the gains in efficiency, Ford's Model T dropped from an initial price of $825 in 1908 to a cost of $575 in 1912. Ford's introduction of assembly line technologies and standardization resulted in his capturing 48 percent of the automotive market by 1914. Twenty-five years later, Ford Motor Company would be called upon by the United States government to aid in the war effort. Led by Charles Sorenson, Ford's vice president of production, the company transformed the production of the B-24 Liberator from a one-off bespoke operation to a standardized, assembly line production to serve U.S. war efforts. Production raced ahead from one Liberator a day to a peak output of one Liberator an hour.

A similar automation opportunity presents itself to us today. Much has been accomplished in the federal government regarding its ability to deliver information technology (IT) infrastructure in a timelier manner, but much is left to be done. Automation, the elimination of waste, duplication, and manual effort, is a key ingredient to enabling cloud computing within government, education, and healthcare industries. Today, federal government IT professionals are yearning to be given the opportunity to match the pace of their commercial peers.

A recent International Data Corporation (IDC) study[1] acknowledges that the increasing demands of business transformation have served as a catalyst for "IT departments to become agile in responding to evolving business needs." In the study, a commercial off-the-shelf (COTS) DevOpsSec solution was found to drive a 531 percent five-year return on investment (ROI), with 66 percent faster application development life cycles, 35 percent less IT staff time required per application developed, 38 percent lower IT infrastructure and development platform costs per application and a $1.29 million average annual benefit per 100 developers deployed. With tens of thousands of developers deployed throughout the federal government, and systems integrators developing on behalf of the government, the potential returns are significant.

The benefits of automating federal government IT systems are manifold. The main points of these recommendations will focus on:

- Automating existing applications and infrastructure.
- Automating cloud deployments and migrations.
- Integrating the automation of Application Development, Operations, and Security (DevOpsSec).

1. Establish an automation first goal for IT modernization efforts

a. Automation of existing applications and infrastructure.

According to the Government Accountability Office's (GAO) Report GAO-16-696T,[2] the federal government spends more than 75 percent of its $80 billion technology budget on ongoing maintenance and operations. Alarmingly, this report goes on to note that "Specifically, **5,233** of the government's approximately 7,000 IT investments are spending **all of their funds on operation and management activities.**" This presents a target rich environment for the automation of processes, deployments, and configuration of IT assets.

1 https://www.openshift.com/sites/default/files/idc-business-value-of-openshift.pdf

2 http://www.gao.gov/products/GAO-16-696T

Manual approaches to packaging and deploying workloads are naturally lengthy, error-prone, and difficult to maintain. Even in situations where automation has been used, any initial understanding between business, development, and operations fades quickly over time as resources move up or out of the team, documentation lags, and specialized technical skills dwindle. An appropriate IT automation strategy can enable teams to treat legacy environments like DevOps, predictably automating provisioning and deployment with tools that foster understanding and involvement across the organization. Establishing an intelligent approach to developing, deploying, and managing automation requires more than a reliable and understandable platform. It requires informed governance that ensures reliable operations and responds readily to new challenges. Teams must collaborate across traditional departmental boundaries to share their latest challenges and insights. Careful consideration must be made to the organization and people/talent aspects of moving to such a model. Organizationally, a cross-functional team must be present to embrace automation; whereby each component that is to be automated (network, storage, compute, application) should all be included in such a team.

Skill-sets should also be examined for success. Traditional scripting skill-sets found within the datacenter infrastructure realm will only serve so far and examining integration engineering skills to stitch together application programming interfaces (APIs) calls to automate processes end-to-end should be considered.

b. Establish interoperability standards.

Currently, most automation capabilities are vendor-specific. As more metadata is required to define virtual networks, security requirements and compliance standards, these interoperable "blueprints" can become the pattern that facilitates true cloud brokering and application mobility. The administration should establish an iterative partnership with industry for identifying target workloads for automation and focus on the following:

- **Discover and assess.** Discuss goals, solution approaches, and next steps to:
  - Identify challenges and potential issues as well as viable approaches and technologies, necessary participants, and desired outcomes.
  -
  - Outline current state, target state, and opportunities for change.
  - Assess the current state against an industry benchmark as published by an authoritative third-party source (e.g., Gartner).
- **Design.** Develop an intelligent plan that delivers a(n):
  - Analysis of the current state architecture and organizational practices for the migration.
  - Strategy across people, processes, and technologies to deliver and scale IT services.
  - Architecture definition that addresses target environments.
  - Automation built into the design to minimize manual configuration and management of applications.

- **Deploy.** Work with industry subject matter experts, who will integrate with and guide your team to:

  - Modernize legacy approaches by automating configuration, provisioning, and deployment of systems and workloads.

  - Standardize tools, processes, and governance and centralize management for enterprise-wide automation.

  - Optimize culture, such as work methods, to promote collaboration and accelerate work.

  - Use an automation-first model where applications can be deployed and redeployed on a consistent basis. This benefits the entire organization from development to production.

c. Automating cloud deployments and migrations.

Throughout the commercial world, we have seen success with moving workloads to cloud providers. Federal government agencies are keen to capitalize on these opportunities - but need to understand that the value is not simply in applying an Operational Expenditure (OpEx) versus Capital Expenditure (CapEx) model - in leveraging the dynamic nature of cloud resources. These dynamic capabilities inherently call for cloud deployments to be fully automated.

Additionally, to guarantee the long-term viability of cloud deployments, it is incumbent upon chief information officers (CIOs) to have a verifiable cloud exit strategy. By automating deployments into clouds, we begin to automate how workloads will be moved out of that cloud, as well. Whether the next destination is another cloud provider or simply back to a government datacenter, automation will prove key in reducing the burden of moving that workload.

Increasingly, federal agencies are looking to use hybrid cloud, and even more recently, cross-cloud capabilities, to best ensure system availability across geographies and to realize the benefits of spot market conditions to drive down costs of government IT. As federal agencies move into these advanced deployment paradigms, manual administration, and rationalization of chargeback/showback accounting and governance becomes taxing, if not impossible. Cross-cloud services will be required to automate the discovery, metering, management, and provisioning of the workloads to support their applications across multiple cloud providers.

Manual systems imaging, deployment and patching is onerous and error prone. A significant portion of systems administration time is spent on these manual tasks and without a single system of truth from which to validate consistency across the enterprise -- verifiable consistency is impossible and they are prone to error. As agencies move into the cloud, the ability to guarantee consistency across cloud providers becomes mission critical and can only be achieved through automating the provisioning (Day 0), management (Day 2) of the workloads, and even a redeployment model that regularly redeploys the application to eliminate persistent threats.

Governance is also key to ensure visibility and continued risk assessment across the entire IT ecosystem, enabling traditional data center best practices in a multi-vendor cloud ecosystem as well. Federal agencies are already feeling the pains of cloud sprawl and cost creep. While the agility and power of cloud is gained, best practices for continued success with cloud is required. Automation and cloud tooling will provide much of the data required for a solid governance platform.

d. Integrating the automation of application development, operations, and security (DevOpsSec).

The marriage between the application development and operations teams is something that has been widely adopted by the commercial industry for several years. Only recently has the federal government initiated the examination of adopting a DevOps model to determine how they can restructure teams and/or contracts to embrace the inherent advantages (e.g., quicker time to support mission). To achieve the results desired, automation is a key ingredient to allow for the operations team(s) to keep up with the application developer's needs. Automating the infrastructure components are table-stakes, but how the operations team can offer automating the progression of an application from test/development to production environments is what's critical to success. This effort cannot be done only by development or only by operations. Only by working in partnership will they achieve the goal of being able to consistently deploy infrastructure, platforms, and applications to achieve the goal of continuous integration.

e. Automating security assessment processes.

Recently, in collaboration with the Office of American Innovation (OAI) and the American Technology Council (ATC), the General Services Administration (GSA) and the Federal Risk and Authorization Management Program (FedRAMP) issued a Request for Information (RFI), seeking to identify ways to incorporate automation into the Authority to Operate (ATO) process. This is an important step forward, as automating aspects of the Initial Authorization or Continuous Monitoring (aka Ongoing Authorization) processes would enable both government agencies and cloud service providers (CSP's) to gain important efficiencies. In this context, automation can also improve visibility for those charged with reviewing service provider security packages and/or agency implementations of security controls. Ultimately, greater visibility often helps organizations prioritize and improves security. Moreover, GSA and FedRAMP explicitly cited that automating authorization processes is intended to streamline processes, reduce risk of human error, and provide real-time data to understand vulnerabilities and to mitigate risks.

While it is encouraging that GSA and FedRAMP are taking steps to integrate automation, there are many areas in which automation could be helpful, and it may be most effective and efficient to determine priority areas to focus initial resources and efforts. In particular, System Security Program (SSP) documentation and ATO review comments and requests are two areas in which GSA and FedRAMP would be well served in focusing their attention. For SSP documentation, GSA and FedRAMP should standardize an eXtensible Markup Language (XML) or Javascript Object Notation (JSON) schema, incentivizing organizations to develop tools for data generation and consumption; then, CSP's and agencies could exchange system security plan information as data rather than maintaining and consuming potentially thousands of pages of system security plans and related attachments as documents. For ATO review comments and requests, rather than sharing comments over email and through spreadsheets, resulting in challenges in tracking and often duplication of work, GSA and FedRAMP should consider using a system like Team Foundation Server (TFS).

2. Facilitate access to cloud marketplaces.

The concept of a cloud marketplace may be relatively new for the federal government, but it is not new itself. All CSP's offer services using an online market concept. Access to cloud computing is attractive to federal agencies because it can quickly deliver IT capability, improve the delivery of constituent services, provide on-demand access to a shared pool of scalable computing resources, consolidate the need for capital expenditures for data centers, reduce duplicative system, and provide enterprise-level security.

To further facilitate the selling and purchasing of off-the-shelf commercial cloud-based services to the federal government, policymakers should consider leveraging commercial cloud marketplaces that will enable agencies to acquire cloud and cloud-based services in a commercial-like transaction. Given the relatively new concept of a cloud marketplace, we recommend that GSA convene a working group composed of private-sector experts and other key stakeholders to create a process whereby agencies can use a government-wide marketplace to acquire software through existing commercial marketplaces easily. If the federal government decides it wants to develop a pilot for the cloud marketplace and examine the option of accessing commercial cloud marketplaces, then the government should keep in mind the following principles to ensure a non-proprietary and open approach:

- **Ensure the fundamental principles of federal government procurement policy, including competition, are upheld**.

- **Clarify objectives:** What does the federal government seek to achieve with the marketplace? What are their objectives and priorities? Understanding and communicating the answers to these questions are necessary to inform the design of a marketplace and a process by which companies externalize their offerings.

- **Define the marketplace:** It is important to establish what a marketplace means. A marketplace should be a consolidated one-stop-shop for federal government agencies to be able to acquire cloud capabilities and associated services, and compare provider offerings against each other. This should include the ability to acquire multiple types of technology based solutions independent of vendor specific platforms and architectures.

- **Identify agency information needs:** The proposed working group's recommendations should also address the information that federal agencies need to have and share about their functions and their need to design a comprehensive cloud platform that provides a standardized format for detailing cloud solutions and their capabilities for agencies to objectively evaluate.

- **Establish a road map:** The proposed working group's recommendations must lay out an ideal future state, while acknowledging the current road-blocks to reform. They will help explain how the federal government can achieve the future state over time, while making immediate changes to improve the process of cloud acquisition now.

- **Operation by a neutral third-party:** The federal cloud marketplace should be run by a neutral third-party, such as GSA, but it should also involve a public-private partnership to facilitate the process by which vendors can update and manage their listings.

- **Embrace industry best practices:** The federal government should seek to understand current best practices in industry to see how commercial cloud marketplace examples can be leveraged. While these industry best practices will not always be a perfect fit for the government due to the unique regulatory landscape for federal sourcing, they should serve as a guide.

- **Leverage existing security standards**: The federal government should consider how it can leverage existing security certifications (i.e., FedRAMP, ISO 27000) to authorize accredited buys off commercial marketplaces.

- **Align federal government policies with commercial practices:** If the federal government wants to successfully utilize commercial cloud marketplaces for commercial cloud and cloud services purchases,

it should do so under commercial terms and conditions, not government-unique regulations. If the federal government decides to set up the marketplace, the government will need updated policies for procuring cloud services at the agency level. Working with policymakers to update statute to streamline the acquisition of cloud services via a marketplace[3] should be encouraged. Marketplace content should also consider including existing Government Wide Acquisition Contracts (GWACS) and Blanket Purchase Agreements (BPAs) as a model for how to structure buying strategies via a marketplace. The first steps toward a cloud services marketplace are seen with the recent creation and use of SIN-40 on GSA Schedule 70. Departments are already leveraging SIN-40 as the basis of cloud-specific contract vehicles, like the Department of Homeland Security (DHS) ECS (Enterprise Computing Services). There likely needs to be broader enablement on SIN-40 across federal agencies to ensure usage at levels like the rest of Schedule 70. While the Schedule itself is not a marketplace, it does provide mechanics and a basis from which to build.

3. Cloud migration and transformation – a recommended process.

Federal agencies are under tremendous pressure to migrate to cloud as part of the Office of Management and Budget (OMB) cloud-first policy, however, agencies continue to struggle to determine the best form of migration for the individual applications within their respective portfolios. The cloud-first policy was an unfunded mandate that has had varying levels of success, depending on how progressive the CIO is and associated driving factors such as budget cuts.

Cloud transformation should not be just about moving applications to a different environment. Instead, use cloud implementations to digitally transform processes, including the way that citizens, other agencies, industry, and other governments interact [4]. In some cases, this includes retraining the workforce to enable the IT staff to leverage cloud technologies. In other cases, technologies have already been extended to support hybrid (on-premise or cloud) environments with no retraining required. In all cases, agencies will need to empower mission staff to think digitally.

When looking at the possibility of moving an application to a cloud environment, there are a series of questions that should be evaluated and answered as part of determining that possible best end-state:

- How do I develop and test applications in the cloud?
- How do I manage applications in the cloud?
- What applications should I move to the cloud?
- How do I assess which are the first and last to move to the cloud?
- What cloud service provider is best suited for each application?
- How do I make applications ready for the cloud?
- How do I integrate applications in the cloud with my other applications?
- How do I ensure portability and avoid vendor-lock in?
- And more importantly, how do I integrate my business processes with applications and workloads in the cloud?
- How do I secure applications in the cloud?
- How do I design for the user experience in the cloud?
- How do I design for availability in the cloud?
- How do I maintain visibility in the cloud?
- How do I architect for the cloud to allow portability between cloud service providers?

Leveraging a process to drive the transformation of applications to cloud enables federal agencies to determine cloud suitability for their applications as they plan the transformation of their application and infrastructure environment. The process is comprised of five steps as described below:

---

3 For further recommendations on how to better streamline government acquisition, please see Purchasing section of this document.

4 For further recommendations on process digitization and citizen services, please see the Citizen Services section of this document.

- **Establish a cloud strategy.** The purpose of the cloud strategy is to help federal agencies shape their journey to the cloud, and prepare their organization to adopt cloud technologies. During the development of a cloud strategy, agencies need to develop an understanding of mission and business essentials that cloud technologies need to address. Agencies also need to develop operational and technical representation of the future state, leveraging cloud technologies.

- **Proper Planning.** The key to a successful cloud transformation starts with the proper planning, team organization, creating a timeline for the effort, and defining metrics for success. When planning, federal agencies need to establish the imperative that drove the decision to migrate to the cloud, define the future state of the organization in the cloud, discuss the information blueprint and conduct the map-n-go between as-is and the future state.

    - Organize the agenda: what are the organization's mission requirements?

    - Develop a method for determining ROI in the federal government, as this is often what brings the most value at the lowest or quantifying cost within an acceptable risk tolerance benefit, where mission effectiveness is the decision-making driver.

    - Pick the right people and partners: establish senior departmental or agency support for the effort; identify a senior level cloud champion within the organization; and, leverage industry expertise to complement internal base knowledge.

    - Manage the team & stakeholders: identify all stakeholders and communicate regularly to sustain engagement and support, and to influence cloud adoption across teams.

    - Report Progress: this drives accountability, and highlights the progress through milestones.

- **Assess the applications for suitability to the cloud**. This is a critical step, as not all applications should be moved to the cloud. Only those applications which will yield value from running on cloud infrastructure should be moved.

This step includes the collection of key application/infrastructure data, mapping them to business functions/processes, collecting functional/technical/financial data, identifying potential improvement options, looking at the IT organization model, and, reviewing current projects and the portfolio management methods/processes.

Mission/Business

- Mission Purpose/Impact
- Strategic Contribution
- Geographic regulatory requirements
- Workload variability
- Software licensing restrictions
- Software vendor support
- Service level requirements
- Security policies
- End User Experience expectations
- Application availability requirements
- Impact on mission
- Total Cost of Ownership
- Application end of life profile
- Availability of COTS/GOTS replacement
- Range in variability in usage

Technical

- Architecture
- Process Requirement
- Mission critical or non-mission critical/ supporting
- External dependencies
- Language of application
- Physical hardware dependencies
- Data encryption
- Operating system requirements
- Parallel processing
- Regulatory requirements
- Backup and recovery processes
- Number and complexity of interfaces

In general, there are two broad categories of application characteristics that should be looked at: An explanation of these characteristics can be found in **Appendix A - Application Suitability Characteristics**.

- **Identify the target platforms.** This step answers whether the application should be moved. The intent is to leverage cloud technology wisely by following these guidelines:

  - Determine the type of environment that is the best fit (public cloud, community cloud, private cloud, hybrid cloud, managed cloud services, traditional data center, hybrid deployment).

  - Identify the user experience requirements, including performance expectations and access requirements.

  - Make applications ready for the cloud by leveraging cloud native capabilities. In "lift and shift" cases, these steps can be quite minimal. In "born on the cloud" or new applications, cloud native capabilities can also be leveraged.

  - Consider typical first-choice workloads such as disaster recovery, virtual desktop, or new cloud-native applications. "Lift and shift" is also a typical first-choice, and can be a good first step in migrating a workload to become cloud-native.

  - Move common applications that are not core nor unique to the mission of the organization to the cloud.

  - Applications with seasonal or periodic surges in demand are ideal for the cloud.

  - New laws, policies, executive orders, and directives with specific deadlines can necessitate the use of cloud to meet tight timelines (e.g., Federal Aviation Administration (FAA) Drone Registry).

  - Don't underestimate security and privacy concerns. Recognize the need to protect the content and mitigate evolving security threats in the cloud.

  - Don't underestimate the time required to attain ATO status when migrating to the cloud.

  - Identify the level of visibility needed to make business and technical decisions.

  - Aligning cloud migrations with the normal release cycle of existing applications.

  This is where overlaps and gaps are identified, the application value is assessed, and the definition of the future state or To-Be architecture is created. From here the target approaches are developed and a high-level cost/benefit analysis is performed. A milestone review of the recommendations, opportunities for improvement and their alternative solution approaches is recommended. This will build consensus for the most viable opportunities.

- **Modernization of the applications and associated processes.** There are five strategy domains leveraged in modernizing the application. Each of these domains should be considered individually for each application:

- Re-Host
- Replace
- Integrate
- Re-Compile
- Re-Factor
- Re-Architect
- Retire

A definition of these transformation end states can be found in Appendix B – Transformation End States.

The evaluation of candidates for cloud should use one of the recognized industry Enterprise Architecture tools and techniques to inventory, rationalize, and plan for the cloud migration. The use of automated tools to capture the 'ground truth' of the application environment, including external dependencies, can be crucial to the success of the transformation.

- **Build the roadmap.** Prioritizing opportunities and recommendations complete the assessment process, developing the roadmap and approach, assessing risks, finalizing the business cases, putting the roadmap schedule together, along with the proposed governance structure and processes, and making the final presentation of recommendations to the approving authority.

  - Produce recommendations for Infrastructure-, Platform-, and Software-as-a-Service
  - Private, public, community or hybrid clouds
  - Business and IT benefits
  - Recommended target architecture
  - Cloud vendor diversity/redundancy
  - Application Service Tiers/Service Level Agreement
  - Automation of elasticity/manageability
  - Service brokering/back-out plan
  - Onboarding & continuous delivery
  - Business continuity and disaster recovery
  - Conditional access for span of control
  - Cloud vendor billing visibility/monitoring
  - End User experience analysis
  - Risk tolerance analysis
  - Security analysis
  - Chargeback and cost allocations
  - Staff Training on migration and service models

This involves taking the top candidates from the evaluation and performing an analysis that includes:

- **Concluding thoughts on a recommended process:**

  - Follow a defined, method-based process for determining if and how an application should be transformed to cloud.
  - Ensure that processes and organizational changes are enacted to support the transformed environment.
  - A clear understanding of what support models will be required and what services will still be needed in a post cloud scenario.
  - Avoid vendor lock-in and ensure you can continue to innovate and drive costs down with a cloud model.
  - Success breeds success:

- Use the federal CIO council to document, communicate, and promote successes.
- Recognize and reward desired behaviors.
- Look to leaders in cloud adoption for best practices (e.g., Estonia).

4. Accelerating cloud adoption in the federal government.

Cloud-based services offer federal agencies the potential to realize benefits in terms of modern infrastructure, security, cost savings, greater agility, faster time to market, and better end-user experiences. Agencies should aim to reap improved mission outcomes by leveraging these benefits and the innovations made possible through cloud-based services.

a. Evaluate the current accreditation process.

Engage the FedRAMP Program Management Office (PMO) to understand its roadmap for improving FedRAMP and how CSPs can engage, making the program more efficient both for government agencies and for vendors. Some potential areas for improvement include:

- **Support stakeholders and funding models.**
  - The federal government must more effectively fund the FedRAMP PMO so it can resource and maintain CSP provisional authority to operate (pATO). More broadly, the federal government should assess FedRAMP stakeholder responsibilities and determine whether they are sufficiently resourced to execute on those responsibilities or need additional funding and support, including from the National Institute of Standards and Technology (NIST).
  - Currently the FedRAMP PMO is capping pATOs due to lack of DHS and PMO funding. This approach slows down the level of innovation/technology that can be introduced to the government. New technologies could take over six months to get in the FedRAMP queue and another 6-12 months to become authorized.
- **Reduce redundancy for federal government agencies and vendors.**
  - The federal government must ensure that the implementation of FedRAMP is cost efficient for both agencies and vendors by reducing redundancy in assessments and authorizations.
  - Currently, many agencies and departments are repeating baseline security assessments done by others across the government. Instead, there should be ATO reciprocity. A FedRAMP Joint Authorization Board (JAB) ATO should be able to be leveraged by all agencies without them having to re-assess the cloud service. An agency or department ATO should be leveraged by all components within that agency or department (e.g., a cloud service that receives a FedRAMP Moderate ATO should be able to be leveraged by multiple components within the same agency or department that have workloads appropriate for a moderate environment).
  - The Department of Defense (DoD) requires additional controls on top of the FedRAMP authorization, (aka, FedRAMP+). For industry supporting both FedRAMP and FedRAMP+ authorizations, these efforts are duplicative and costly. It would be more efficient to streamline the documentation system and process across FedRAMP and FedRAMP+.

- Currently, FedRAMP leverages MAX.gov and FedRAMP+ leverages the enterprise Mission Assurance Support Service (eMASS), which results in documentation management in two different repositories and in multiple formats. Additionally, eMASS requires common access card (CAC) login, which can be a challenge for companies where the information security resources supporting the FedRAMP+ efforts are not the same resources tied to actual DoD contracts that make them eligible to receive CACs. The same applies for 3PAO resources. Better synergy between FedRAMP and FedRAMP+ is recommended to allow a more expeditious and less costly path to compliance/authorization.

- Many of the same products and capabilities require redundant security approvals for use, to include Evaluation Assurance Level, DoD Security Technical Implementation Guides (STIGs), and the National Information Assurance Partnership (NIAP) that overlap or are redundant with the FedRAMP controls.

- **Accelerate the accreditation process.**

  - Many technology companies, especially cutting-edge startups, simply avoid the public sector market. The process for acquiring IT products and services is keeping federal IT behind the innovative pace of the commercial market. FedRAMP, while well-intentioned, needs significant streamlining to permit both existing and new FedRAMP vendors to quickly bring new products to the federal marketplace. In the last 18 months, the FedRAMP program has demonstrated that it can be responsive to industry and improve; for instance, FedRAMP Accelerated has been a meaningful improvement, and the FedRAMP Tailored proposal also will help certain cloud services be adopted with greater agility. Additional efforts are required, however, to further streamline the process of bringing solutions to the federal government marketplace faster.

  - Consider a temporary authorization waiver for CSP's that have active FedRAMP authorizations to bring new products to the market early. Allowing the products to be used in the federal space for up to 1 year (for example), before moving into a FedRAMP ready status. This allows the vendor time to build a business case to support the cost of a new FedRAMP authorization and allows the government to leverage new, innovative technology faster, which could further evolve the technology towards government requirements since they are engaged early.

  - Allow Infrastructure Service providers to self-certify with a certified accreditor and make the documents available for audit by the FEDRAMP PMO.

  - Expand the scope of FedRAMP Tailored, scoping in not only low-impact software-as-a-service (SaaS) offerings that leverage FedRAMP-certified infrastructure, but also Low-confidentiality, Moderate-integrity, and Moderate-availability SaaS offerings that leverage FedRAMP-certified infrastructure. There is a very limited set of cross-agency use cases for a baseline that requires data or systems to be characterized as "Low" impact for confidentiality, integrity, and availability. Alternatively, public-facing websites, which are often characterized as Low-impact for confidentiality and Moderate-impact for integrity and availability, represent a major cross-agency use case; at a minimum, this use case should be immediately scoped in for the Tailored baseline.

  - Federal agencies should understand that they ultimately define mission/business risk and must have a formal risk management approach. This also suggests that there may not be a need to wait for pATOs and that a pATO may not be necessary with the right risk management approach.

  - The FedRAMP PMO should conduct a formal evaluation of the overlap between Common Criteria

certifications and FedRAMP. Although, the PMO cannot change Common Criteria, they could collaborate with the Committee on National Security (CNSS) responsible for Common Criteria, to communicate this policy around cloud computing and FedRAMP more effectively. ITAPS member companies do not believe that the Common Criteria certification for cloud is necessary and, that the FedRAMP certification serves well as the primary security assurance test necessary for cloud adoption. Continuing along the current path of requiring both will significantly undermine cloud adoption.

- Unify FedRAMP requirements for existing DoD and federal on-premise hosting services to standardize and make it simpler for applications and services to move across the on-premise and off-premise boundaries, with minimal policy friction.

- **Establish a high baseline watermark.**

  - While civilian agencies tend to have less sensitive missions and can therefore host their data in cloud offerings approved as FedRAMP Moderate and below, many DoD and intelligence agencies have data that is sensitive/classified and requires private clouds or clouds that meet the FedRAMP High/DoD Cloud Security Requirements Guide Level 6 or higher. Consistent with the recommendation above to reduce redundancy and promote reciprocity and efficiency, in the high environment context, the federal government should clarify requirements and, to the greatest extent practicable, have a consistent approach across agencies and departments.

b. Enablement/Transparency.

The resources and time it currently takes vendors to individually educate federal government agencies on new and innovative offerings causes government to lag on technology adoption and is inefficient for all parties. The FedRAMP PMO hosts cloud technical exchange meetings between government and industry to connect vendors and agencies, but it is unclear how well this is publicized or how successful these have been. More widely attended and robust exchanges would enable vendors to better understand agency needs and allow for a better alignment of vendor proposed offerings to actual federal agency requirements. These exchanges could also include opportunities for the vendors to describe how they use their own products, along with published customer case studies.

One area that would benefit from greater FedRAMP PMO involvement is contract language. Government agencies have a legitimate need to protect their own information and information systems, and to assure safeguarding of data that it shares with or obtains from its contractors. This is currently imposed through increasingly complex regulations and the imposition of specific, directive-type measures including, but not limited to FedRAMP, Security Requirement Guides (SRGs), and various Federal Acquisition Regulations (FAR) and Defense Federal Acquisition Regulations Supplement (DFARS) clauses. For industry, especially commercial cloud computing companies, this approach is anachronistic, unnecessary, and unduly burdensome. The investment by commercial companies in continuing security, and the tools and technology they employ, suggests that the specific rule-based regulatory approach constrains rather than improves realized security. Especially, as more government and private sector functionality moves to the cloud, the federal government should eliminate contract specific regulations and requirements that do not actually improve security measures that are entrusted to the provider, rather than the customer.

Over the last several years, the federal government has implemented several new FAR and DFARS clauses pertaining to network security and the acquisition of cloud services. In addition to creating new categories of data (Covered Defense Information), these clauses impose obligations to protect and report breaches involving such data that are different than those required by FedRAMP and SRGs. Such additional layering

creates a burden to affected defense contractors that is unnecessary, increases costs, and potentially hampers innovation and the ultimate security of the information the federal government seeks to protect.

With respect to cloud services with an ATO, federal government agencies should rely on FedRAMP and SRG. These two programs cover a very extensive list of controls including, but not limited to, physical security, personnel security (including background checks, training of data center personnel, and nondisclosure obligations of data center personnel), use of customer data, security incident notification, media storage, encryption, and audit of data. The federal government has been very involved in developing and vetting the rigorous controls required under these two programs. The government should not then layer additional, sometimes conflicting, controls into the contract itself.

Federal agencies should take advantage of the FedRAMP process and the benefits it offers in terms of efficiency and security. FedRAMP/SRGs requirements are constantly evolving to comply with evolving security standards and controls. Adding rigid contract clauses that lock in security controls directly into the contract itself creates a situation where the contract terms and conditions are likely to lag or conflict with FedRAMP/SRG. Such rigidity also prevents the CSP's from being able to provide, and the federal government the benefit of receiving, the most up-to-date and innovative security detection and prevention capabilities. Due to the rapidly evolving nature of technology, contracts need to be structured in a way that focuses on outcomes and stated goals rather than prescriptive methods and check-the-box controls, to ensure the federal government is receiving the most current functionality.

Thus, FAR and DFARS clauses to cloud services should be revised to either not apply to commercial items, which currently some clauses provide an exemption that is only for COTS, for which government community cloud services do not meet the definition; and/or apply solely to those cloud and other IT systems that do not have a FedRAMP, and the SRG ATO at the appropriate level.

The burdens and costs associated with additional layers of controls imposed by the FAR and DFARS is exacerbated by similar approaches taken by individual federal agencies. For example, DHS recently issued a contract deviation and proposed rule on safeguarding controlled unclassified information. This rule includes yet another set of security incident notification rules, procedures and other security controls that differ from and/or are in addition to those required by FedRAMP, the SRG and the FAR and DFARS.

Further, when responding to federal government solicitations for cloud services, it is common for FedRAMP-certified providers to encounter a host of agency-specific security clauses and requirements that, in some cases, may conflict with the FedRAMP standards, controls, and procedures that we must perform to maintain accreditation. In other cases, it is not reasonably possible for contractors to address exactly how FedRAMP security measures map to and comply with all the various federal agency-unique security mandates, owing to the sheer breadth of the gap analyses that would have to be undertaken by the contractor to do so. We have seen contract and subcontract awards to FedRAMP providers held up by weeks and months while Information Security and Contracts teams on both sides attempt to negotiate through such confusion.

These types of individual requirements are not only untenable from a commercial cloud service provider perspective, but they are also extremely costly in terms of compliance. In enacting agency-specific requirements, rather than relying on controls established specifically for the type of data being protected, the federal government is impeding its own efforts to increase security and reduce costs.

Another key enabler is to better prepare the applications themselves to be built or matured to a cloud ready state. Currently, application development standards do not mandate many of the architectures or standards that are required to support an application in a FedRAMP cloud. As a result, many of these

applications are tied to their current hosting facilities, requiring costly re-platforming and re-architecturing to migrate. There are several ways to enable these applications to be cloud ready:

- First, establish a standard set of application requirements that would enable currently maintained and future applications to better leverage cloud delivery models. These requirements would be embedded into future application acquisition and maintenance contracts.

- Second, increase the deployment of on-premise cloud to function as an incubator to allow developers to transition their applications to cloud delivery models and make a transition to a FedRAMP cloud facility low risk and low complexity.

c. Evolution.

Establish a cadence to evaluate policies (e.g. Cloud / Digital Strategy / Future Ready Workforce / Data Center Optimization) that are being focused on and have impact based on agencies adoption to determine if it conflicts with cloud adoption. Part of this cadence should evaluate the impact of agency enforcement of a broad policy, based on their interpretation of policies, in the areas of Mobile, Teleworking, and application programming interface (API) adoption.

Cloud/Infrastructure
Appendices

Appendix – A: Application Suitability Characteristics

Business characteristics:

Geographic or regulatory requirements – Is the application subject to regulatory requirements such as the Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), or other such statutes or regulations, or required to run on a government certified system image? Agencies should verify that their chosen cloud service provider is able to provide a solution that enables the agency to meet its regulatory requirements.

Workload variability – If the workload does not vary, does it make sense to run in the cloud?

Software licensing restrictions – Can you run that application in a highly virtualized environment and still conform to your licensing model with the software vendor – if your scope includes packaged applications?

Vendor support – Will the software vendor provide support for the applications in the new environment? Are they "certified" to run in the new environment on that specific operating system?

End User Experience – Performance and accessibility drives user adoption to cloud applications. These characteristics can also be considered security requirements. For example, end-users expect instantaneous performance and mobile access to the application (per today's internet trends). If the cloud application does not meet these expectations, end-users will most likely move the content elsewhere and the federal government could start to lose control of their own content.

Cloud Availability – The impact of downtime to the cloud application means that users cannot interact with the application hosted in the cloud. What is the application's risk to this occurring? Such as how do you mitigate risk for what you don't control? There are many components of cloud architecture such as DNS, application layer, network layer, etc., to consider.

Technical characteristics:

Is the application considered mission critical or non-mission critical/supporting? Context applications are applications that support the business, but don't bring down operations if they fail. Exchange, business intelligence reporting applications, marketing and sales tools can be core as applications that the business depends upon to carry out its critical operations.

Are there any external dependencies or physical hardware dependencies? Physical hardware dependencies include software license dongles or legacy gear like token ring network cards, graphics cards and the like.

What is the language of the applications? Older technologies are less likely be to be supported by sophisticated tools and cloud standards and programming styles. One consideration is the ability of the application, natively, or post-modernization to support parallel processing? Will the platform and infrastructure support this?

Appendix – B: Transformation End States

End-State Options

Re-Host: This is the most non-invasive approach and is for the most part a lift and shift. Migrating the application as-is over to the new infrastructure.

Replace: With some custom applications, it may not make sense to continue maintaining them. Alternative replacement strategies should be reviewed in the market and considered. For example – if this is a custom customer relationship management (CRM) application, it may make more sense to replace this with something like a SaaS CRM cloud offering. Such alternatives may provide more features and benefits at a more competitive price.

Integrate: The integration of off-premise cloud applications is frequently identified in analyst reports as a barrier to cloud adoption. For this reason, the approach may include the building of an enterprise integration platform enabled via an enterprise service bus, or it may require the wrapping of existing legacy applications to expose them as web based services. This domain could leverage service oriented architecture (SOA) and Integration Services.

Re-Compile: This lowest cost option allows for immediate recognition of the modernized platform. Agencies can recompile with the current compilers, using existing source code, and deploy applications taking advantage of postmodern mainframe hardware and software. The newest compiler releases implement the most efficient optimizations, speed applications by reducing batch windows and significantly reducing transaction response times. Applications can be prioritized for recompilation based upon the applications central processing unit (CPU) usage and required response time. There is no need to make changes to the source code to recognize the advantages.

Re-Factor: This option allows for short-term recognition of the modernized platform. Legacy applications, can be reviewed to identify inefficient code, poor coding practices or code that can be optimized to take advantage of the newest technologies in the compilers, operating system, and hardware. Code changes to the applications that take advantage of the platform improvements provide cost savings that can out-weigh the cost of modernization.

Re-Architect: This option is a long-term strategy to optimize applications and their use of the modernized platform. Legacy applications were written using the hardware and software available at the time of their creation. Taking full of advantage of the modernized hardware and software requires that some applications must be comprehensively restructured. Using modern coding practices, compilers and hardware are necessary to gain the full benefit of a modernized platform.

Retire: In the case where the application is no longer required or has its functionality duplicated by another application.

Cloud/Infrastructure
Additional Resources

Akamai

Best Practices from Your Cloud Co-pilot: Minimize Risk & Improve End-user Experiences
Akamai Public Sector customer case studies.

https://www.akamai.com/us/en/our-customers.jsp
filter on the Industry drop down and select Public Sector.

CSRA

CSRA' s Digital Platforms
https://www.csra.com/what-we-do/our-expertise/digital-platforms/

Cloud Adoption in the Federal Government
https://www.csra.com/media-room/presentation/presentation-cloud-adoption-federal-government/
https://www.csra.com/media-room/article/cloud-adoption-federal-government/

Cloud is the Foundation of IT Modernization
https://www.csra.com/media-room/article/cloud-foundation-it-modernization/

FedRAMP Goals Coincide with Increasing Demand for Cloud Services
https://www.csra.com/media-room/article/fedramp-goals-coincide-increasing-demand-cloud-services/

Top 5 Reasons Federal Agencies Are Moving to the Cloud
https://www.csra.com/media-room/article/top-5-reasons-federal-agencies-are-moving-cloud/

HPE

Right Mix: Transforming to a Hybrid IT Infrastructure:
https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-3270ENW.pdf

How to Transform to a Right Mix of Hybrid Infrastructure:
https://www.hpe.com/h20195/v2/GetDocument.aspx?docname=4AA6-6503ENW

Right Mix:
https://community.hpe.com/t5/Grounded-in-the-Cloud/The-Right-Mix-part-1-of-4-An-Impetus-for-Change/ba-p/6822249#.WXZB_-mQwcA

The Right Mix: An Impetus for Change (in 4 parts):
https://community.hpe.com/t5/Grounded-in-the-Cloud/Three-focus-areas-for-implementing-the-right-mix-of-hybrid-IT/ba-p/6895155#.WXZCK-mQwcA

Red Hat
IDC White Paper | The Business Value of Red Hat OpenShift

Empower Federal Government Employees - Microsoft

Optimize Federal Government Operations - Microsoft

Transform Federal Government Services - Microsoft

Government Connected Field Service Solutions - Microsoft

Cloud Migration - Microsoft

IT Alliance
for Public Sector
A Division of ITI

Cybersecurity
Topline Recommendations

1. **Establish governance & accountability as essential to achieving a more assured state.**
2. **Acquisition reform is critical to IT modernization and cybersecurity.**
3. **Leverage the successful model used to create the Cybersecurity Framework to further improve cybersecurity.**
4. **Close the federal government's cybersecurity skills gap.**
5. **Redefine the federal IT network architecture.**
6. **Devote resources to cybersecurity research and development.**
7. **Institute more robust information sharing mechanisms with the goal of automating the task.**

Cybersecurity
Detailed Recommendations

Executive Summary

The IT Alliance for Public Sector is pleased to present recommendations to modernize federal cybersecurity practices. With the interconnected and global nature of today's digital environment, strong cybersecurity must be a fundamental underpinning of any effort to transform federal IT systems and is essential to realizing the expected economic and efficiency benefits of modernization.

The diversity of recommendations contained within this section are a reflection that enhancing cybersecurity requires a comprehensive strategy that leverages people, processes, and technological innovations to actively prevent cyberattacks and holistically reduce enterprise cybersecurity risks. These recommendations outline actions that can be taken now to enhance the federal government's cybersecurity posture, such as requiring regular, automated, vulnerability scanning of all federal network environments, updating procurement guidance to reflect the speed of cyber threats and the rapid evolution of security technologies, and expanding existing programs to recruit and retain a strong cybersecurity workforce.

Importantly, this section also offers key themes and recommendations focused on taking advantage of new evolutions in technology and natively integrating strong security tools into IT deployments. To succeed in new shared service and cloud-based environments, it is critical for government to prioritize implementing security technologies that can work together in an automated, holistic way to actively prevent, not just detect, cyberattacks across the entire federal government's network infrastructure. To keep up with the pace of modern cyberattacks and reduce risk on an enterprise-wide basis, security tools must be capable of automatic reprogramming, based on new threat data, to deliver consistent security across the entirety of the network, including all cloud and endpoint environments.

Adopting IT systems with agile security technology that can protect digital infrastructure at scale is vital, because the federal government simply cannot continue to divert people and resources towards manually maintaining antiquated systems or manually correlating cybersecurity incidents. Indeed, new, and emerging technology trends — including the increased adoption of cloud, shared services, and virtualized networks — also present critical opportunities to fundamentally simplify and automate how the government consumes and delivers cybersecurity tools to reduce enterprise risks. The emergence of shared, cloud-based marketplaces where security capabilities can be seamlessly tested and deployed as application-based software — an alternative to time-intensive hardware procurement, evaluation, installation, and system integration cycles — represents the agility to which the government must evolve.

Similarly, there must be a focus on making information sharing as automated and actionable as possible. This means collapsing the amount of time between when an organization receives a technical indicator and the implementation of a preventive control to enforce security based on that threat information. Further, government and industry must mature information sharing processes to focus on sharing more than isolated indicators of compromise and incentivize the sharing of correlated threat indicators that link together multiple steps of the adversary's playbook, aligned to each phase of the attack lifecycle—including reconnaissance, weaponization, delivery, exploitation, and command and control.

Finally, the recommendations, in no particular order of prioritization, offer opportunities for continued public-private partnership. An integrated approach between government and industry can enhance everyone's collective cybersecurity by fostering a shared understanding of the cyberthreat landscape,

facilitating a more robust and systemic public-private threat information sharing environment, jointly developing effective policies, and partnering to raise education, awareness, and overall levels of cybersecurity skills. Private sector innovation will be critical in replacing legacy federal IT systems with next-generation solutions that both spur greater efficiencies and strengthen the security of the nation's digital infrastructure.

1. Establish governance & accountability as essential to achieving a more assured state.

Governance and accountability are critical for the successful improvement of cybersecurity and need to be employed in conjunction with the overall federal IT modernization efforts. Modernization is not just updating systems and infrastructure. Modernization includes improving the approach to operations, to include continuous development and enhancement: a DevSecOps approach. Doing so will enable far more agility for federal IT to adopt current recommended technologies, like provisioned/shared infrastructure, and more quickly integrate emerging technologies into agency production environments. Without this flexibility, the federal government will not be able to adapt to the rapidly evolving, dynamic landscape. Applying current and previously recommended cybersecurity policies and mandates as part of the overall federal IT modernization would be more cost-effective. Additionally, the federal government should work with private sector industry leaders and actively engage with industry working groups as part of the continual process of development necessary to achieve IT modernization.

Two critical factors necessary for the improvement and success of cybersecurity have been made official policy by Executive Order 13800[1] : (1) risk management, and (2) accountability. Risk management at the executive level is a key part of addressing cybersecurity. This includes ongoing risk assessment and risk awareness education for all federal employees. Continual risk assessment and educational awareness is required to match a constantly changing threat landscape. Accountability must be clearly defined and enforced when there is failure to meet compliance. None of the following recommendations - no laws, no mandates, no required standards, nor policies - will be effective without accountability.

We offer these key points to best establish governance and accountability in cybersecurity modernization within the federal government:

a. Support key cybersecurity legislation.

Getting consensus on new legislation is difficult and time consuming, however, there are currently two bipartisan bills which would allocate funding toward improving cybersecurity that we recommend the Administration support:

- Modernizing Government Technology Act of 2017[2] , which establishes a Technology Modernization Fund to reduce budget restrictions for modernization and cybersecurity efforts
- Developing Innovation and Growing the Internet of Things (DIGIT) Act [3], which directs the Secretary of Commerce to convene a working group of federal stakeholders to advise Congress on how to plan and prepare for the Internet of Things (IoT).

b. Work with international organizations that develop standards for privacy and cybersecurity.

The federal government should work with international organizations that develop standards for privacy

1 Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, Section 1, paragraph a

2 https://www.congress.gov/bill/115th-congress/house-bill/2227

3 http://www.fischer.senate.gov/public/_cache/files/03de7771-088b-45ac-8552-f82ddc0aa480/digit-2016---final-bill-for-filing.pdf

and cybersecurity to ensure that U.S. policies and regulations do not disrupt cross-border commerce and internet interoperability.

c. Require full accounting and continuous monitoring of all IT assets.

Continuous monitoring of IT assets is essential at the federal scale from a governance perspective. It is critical that assets are inventoried - including third-party provisioned virtual assets - so that redundancies, inefficiencies, and vulnerabilities can be promptly identified and remediated.

d. Require regular and automated vulnerability scanning of all federal network environments.

Compliance cannot be assessed without a full accounting of all assets within the enterprise. Federal IT needs to follow the private sector's example of vulnerability assessment with regular and automated vulnerability scanning. This has been a successful and standard practice across the private sector.

e. Work with industry leaders to develop solutions that lower cybersecurity risk.

The federal government needs to actively collaborate with the private sector and industry by participating in working groups. This would enable direct government input in establishing standards and policies, development of solutions and policies for reducing cybersecurity risk, and modernization of national IT infrastructure (public and private). It is critical that we empower federal IT to be as adaptable as the private sector, to match what is now an ever-changing threat landscape.

f. Mandate adoption of a DevOps security, or DevSecOps, approach for continual development and modernization.

It is critical that the federal approach to operations and maintenance (O&M) is modernized along with the federal IT infrastructure. The government needs to be adaptable and flexible to quickly adopt new risk-mitigating technologies and confront ever-changing threats. Agencies need to be required to adopt a DevSecOps approach to O&M so that development, testing, and enhancements are executed in parallel with operations.

Modernizing the approach to O&M to a DevSecOps approach enables this flexibility. When applied to a current system, a DevSecOps approach will be able to modernize the system and continue ongoing enhancements with minimal investment into new infrastructure. While a DevSecOps approach may increase lifespan of some current systems, there are still going to be systems which will require infrastructure modernization or full replacement. Specifically, those aging or legacy systems where development and enhancement are no longer cost effective or even possible.

g. Reinforce the preference for commercial items over do-it-yourself government-unique development.

To increase the pace of federal IT modernization, procurement policies need to discourage "do it yourself" development of government-off-the-shelf (GOTS) solutions in favor of more cost-effective commercial items and commercial-off-the-shelf (COTS) solutions. GOTS solutions are costly to develop and expensive to maintain over time. COTS solutions, meeting the same functionality and security requirements, require no development cost, are less expensive to maintain, and will be more flexible for continual enhancements within a DevSecOps environment.

h. Institutionalize "security by design" for federal IT modernization and development.

Included within a DevSecOps approach needs to be a "security by design" process, such as a System-Theoretic Process Analysis for Security (STPA-Sec) for all future development. Security is not an add-on, it needs to be a fundamental part of all IT design, from start to finish. Furthermore, it should prioritize procurement from vendors or manufacturers that adopt secure engineering standards and certifications for all hardware and devices, software, and solutions.

i. Attach dedicated cybersecurity funding to all IT modernization acquisitions.

To ensure funding is properly applied to cybersecurity improvement, we recommend that budget allocations for any IT acquisitions include dollars specifically dedicated for cybersecurity. These funds would be applied to securing all new acquisitions of hardware and software, as well as secure integration of provisioned/shared services platforms. Further, these funds should not be permitted to be used for staffing of employees or contractors.

j. Mandate end-to-end encryption on all federal networks when appropriate and applicable and establish a public-private partnership for implementing strong authentication while protecting privacy.

The government should mandate encryption for government communications when appropriate and applicable, working with the private sector to help in that development. Furthermore, improvements in identity lifecycle management, requiring multi-factor authentication and elimination of password-based authentication entirely are essential, as are strict role and policy-based access control for the protection of federal data.

k. Develop a framework for determining IoT security policies that addresses IoT device functionality.

It is critically important that the government work with industry leaders and working groups as IoT policy is created. It is equally important to consider the diversity of IoT devices and the environment in which the devices will be used as new/revised standards and policies are developed and to review the approaches used for current standards. How an IoT device needs to be secured is a direct result of its function and a determination of "fitness for purpose" or "fitness for use" in the environment in which the devices will be used; therefore, a single standard or policy is insufficient to address all devices. A single universal standard/policy other than National Institute of Standards and Technology (NIST) Special Publication 800-161 would likely impede integration of IoT, or worse, create an unmanageable set of exceptions at the agency and organizational level. Using an approach of categorizing functionality and communication requirements will result in a set of appropriate security policies. Until formal IoT security policies have been created, agencies should follow industry's general best practices, including changing factory-default credentials of any internet-connected device, disabling unnecessary communication services like SSH (Secure Shell), and applying inbound/outbound firewall rules to prevent unauthorized external connections.

l. Enforce Federal Risk and Authorization Management Program (FedRAMP) compliance for provisioned cloud services, and increase funding to FedRAMP Program Management Office (PMO).

FedRAMP has defined baseline security controls that apply in the federal public sector for cloud service providers (CSPs). It is important that all agencies continue to be required to use CSPs with FedRAMP Authorizations to Operate (ATOs). Agencies must, however, recognize that FedRAMP security controls are baseline standards. Agencies are responsible for ensuring that CSPs' environments meet any additional security control requirements. The FedRAMP PMO needs to be properly funded for the program to be successful in issuing ATOs under the principal of "do once, use many." Finally, the FedRAMP PMO has made improvements in the time needed to award ATOs, but without proper funding, the FedRAMP PMO

will have limited resources to make the program more efficient and limit the number of Joint Advisory Board ATOs which could be awarded.

m. Address shortages in agency cybersecurity skills.

The Government needs to address the shortage of cybersecurity expertise within the federal workforce. To address recruitment, we recommend the continuation and expansion of the CyberCorps, a scholarship for service (SFS) program [4]. To increase skills among current federal workers, we recommend expanding the Department of Defense's (DoD) Information Technology Exchange Program (ITEP)[5] to other agencies.

n. Continue to encourage agencies to create Chief Risk Officer (CRO) positions.

More agencies should establish a Chief Risk Officer (CRO), tasked with assessing risk, determining what risks require mitigation, and which risks are acceptable. A CRO can educate agency personnel about how risk mitigation is everyone's responsibility. Since threats like malware are often inadvertently introduced by users within the network, every federal employee needs to be a part of risk mitigation efforts. As is common practice in the private sector, every federal employee should be required to complete cybersecurity and risk awareness training when initially hired and at least once per year during their employment. Any improvement in cybersecurity cannot be achieved without accountability.

o. Accountability requires a named, responsible owner and reporting transparency.

Accountability is best achieved through designating a named, responsible owner and reporting transparency. This means that for every task, development effort, and ongoing O&M, there needs to be a named federal employee who is accountable for ensuring that all applicable security standards, mandates, and policies are continuously met. It is important that responsibility is placed on a federal employee, not a contractor, and not a third-party provisioned services provider. It is the federal government/agency's responsibility that contractors and third party-provisioned services providers are within federal/agency compliance; therefore, a named federal employee needs to be responsible.

p. Expand current Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) dashboards to include reports for modernization and security compliance.

Accountability starts with identifying progress toward compliance and where compliance has not been met. OMB has the federal IT Dashboard[6] , and NIST has dashboard reports for Internet Protocol v6 and Domain Name System Security Extensions (DNSSEC)[7] compliance . Both dashboards should be expanded to include progress toward federal IT modernization goals and compliance with cybersecurity mandates and standards. Dashboards should be leveraged not just for reporting visibility, but also for underlying automation and related remediation workflows. OMB and the Government Accountability Office (GAO) must follow through on enforcement of current and future standards, policies, and regulations. Since lack of funding is commonly attributed to a failure to meet compliance requirements, we should look at ways to encourage both IT modernization and compliance with funding incentives.

q. Reward agencies that have implemented cybersecurity controls and standards with a preferential weighting system for strategic plan and budget submissions (i.e. OMB 300s).

4 Provides scholarships and internships in exchange for students working 2-3 years in federal government service after graduation. https://www.sfs.opm.gov

5 IT professional exchange between the DoD and private sector. http://dodcio.defense.gov/In-the-News/Information-Technology-Exchange-Program/

6 https://itdashboard.gov

7 https://fedv6-deployment.antd.nist.gov/CGI-bin/generate-gov

One way to incentivize agencies would be to reward those that have implemented cybersecurity controls and standards with a preferential weighting system for strategic plan and budget submissions (i.e., OMB 300s). Agencies would have an opportunity to have future planning and budget requests prioritized for funding by investing now to meet security compliance. According to the May 2016 on Legacy Systems, [8] the O&M of legacy systems[9] is consuming a large portion of federal IT budgets. Specifically, the GAO states that 75% of all federal IT investment has been spent on O&M. Because of the high cost of O&M, federal investment in IT development, modernization, and enhancement activities, has declined by $7.3 billion since 2010.

r. Reduce budget allocations for the operation and maintenance (O&M) of legacy systems.

A possible solution to the practice of allocating budget to O&M of legacy systems may be to stop funding to maintain the aging systems and instead begin funding the modernization of systems. Modernization here does not just refer to modernization of the system and infrastructure, but also the modernized approach to O&M recommended above in sub. (g) that includes development and enhancement with O&M. For this recommendation, aging or legacy systems specifically refers to IT systems that are obsolete to the point where further development and improvement would be too expensive or simply not possible.

Finally, while funding incentives may be effective in encouraging modernization and cybersecurity enhancement, simply encouraging such efforts may not be enough. Accountability needs to be enforced. One way to enforce accountability would be to impact budgetary allocation, perhaps withholding or delaying funding until compliance has been met.

s. Increase Focus on Protecting Data from Unintended and Unauthorized Disclosures.

ITAPS recommends placing additional emphasis on securing the government's data itself against data loss, accidental forwarding, phishing attacks, etc. Focusing on the users and the devices are necessary and foundational components of an enterprise security model, but an increased focus on protecting sensitive data from unintended and unauthorized disclosure is also ultimately required to prevent data loss and breaches.

2. Acquisition reform is critical to IT modernization and cybersecurity.

Cybersecurity threats to the U.S. government are outpacing the federal acquisition process, which are creating vulnerabilities. ITAPS has recommended to both the Administration and the Congress that the path to achieving the goal of increased cybersecurity protections for government networks is through IT modernization. Acquisition reform is essential to the ability to modernize IT in the government and attain greater cybersecurity assurance. In other words, we cannot have cybersecurity without IT modernization, and we cannot acquire the goods and services we need for either of these goals without changing the way we acquire IT. To make progress on this goal, ITAPS makes the following recommendations:

a. Encourage full utilization of and update government procurement rules to enable agencies to compete with hackers.

Current procurement rules preclude agencies and departments from effectively countering the hacker threat in a timely manner. It is critical that DHS and other federal agencies have access to the same tools and capabilities that are available to the private sector and this can only be achieved by encouraging full

8 Government Accountability Office Report on Legacy Systems, May 2016

9 GOA defines "Legacy Systems" as IT systems using obsolete languages or hardware as well as steady state systems which are operated and maintained without further development. The definition within the Modernize Government Information Technology Act states, "the term 'legacy information technology system' means an outdated or obsolete system of information technology."

use of current procurement rules, and by looking for opportunities to update those rules where necessary. Currently, there are numerous ways federal agencies can acquire products and services rapidly including:

- The Federal Acquisition Streamlining Act of 1994 (FASA), mandates use of simplified acquisition procedures, to the maximum extent practicable, for products and services not exceeding the simplified acquisition threshold.
- The Competition in Contracting Act of 1984 (CICA) allows federal agencies to accelerate the acquisition process where there is an urgent need, or where requiring full and open competition could compromise national security.
- The U.S. General Services Administration (GSA) maintains a supply schedule for information technology (Schedule 70), where pre-vetted vendors with pre-negotiated terms offer cybersecurity products.
- Congress authorized the Continuous Diagnostics and Mitigation (CDM) program at DHS, which allows federal agencies to expand their CDM capabilities through the acquisition of commercial tools with robust terms for technical modernization as threats change.
- Congress has granted 11 agencies (including DHS) the ability to enter into "other transaction agreements", which generally do not follow a standard format or include terms and conditions normally found in contracts or grants, to meet project requirements and mission needs.

In addition to encouraging federal agencies to fully use these authorizations, procurement policy and acquisition procedures must evolve more rapidly to match the pace of information technology development and adoption by hackers, criminals, and other bad actors. Currently, little guidance exists in the Federal Acquisition Regulations (FAR) regarding the procurement of cybersecurity technology; rather, the FAR leaves cybersecurity implementation to each individual federal agency. Agency officials and contractors must consult a myriad of different regulations to ascertain if and how to implement acquisition regulations regarding cybersecurity. This diversity in agency cybersecurity regulations undermines security requirements and policies governing federal procurements. Harmonizing cybersecurity acquisition requirements would allow agencies to: (1) target security to highest-priority data and threats; (2) obtain greater value through reduced compliance obligations and increased contractor focus on high-value cybersecurity investments; and (3) enhance agency cybersecurity through the adoption of best practices, tempered through public review and comment.

- The Director of OMB, in consultation with the Administrator of the Office of Federal Procurement Policy, as key national priorities should: (1) provide clear direction to security and acquisition officials across government that cybersecurity solutions should be acquired and implemented rapidly; (2) advise and train security and acquisition officials on existing authorities available for the rapid acquisition and implementation of cybersecurity solutions; and, (3) expeditiously identify impediments to the rapid acquisition and implementation of cybersecurity solutions that need to be addressed by Congress and report those impediments to the relevant committees of jurisdiction for redress.
- The Administration should assess disparate cybersecurity acquisition requirements across agencies and make recommendations to harmonize requirements to the extent possible.

b. Adopt agile practices.

ITAPS believes that federal agencies should be using agile management and development processes across the enterprise to aid in IT modernization and procurement. Agile is not simply a software development methodology, but rather an overarching business model. Government agencies should be utilizing agile principles at all levels of the organization, including procurement, recruiting, reporting, and in systems development and modernization.

Agile development methods can help prevent waste from occurring in federal IT, such as building duplicative or unnecessary software modules. Currently, federal agencies have difficulty gaining central visibility into projects as they use disparate systems and inefficient processes to track and report on progress. Management decisions are often misaligned with agency missions and projects are often delayed.

Leading private sector entities have adopted agile practices, which allow for iterative development and feedback loops, resulting in stronger outcomes. ITAPS believes federal agencies should adopt these same methodologies to provide more efficient, more secure, and less costly IT services on behalf of taxpayers.

- The Administration should leverage agile and transparent acquisition approaches, as appropriate, that provide security officials with the flexibility to procure the technologies they need expeditiously. For example, the government should consider the use of accelerated and national security contracting authorities once identifying an appropriate technology that satisfies a defined, urgent cybersecurity requirement.

c. Protect federal networks through accelerated adoption of Einstein and Continuous Diagnostics and Mitigation (CDM).

A significant number of recent federal breaches resulted from compromised identities, including those of privileged users. The EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs, when fully deployed[10] , will help government agencies acquire vital security capabilities and tools to better secure government networks and systems. The EINSTEIN program is designed to detect and block cybersecurity attacks from compromising federal agencies, and to use threat information detected in one agency to help other government agencies and the private sector to protect themselves. The CDM program provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Our primary recommendations are the need for deployment, procurement flexibility and improvements in the workforce development process. Currently, federal agencies recognize the value in deploying CDM solutions. They recognize, however, that these deployments could be paid for by DHS in the following appropriations cycle. Agility and speed are very important in this context. Ultimately, a plan and a strategy are inconsequential without deployment. There is a distinct risk of a moral hazard where agencies will fail to prioritize cybersecurity funding in the short term, thinking these costs will be eventually covered by DHS, leaving them susceptible to risk of a significant breach in the interim. Further, DHS partners with the GSA on the development of contract vehicles for these programs, and there is a need for more trained contracting personnel to accelerate deployment of these new vehicles.

Most departments and agencies have already deployed a variety of authentication and authorization solutions as part of both their internal and citizen facing applications. ITAPS recommends that any government-wide solution add value and not create disruption and unintended expense by replacing the existing work that has been done. The applications that have been built and secured with these existing Federated Identity, Credential, and Access Management (FICAM) solutions are servicing millions of people today. Agencies should be encouraged and funded to do what is best for meeting their mission and business requirements, like leveraging Application Programming Interfaces to further extend their baseline solutions and adding additional safeguards, like privileged account and shared account management. Any

10 As evidenced by GAO-16-294, DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System, thoughtful deployment must consider compatibility with newer/ modern technology adoption so agencies can reflect a holistic security risk posture while aligning with the Administration's IT modernization goals.

new policies coming out of this program should consider and augment the investments and the services already being provided, not direct the investments to new platforms, thus distracting agencies from the ancillary opportunities.

In the wake of the OPM breach announcement in 2015, where tens of millions of government employees' records were stolen, government officials worked tirelessly to improve systems. These are committed individuals, and the sense of urgency following the breach resulted in quick and decisive action to resolve significant challenges that became immediately apparent. The long-term success in implementing those decisions, however, may be hamstrung by backlogs in the procurement process. Reacting to specific events to shore up defenses is different than proactive planning. As we look forward, we believe there is opportunity for DHS and its partner agencies to leverage the lessons learned in the cybersecurity sprint conducted in the wake of the OPM breach to apply them proactively to enhance overall cybersecurity posture across the federal government.

3. Leverage the successful model used to create the Cybersecurity Framework to further improve cybersecurity.

a. The NIST Cybersecurity Framework is a highly successful model.

The Framework for Improving Critical Infrastructure Cybersecurity, known as the NIST Cybersecurity Framework, is widely acknowledged as a highly successful model for a public-private partnership, and should be emulated for future partnerships to address the challenges of IT modernization. OMB is already working to encourage federal agencies to adopt the Framework. The Administration's Cybersecurity Executive Order 13800 mandates government agencies to deploy the Framework, and the private sector is already rapidly adopting it. Here's why:

- The Framework is built around the concept of risk-management based approach which is a superior means for addressing cybersecurity.
- The process was open.
- NIST listened first.
- All participants came prepared.
- NIST engaged all stakeholders.
- The Framework is voluntary.
- Framework updates reflect emerging best practices.

b. There is a real need for protections.

Public-private partnerships (PPPs) created around a topic or issue that is real to both the public and the private sectors have a much better chance of getting the exposure and participation needed to achieve the goal of the partnership. In the case of the Cybersecurity Framework, it was obvious to both groups that the need for a risk management based solution existed. For too long, regulatory compliance had forced industry to spend valuable security dollars to prove something to regulators instead of using those resources to help protect enterprises. The cost of compliance was impacting our ability to secure ourselves.

c. The process was open.

From the very beginning, NIST made it clear the process for developing the Framework would be open and transparent. In the initial meeting, NIST staff described what would be occurring from the Request for Information-submitted comments being made public on a NIST project website to the anticipated

workshop process and general timeline for various milestones. Along the way, NIST staff were quick to ensure that industry participants understood what was happening so there would be no surprises. This created a growing sense of trust as the effort evolved, making the Framework development process more effective throughout.

d. NIST listened first.

One of the more interesting and effective parts of the development was the way NIST staff listened to the workshop participants. There were active discussions that were highly informative from members of various sectors and industries. Dr. Gallagher, NIST's Director at the time, stated quite clearly this was not NIST's framework; this was the community's framework. Having the public side of a public-private partnership listen, instead of dictate, allowed private sector participants to voice their opinions in a much more open and direct way. This, too, built trust as the effort went along.

e. All participants came prepared.

Each of the workshops was very well organized and the topics, panels, questions, and outcomes were well thought-out before each workshop began. This gave participants – both in the public and private sectors - reassurance that their time was being well spent. Open forums with no direction or planning do not give those involved much confidence the effort will succeed. Being prepared also meant participants needed to do their homework, as well. While not always the case, as the workshops advanced, they did so.

f. NIST engaged all stakeholders.

One of the things NIST did to ensure success in crafting the Framework, was to get outside of the Beltway and hold workshops in different locations around the country so the local owner/operators of the critical infrastructure could have their voices heard, ensuring there was a diverse group at each of the workshops and all could participate. The processes used during the workshops encouraged all in the room to contribute - and they did. It was a highly interactive, collaborative environment where real dialogue occurred and produced positive results.

g. The Framework is voluntary.

The fact that NIST is a non-regulatory body also bolstered its credibility and helped shape the private sector's attitude towards participating and contributing. This was a topic area that had a lot of people concerned initially, but as the effort progressed, the private sector participants relaxed and believed in the process. NIST also made it clear in each workshop that they were requiring a non-attribution from all regulators in the room. Each agreed to the rules, making it much more comfortable for real, open, and honest dialog to occur.

While others have tried to copy NIST's success, often they have left out one or more of the characteristics that made the Cybersecurity Framework effort most successful. Both the public and the private sector participants must buy in. To do so requires trust in the process, the effort, and the vision for the outcome to be successful.

h. Framework updates reflect emerging best practices.

Recently, NIST released a draft version 1.1 of the NIST Cybersecurity Framework for stakeholder review and comment. Draft updates include sections on supply chain risk management, identity management and access control, and metrics and measurements, among other updates. In many cases, these changes

reflect the evolving nature of cybersecurity threats and responses. NIST is continuing its effective process of engaging stakeholders and soliciting input on proposed and potential inclusions, which is crucial. This ensures that any final inclusions reflect current industry best practices and can enable stronger cybersecurity.

4. Close the federal government's cybersecurity skills gap.

In 2016, the Center for Strategic and International Studies (CSIS) undertook a study titled "Hacking the Skills Shortage," which was based on a global survey of IT professionals. Some of the findings about the cybersecurity talent gap include:

- 82 percent of those surveyed reported a lack of cybersecurity skills within their organization.
- 71 percent agreed that the talent shortfall makes organizations more vulnerable to attackers, and 25 percent say that lack of sufficient cybersecurity staff has contributed to data loss or theft and reputational damage.
- The most desirable skills cited in all eight countries surveyed were intrusion detection, secure software development, and attack mitigation.
- 76 percent of respondents say their governments are not investing enough in programs to help cultivate cybersecurity talent and believe the laws and regulations for cybersecurity in their country are inadequate.

Since that 2016 study, the numbers haven't improved. According to the most recent Global Information Security Workforce Study, the cybersecurity workforce shortage is projected to reach 1.8 million by 2022. The number of women in the field has not increased, coming in at only 11% globally, according to a Women in Cybersecurity report by the Executive Women's Forum and (ISC)2. In North America, women constitute only 14 percent of the information security workforce. The numbers are even worse for African Americans, who comprise only three percent of information security analysts in the U.S., according to the Bureau of Labor Statistics figures cited in an article in Forbes. Compare these numbers to predicted spending on cybersecurity: Cyber economy research firm Cybersecurity Ventures has predicted that global spending on cybersecurity products and services will surpass $1 trillion cumulatively between 2017 and 2021 and that annual cybercrime costs will reach $6 trillion in 2021. Both figures indicate the serious need for more trained professionals.

The cybersecurity skills shortage is particularly acute in the federal government. Tony Scott, the federal government's former Chief Information Officer, said in a GovLoop article, "There are an estimated 10,000 openings in the federal government for cybersecurity professionals that we would love to fill, but there's just not the talent available." Given the vital role such government agencies as DoD, DHS and the intelligence agencies play in protecting the United States, this skills gap is disquieting and merits particular attention from policymakers.

One strategy for addressing the cybersecurity skills deficit is to automate processes through machine learning and artificial intelligence. Legacy IT systems, however, like many of those in the federal government, lack the ability to take advantage of the most contemporary security architectures and development techniques. While it is possible to isolate or wrap security around a legacy system, the approach is far inferior to a well-designed, secure implementation designed for the security challenges of 2017 and beyond.

This speaks to the need for investments in IT modernization and modern cybersecurity solutions, which the president's executive order addresses. We support these much-needed policy changes. Even after legacy IT is retired, replaced, and modernized with current generation cybersecurity capabilities, we still have the

need many more skilled cybersecurity professionals. We offer the following recommendations:

a. Expand the current CyberCorps Program.

The CyberCorps Scholarship for Service (SFS) program[11] is designed to increase and strengthen the cadre of federal information assurance specialists that protect government systems and networks. The program is structured as such: The National Science Foundation (NSF) provides grants to about 70 institutions across the country to offer scholarships to 10-12 full-time students each. Students get free tuition for up to two years, in addition to annual stipends of $22,500 for undergraduates and $34,000 for graduate students. They also get allowances for health insurance, textbooks, and professional development. Some universities also partner with DHS on these programs.

Students generally must be juniors or seniors and must qualify for the program by attaining a specific GPA, usually at least a 3.0 or higher. Upon completing their coursework and a required internship, students earn a degree, then go to work as security experts in a government agency for at least the amount of time they have been supported by the program. After that, they can apply for jobs in the public or private sector.

The CyberCorps SFS program should receive additional funding to expand to more institutions and reach more students within each of those schools. To date, the federal government has made a solid commitment to supporting the SFS program, spending $45 million in 2015, $50 million in 2016, and the most recent Administration's budget requested $70 million. As a baseline, an investment of $40 million pays for roughly 1,500+ students to complete the scholarship program. Given the size and scale of the cybersecurity skills deficit, policymakers should significantly increase the size of the program, possibly something in the range of $180 million. At this level of funding, the program could support roughly 6,400 scholarships. Such a level of investment would make a dent in the federal cybersecurity skills deficit, estimated to be in the range of 10,000 workers per year. At the same time, this level of investment could help create a new generation of federal cybersecurity professionals that can serve as positive role models for a countless number of middle and high school students across the country to consider the benefits of a cybersecurity career and federal service.

Indeed, this positive feedback loop of the SFS program might well be its biggest long-term contribution. We also recommend that the program include a "give-back" component. The students who enter this program are compensated well; they receive paid internships during their course of study, and they are in line for federal jobs when they graduate. Yes, they are required to work for the federal government for a time equivalent to what they spent in the program, but unlike many other graduates, they have a job in their field where they are enhancing their resumes and skill sets for the future.

We would also suggest that the program adopt a requirement for graduates to give back by becoming ambassadors in the community for the program and for solving the cybersecurity talent shortage. We would not suggest prescribing the specific activity or role; rather, the graduates could use their own creativity to propose how they plan to give back. The CyberCorps SFS program should suggest some possibilities, including volunteering in middle and high schools to teach cybersecurity skills on a regular basis, acting as mentors to students, and taking students under their wing during internships the program might establish with the federal government.

b. Create a Community College Program.

While the CyberCorps program serves college juniors and seniors who are already well along the learning path, another program, or an expansion of the SFS program, should seek to attract high school graduates

11 Provides scholarships and internships in exchange for students working 2-3 years in federal government service after graduation. https://www.sfs.opm.gov

who don't yet have specific career aspirations. Private companies could partner with community colleges in their locale to establish a course of study focusing on cybersecurity.

The federal government could fund all or part of the tuition remission for students. Interested students would be taught both by college faculty and private sector practitioners. For example, an IT company could offer several faculty members/guest lecturers who would participate during a semester. Students would receive free tuition – paid by a federal program, perhaps with private sector contributions – but they would not receive a stipend for living arrangements, as 4-year college students do in the CyberCorps program. Students would receive a two-year certificate in cybersecurity that would be transferrable to a four-year school. Like the CyberCorps program, graduates would spend the same amount of time as their scholarship period working in a guaranteed government job.

Community colleges tend to attract a variety of students, including recent high school graduates, but also returning veterans and other adult students who might have pursued other careers or might even be working full- or part-time. The community college option could also further ethnic and racial diversity in a cybersecurity program, which is something that is badly needed. This diversity would be a plus rather than a minus for the cybersecurity profession, as the field requires a diverse set of skills and individuals. Not all of these skills are strictly technical, and for those that are technical, not all require high levels of formal education. You don't need a Ph.D. – or even a bachelor's degree – to work in cybersecurity. For instance, a four-year degree is not necessarily required to work in a security operations center (SOC). A strong security operation requires different levels of skills, and having a flexible scholarship program at a community college could benefit a wide variety of applicants, while providing the profession with other types of necessary skills. A program like this has the benefit of bringing in private sector experts, interesting younger students who have not yet made a commitment, interesting veterans, attracting a diverse range of students, and probably costing the government less – once the start-up costs were accounted for. Such a program should not substitute, but rather complement, the existing, highly valued CyberCorps SFS program.

c. Train existing government employees and deepen skills within the workforce.

The Government needs to address the shortage of cybersecurity expertise within the federal workforce. To address recruitment of new hires, we recommend the continuation and expansion of the CyberCorps Scholarship for Service (SFS) program. To increase skills among current federal workers, we recommend expanding the DoD's Information Technology Exchange Program (ITEP[12]) program to other agencies across the federal government and substantially increasing the level of agency commitment and participation.

A CRO (suggested elsewhere in this workstream) can educate an agency to the fact that risk mitigation is everyone's responsibility. Since threats like malware are often inadvertently introduced by users within the network, every federal employee needs to participate in risk mitigation efforts. As is common practice in the private sector, every federal employee must be required to complete cybersecurity and risk awareness training when initially hired and at least once per year during their employment.

5. Redefine the federal IT network architecture.

The modern and secure network architecture recognizes two essential tenets: the reality of the redefined perimeter, and the importance of comprehensive visibility through the environment.

The first step in ensuring the security of government networks needs to be the inclusion of security into the overall design of the network architecture. With federal agencies increasingly moving toward

12 IT professional exchange between the DoD and private sector. http://dodcio.defense.gov/In-the-News/Information-Technology-Exchange-Program/

provisioned cloud services, it is critical to define exactly what the network is - both physically and virtually - to determine the overall architecture and security requirements. It is just as important to define which systems will operate within the network, and what are the communication and security requirements of those systems and associated data sets. This is especially important as many systems will be situated within hybrid networks, using both provisioned and non-provisioned infrastructure. Finally, there needs to be careful consideration as to how the systems within the network will be accessed. We offer the following recommendations:

a. Cloud-based environments, whether consumed as a private, hybrid or public model, must be treated as an integral part of any network design and architecture.

Network architecture for cybersecurity is locked in place with an overall effort in federal IT modernization. One of the key initiatives for the overall modernization is the Cloud First initiative. Moving legacy infrastructure to provisioned cloud services is also one of the key recommendations of the recent GAO report on legacy systems [13]. Cloud-based environments, whether consumed as a private, hybrid or public model, must be treated as an integral part of any network design and architecture. "The cloud" is not a side-network; it is a fundamental component and must be designed/supported/secured as such.

b. Ensure the security of cloud-based and hybrid infrastructures by:

i. Adopting strong default and ubiquitous encryption for government communications when appropriate and applicable.
ii. Requiring multi-factor authentication for access to all networks.
iii. Implementing strict-role and policy-based access controls.

To ensure the overall security of federal networks and increase adoption of provisioned cloud services, the government needs to:

- Mandate widespread adoption of strong default, ubiquitous encryption for government communications when appropriate and applicable.
- Improve identity management, including requiring multi-factor authentication for access to all networks, ultimately eliminating password-based authentication entirely.
- Implement strict role- and policy-based access controls.

c. The network architecture needs to account for multiple paths compromise, including:

i. Share provisioned (i.e. cloud), non-provisioned, and hybrid infrastructure.
ii. Mobile devices.
iii. Remote access by government employees and third-party contractors.

"The perimeter" today goes beyond the traditional on-premise infrastructure and now includes cloud-hosted infrastructure, mobile devices, employee-owned assets leveraging an agency VPN connection, interconnections with third-party contractors and partners, and other use cases. Any successful network architecture will – at a minimum – acknowledge these alternate paths to potential compromise.

13 Government Accountability Office Report on Legacy System

d. Secure the network based on needs of the systems and applications.

Historically, network architects securing the perimeter assumed everything outside the firewall was "bad," everything inside was "good," and then deployed applications into that "good" environment. With the modern application (especially as DevOps and containers continue to expand), the entire concept of an application is dynamic, both in terms of location, and even behavior, on the network. Rather than focusing exclusively on securing the network alone, agencies should consider treating the application as the focal point and ensure that any proposed network architecture protection dynamically move with the application.

e. Network architecture needs to account for IoT devices without waiting for definitive federal standards or recommendations, by defining the function and communication requirements of specific IoT devices and following current industry recommended best practices.

As sensor technology continues to pervade the environment, agencies must factor these device types and the data they collect/store/transmit into any broader network architecture planning. In the absence of finalized standards addressing security in the IoT space, agencies should take steps to identify the function and communication requirements of specific IoT devices and follow industry-standard best practices for mitigation of compromises, including:

- Changing factory-default credentials of any internet-connected device.
- Completely disabling the SSH service on any internet connected device (when not needed).
- Application of inbound/outbound firewall rules between IoT devices and the outside-the-agency environment.

f. Implement cloud-based security to extend the security perimeter beyond the traditional network boundaries.

Agencies should not overlook the emergence of shared, cloud-based marketplaces where security capabilities can be seamlessly tested and deployed as application-based software—an improvement over today's time-intensive hardware procurement, evaluation, installation, and system integration cycles.

Government needs to extend the security perimeter beyond the traditional network boundaries by leveraging cloud-based security solutions to mitigate threats targeting both provisioned and non-provisioned infrastructure far upstream from the enterprise network. A highly distributed cloud security platform will provide the scalable infrastructure necessary for mitigation, as well as an additional source of threat intelligence.

g. The modern network architecture must have the agility to rapidly restore availability during any event.

The modern network architecture must support rapid and, ideally, automated failover to ensure the availability or restoration of data/applications. While cloud environments may have availability-centric Service Level Agreements, it is ultimately the agencies' responsibility to ensure availability and restoration of data/applications in any environment. This is especially critical in the event of a compromise, attack, or some other disruptive event.

h. Policy and compliance must be consistently applied across all network components.

Policy – both content and management toolsets – must be consistently applied across all network

components. This includes policy application, compliance/visibility, and enforcement of applications into/out of cloud-based environments.

It is important that agencies are required to use Cloud Service Providers with FedRAMP ATOs. It's just as important, however, to recognize that FedRAMP security controls are baseline standards; specific agencies and networks with more specific security controls should apply those controls to their provisioned cloud environments.

i. **Visibility into network infrastructure is required to see all the traffic that traverses the physical, virtual, and cloud environments to enable inspection, detection, and prevention of cybersecurity threat activity with automated reporting and alerting. In an on-premises environment, this would include visibility into physical device traffic. In a cloud environment, this would include visibility into virtual environments.**

Comprehensive situational awareness at the network level, accomplished primarily through network traffic collection (deep packet inspection), is a fundamental component to good cyber hygiene. Without this visibility, agencies will not know what traffic is transiting the network(s), what the intended traffic should be on those network(s), what is "known good" traffic within the environment, or what the associated firewall and access control list impacts are to applications operating within/between network(s).

Networks (physical, virtual, and cloud) must be architected with chokepoints to permit reliable, automated collection (and short- to mid-term storage) of 100% of network traffic (raw packets and metadata) for forensic purposes. The production environment, and visibility into it, always includes not just "north-south" traffic (ingress/egress at the edge) but also "east-west" traffic (internal or core).

j. **Ensure that all monitoring and alerting tool sets are fully integrated for interoperability.**

Another key capability which should be prioritized is automation of actionable alerts. Correlation of alerts, either from a single security solution or from multiple interoperable solutions, is one method to scale existing solutions to meet today's threats. Automation of response – proactively isolating or shutting down infected devices or even networks – should also be considered, tested, and implemented where it makes sense.

k. **Use network segmentation of key agency functions/assets to slow and isolate potential threats.**

Network segmentation of key agency functions/assets is one methodology to slow (or deny) attackers' progress. Good segmentation design also facilitates reactive isolation of impacted assets and applications, especially when those assets/applications reside within a third-party/cloud-based infrastructure. Agencies must also seek to not only fully document, but actively reduce, wherever possible, the number of access points into the production environment.

l. **Have a clearly defined mitigation plan and ensure (before an incident) that all internal/external incident response entities have a full understanding of the network architecture and systems within the architecture.**

An often overlooked aspect to network architecture is the people who ensure the operation and maintenance of the network. It is critical that they have full understanding of the network architecture and systems within the architecture. Furthermore, they need to have and maintain a clearly defined incident response plan that includes all internal/external incident response entities. Firefighters seldom charge into large, complex burning buildings without consulting some type of blueprint or floor plan first.

6. Devote resources to cybersecurity research and development.

National bug bounty program (NBBP)

Zero-day vulnerabilities are security bugs that become known publicly before vendors that manage the relevant code or users of relevant technology become aware of them, such that there have been "zero days" between when the vulnerability becomes known and when the vendor or broader security community have had the opportunity to develop and issue a patch or other mitigation. zero-days have great offensive and monetary value when they are discovered, either by malicious or non-malicious finders, and have not yet been disclosed to the public.

When a security researcher discovers a zero-day vulnerability, the researcher has a few options:

a. Publicly disclose the vulnerability.
b. Report the vulnerability directly to the upstream vendor or open source community, sometimes for monetary reward in a "bug bounty" program (e.g., when the vulnerability is particularly critical to a vendor's technology).
c. Report the vulnerability to a third party, (i.e. a Computer Emergency Response Team (CERT)) or a bug bounty platform (e.g., HackerOne or Bug Crowd), which then reports the vulnerability to the affected vendor or the open source community.
d. Sell the vulnerability to a "zero-day broker" who buys exclusive intellectual property rights to it to re-sell it to third parties.

Many in the cybersecurity community favor the second and third options. This is demonstrated in a recent survey, published by the Department of Commerce's National Telecommunications and Information Administration[14]. When a vulnerability is reported to a vendor, either directly or via a third party, that vendor can develop a patch or other mitigation, protecting the technology ecosystem. Alternatively, when a vulnerability is publicly disclosed, malicious actors may develop an exploit before vendors can issue a patch, and when a vulnerability is sold to a zero-day broker, there is a risk that the vulnerability will be used and no patch will be developed, increasing risk, and decreasing confidence in the technology ecosystem.

Leveraging a popular phrase in politics, Katie Moussoris, then chief policy officer at HackerOne, now founder of Luta Security[15] , wrote in 2015 about "draining the swamp of vulnerabilities" by leveraging the zero-day market via bug bounty programs. Using a system dynamics model to examine influencing factors on the zero-day market[16], Moussoris and Dr. Michael Siegel of MIT Sloan determined that while price alone is not the only lever affecting the market, bug bounty programs and incentive programs are still effective techniques for "draining the swamp." Price is not the only factor because numerous security researchers are motivated to protect the technology ecosystem; as such, while a zero-day broker may pay a high bounty, that researcher may still decide to report the vulnerability directly to a vendor, either for a bounty or not.

A year before, Dan Geer, Chief Information Security Officer (CISO) of In-Q-Tel[17] , suggested that the government out-bid zero-day buyers by a factor of 10 to corner the market on new vulnerabilities[18] . Geer argued that overpaying would grow the market of professional bug hunters, and that disclosure would

14 https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

15 http://lutasecurity.com/

16 https://www.hackerone.com/blog/the-wolves-of-vuln-street

17 https://en.wikipedia.org/wiki/Dan_Geer

18 http://geer.tinho.net/geer.blackhat.6viii14.txt

devalue zero-days in non-government markets.

The government should institute a NBBP, scoped to government technology systems (and not including commercial technology), to get first access to newly discovered vulnerabilities in government hardware or software. This would be an expansion of agency-driven bug bounty programs, such as the successful "Hack the Pentagon" pilot. In addition, the government should support agencies' development of coordinated vulnerability disclosure policies and programs, which are necessary to prepare agencies to receive and process vulnerability reports. For agency with fewer resources to devote to such programs, the government may consider leveraging third parties, such as bug bounty platforms, to support their implementation.

Further, as noted by Moussoris and Siegel, an incentive program should be included in the NBBP that rewards vulnerability-discovering technologies. This could be instituted as an XPRIZE-style contest [19] that pays a lump sum to companies that submit technologies that accelerate the discovery of zero-days, or prevent the vulnerability's creation in the first place.

7. Establish more robust information sharing mechanisms with the goal of automating the task.

The inherently distributed nature of cybersecurity-related threats requires a more collaborative approach that leverages the unique capabilities, visibility, and authorities of companies and governments. The emergence of new, innovative models for the automated sharing of cyber threat indicators to directly inform preventative action against cyber threats is one important manifestation of this collaboration.

Cyber threat information sharing, while critical, is not a cure-all or the end goal. Information sharing is one necessary tool within a much larger strategy that leverages people, process, and technology towards raising costs for our adversaries and actively preventing cybersecurity attacks. We offer the following recommendations:

a. DHS National Cybersecurity and Communications Integration Center (NCCIC) should remain the centralized federal aggregator and source for threat intelligence.

The NCCIC has been effective in aggregating threat intelligence and disseminating information about active threats and vulnerabilities. Acting as the primary, federally centralized organization for cybersecurity, it is now effectively collaborating with 64 private entities and 11 federal agencies.

b. Efforts to duplicate the NCCIC would be costly and cause confusion among private- and public-sector organizations as well as threat intelligence vendors.

Since the NCCIC has already been established with considerable investment, ITAPS recommends that the NCCIC remain the centralized federal aggregator and source for cybersecurity threat intelligence. Creating separate cybersecurity collaboration and education centers, such as that recently announced by The Department of Health and Human Services (HHS)[20] , would cause confusion among both public and private sector organizations with respect to reporting and gathering reports. Furthermore, it would create yet another system for reporting and aggregation, which is one of the key issues raised by the GAO as a risk.

c. NCCIC should proceed with implementation of the key recommendations of the released in February 2017[21], outlining several key recommendations for improving the effectiveness of the NCCIC and the

19 http://www.xprize.org/about/what-is-an-prize

20 https://fcw.com/articles/2017/06/21/hhs-cyber-center-hearing-hsgac.aspx

21 http://www.gao.gov/assets/690/682435.pdf

ability collaborate with other organizations.

1. Consolidate reporting methods and incident logging.
2. Consolidation or seamless integration of multiple aggregation systems.
3. Eliminate manual entry of incidents.
4. Ensure access of information.

We recommend that investment into the NCCIC should continue toward improving the efficiency and capabilities of the NCCIC. The GAO (previously cited) released a report in February outlining several key recommendations for improving the effectiveness of the NCCIC and the ability to collaborate with other organizations.

The GAO report also calls for DHS to address concerns over accessibility for both providing and accessing data. The specific example in the report is the migration the NCCIC portal to the Homeland Security Information Network, which is categorized as a FIPS 199 high-impact system requiring authentication of individuals with access to the system. For international partners, the concern is this migration would prevent collaboration because continued access would require the submission of international participants' passports and other sensitive personal information to a U.S. government entity. It is conceivable that such restrictions could also impact US private sector collaborations. We recommend that DHS investigate how to address this barrier, perhaps creating a proxy web interface which would not require direct access to a DHS high-impact system.

d. Ensure information sharing is as automated and actionable as possible.

There must be a focus on making information sharing as automated and actionable as possible. This means collapsing the last mile; the amount of time between when an organization receives a technical indicator and the implementation of a preventive control to enforce security based on that threat information. Further, we need to focus on sharing more than isolated indicators of compromise and incentivize the sharing of correlated threat indicators that link together multiple steps of the adversary's playbook, aligned to each phase of the attack lifecycle — including reconnaissance, weaponization, delivery, exploitation, and command and control.

To meet this goal, we recommend that DHS:

1. Complete the previously recommended data set and network consolidation
2. Ensure the functional accessibility of data.

e. Agencies and NCCIC need to communicate with respect to their needs for data aggregation and intelligence sharing. Specifically:

1. **How organizations can best provide aggregated information?**
2. **How NCCIC can better provide access to data?**
3. **How NCCIC can better organize data for an agency's needs?**

Functional specifically means that data be searchable. Furthermore, DHS needs to have a system which would apply search filters based on the classification level data sets and user privilege. For example, searches by users from one organization would have filters applied that restrict them to data that has been classified as publicly available. Users with sufficient clearance levels would have filters that would include search results including more restricted data sets.

In addition to the recommendations of the GAO report, DHS needs to work with other agencies, especially

ones considering creation of their own cybersecurity centers, like HHS. DHS should open dialogues with specific agencies to determine what their specific needs are and what factors are drivers for the creation of a separate cybersecurity center, so that improvements can be made to NCCIC.

f. Reduce dependence on Trusted Internet Connection (TIC) and EINSTEIN programs for data aggregation and mitigation by defining a standard and process for provisioned security solution vendors to be able to provide the data to DHS, while mitigating threats upstream from the TIC in a near real time fashion.

TIC requirements and programs such as Einstein (E3A) have been successful in providing DHS key threat intelligence. The data, however, is only aggregated at the TIC. This has caused a dilemma for some agencies considering using a cloud security solution. The cloud security solution would have far more scalability for the mitigation of threats, but threats would be mitigated upstream from the TIC/E3A, preventing that information from being aggregated by DHS.

Our recommendation would be to create a standardized policy and process for providing the data captured by upstream cloud security solutions to DHS. If we consider the established Structured Threat Information Expression (STIX) protocol as the standard, then it's only a matter of establishing the process workflow for sending the data to DHS. By having a standard process for reporting on upstream mitigations, it would enable organizations to leverage provisioned cloud security services without concerns regarding reporting requirements. Furthermore, this approach will enhance the amount of threat intelligence being gathered by DHS.

g. Mandate near real time sharing of attack information between agencies and DHS

One regulatory recommendation for information sharing would be to mandate near real-time sharing of attack information between agencies and DHS. The value of information made available by the NCCIC would be significantly increased by increasing the size of the data sets being analyzed. While many agencies are proactive in reporting this information, a mandate would increase adoption of this practice and require it to be done in a timely, near real-time manner, which would provide DHS better visibility into active threats and allow agencies to be better informed and mitigate threats experienced by other agencies.

To quickly establish compliance with such a mandate, it is important to fund this mandate. As we have seen in the past, unfunded mandates are much more slowly adopted. Remember, this is not an investment into individual agencies. It is an overall investment into aggregating threat intelligence for all federal agencies and partners.

Cybersecurity
Additional Resources

Cloud Security insight articles and solutions - Akamai

DNS and DNS Security information - Akamai:

DDoS Mitigation - Akamai

Federal Government Case Studies:
https://www.akamai.com/us/en/our-customers/customer-stories-united-states-census.jsp

https://www.akamai.com/us/en/our-customers/customer-stories-federal-aviation-administration.jsp

https://www.akamai.com/us/en/our-customers/customer-stories-us-digital-defense-service.jsp

https://www.akamai.com/us/en/our-customers/customer-stories-virginia-department-of-elections.jsp

Tech Industry Task Force Offers Cybersecurity Recommendations to the White House after OPM Hack Attack Effects Millions of People

Cybersecurity In Government - Microsoft

Future Trends

Topline Recommendations

The Future Trends workstream within the IT Modernization sprint exercise seeks to future proof the recommendations of the other workstreams so that the federal government is not simply catching up, but potentially jumping ahead in its adoption and use of IT. This workstream group also discussed the importance of addressing additional innovative technologies that should be considered within the report scope.

1. **Reduce costs, complexity, and vendor lock-in and drive increased agility, employee productivity and efficiencies by establishing interoperability as a baseline requirement for information technology (IT) projects.**

2. **Enable U.S. competitiveness in 3D printing (3DP) by developing and harmonizing policy and regulations and coordinate standards at the international, national, state, and local levels.**

3. **Support continued development of blockchain technology and avoid regulation before the technology is matured.**

4. **Nurture the development of artificial intelligence (AI) through policy development and support for research, including the application of AI capabilities to federal government uses not yet imagined.**

5. **Accelerate the adoption and deployment of 5th generation mobile networks (5G) through investment in research and development and early adoption by the federal government to enhance mission success.**

Future Trends
Detailed Recommendations

1. **Reduce costs, complexity, and vendor lock-in and drive increased agility, employee productivity and efficiencies by establishing interoperability as a baseline requirement for IT projects.**

Despite increasing deficits and budget austerity measures, federal, state, and local governments are expected to provide better, timely, efficient, and more secure services with dwindling resources. Driving commonality throughout federal government systems presents the best opportunity to meet these objectives, while better leveraging taxpayer dollars. Recognizing the value presented through interoperable IT systems, several agencies have endeavored to consolidate and streamline their IT resources.

As articulated in the Technology CEO Council's January 2017 government efficiency report, The Government We Need, shared services offer a viable pathway to drive greater interoperability in government.

> "Transitioning common administrative agency functions to shared service centers is a proven method to reduce costs while increasing the effectiveness and efficiency of service delivery. Shared services represent an opportunity to transition agency resources from focusing on administrative tasks, such as processing human resources and finance transactions, toward strategic, value-added activities." [1]

The Office of Personnel Management (OPM) has already demonstrated the value of shared services through the consolidation of 26 payroll systems streamlined into six federal and four private payroll shared service centers (SSCs). The move has generated $1.6 billion in savings from fiscal year (FY) 2004 to FY 2015, with continued estimated savings of $184 million per year. As OPM notes in their Cost Benefits Analysis of shared human resources (HR) services, "delays in agency migrations to SSCs have resulted in a significant loss of potential HR cost savings and a delay in the realization of HR cost avoidance."[2] Private industry has the experience and expertise to help the federal government achieve its interoperability goals. To that end, collaborative industry initiatives, such as Redfish, created by the Distributed Management Task Force, Inc.[3] , are working on behalf of government, enterprise, mid-tier, and small businesses to facilitate the attainment of widely recognized shared services value propositions[4].

The value propositions of interoperability for government and enterprise are:

Reduced:

- Vendor Lock-in.
- Costs (i.e. these are open standards and possibly sourced-based and not proprietary).
- Complexity – (systems "act alike" and not as individual "snow flake" offers).

1 http://www.techceocouncil.org/clientuploads/TCC%20Government%20Efficiency%201-10-17.pdf

2 https://www.opm.gov/services-for-agencies/hr-line-of-business/cost-benefit-analysis/fy-2011-cost-benefit-analysis-report.pdf

3 https://www.dmtf.org/standards/redfish

4 http://www.eweek.com/it-management/dell-hp-emerson-intel-team-up-on-data-center-standard

Increased:

- Government agility (since systems are interoperable, government customers can move to the most advantageous vendor, which allows them to take advantage of latest technology).

- Employee productivity (having one construct to know, implement, run, and administrate drives employee efficiency through reduced training times, standardized certifications, and cross agency collaboration).

Redfish is an industry effort started approximately three years ago to provide interoperability among multiple server leaders (the computational "engines" of enterprises, the clouds, and the internet).

Before that, there was a plethora of non-comprehensive and dated standards and proprietary implementation, management, and signaling methodologies from individual server vendors that led to multiple inefficiencies. Redfish is designed to provide the rigorous definitions for a modern, simple, and secure management interface. The Redfish standards are on a rapid publication cadence (3 times/year), which has enabled the standard to add more comprehensive server management capabilities, and react to feedback from the industry and its customers for optimizing interoperability and performance. Interoperability plugfests[5] have begun, and efforts are starting to add Redfish support to open source projects (like OpenStack, Puppet, and Nagios) and other management solutions.

The efforts and results of Redfish have accelerated since the initial publication in August 2016, and it is on the cusp of being able to clearly show the value proposition and benefits described above.

In addition to use on a server, there are efforts underway to define interoperable Redfish-aligned management standards for:

- Storage.

- Networking.

- Data Center Power and Cooling (typically the 2nd or 3rd largest monthly cost for operating a data center).

Recommendations:

- Adopt innovations and advancements, such as Redfish, to deliver even more savings that the federal government could re-use to fund other innovation. For example, savings could be used to move from operations and maintenance of IT systems to a mode of innovation.

- Promote technology training in other IT areas of the government to drive adoption.

- Provide code samples utilizing Redfish in the open forum Distributed Management Task Force (DMTF) to user groups within the industry to accelerate adoption.

2. **Enable U.S. competitiveness in 3D printing by developing and harmonizing policy and regulations and coordinate standards at the international, national, state, and local levels.**

Two key examples of innovation – 3D Printing (3DP) / Additive Manufacturing (AM) and Blockchain technologies – will require broad-based enablement (including IT innovation) at the national level if the United States is to establish and maintain global competitiveness in these strategic areas over time.

5 https://www.pcmag.com/encyclopedia/term/49399/plugfest

The coming 4th industrial revolution [6] (i.e., digital manufacturing or Industry 4.0) will surpass all other industrial revolutions in terms of scale, scope, and complexity.

The ability to seamlessly transport data from the physical world to digital (e.g., advanced scanning/modeling), then from the digital realm (e.g., design blueprints) back to the physical world (e.g., 3DP) represents a seismic disruptive opportunity, as well as very real challenges to scale. 3DP will revolutionize, localize, and democratize the $12 trillion global manufacturing sector. To put that figure into perspective, the United States' 2015 gross domestic product (GDP) was just under $18 trillion compared to China's 2015 GDP of nearly $11 trillion and Germany's 2015 GDP of $3.4 trillion. There will be a very material, sectoral share shift of manufacturing during the Industry 4.0 revolution.

Who will be well-positioned to reap the resulting economic growth and who will not? The democratization of this new hybrid-reality ecosystem will break existing value chains and replace them with geographically dispersed centers of excellence. Existing supply chains and business models will be disrupted at an accelerated rate as new sources of superior value are established in the marketplace.

Examples of value centers include those industry participants who utilize immersive computing to provide the specific on-ramps to the digital world, allowing creators globally to realize their vision. The analog to digital shift in printing will enable next-generation personalization capabilities on new materials (e.g., plastic, textile, metal, biosynthetic, etc.). We are already witnessing the mainstreaming of 3DP/AM technologies with a current focus of shifting from rapid prototyping to mass manufacturing, despite barriers to scale.

Clearly, this administration and the industrial base do not want the U.S. to cede leadership in 3DP and immersive computing. The opportunity for economic expansion will be driven by many Industry 4.0 value levers, including mass customization, distributed value centers vs chains, rapid product lifecycles, business model disruption/creation, unprecedented design capabilities and the potential for a significant and sustained impact on global sustainability. 3DP capabilities are seeing dramatic year-on-year improvements in terms of part quality and part cost. The transformation to digital manufacturing is beginning to be constrained by other elements of the ecosystem: design software capable of effectively defining materials and parts at the voxel level; design engineers with deep knowledge of 3DP; production workflow and supply chain tools optimized for 3DP; and, capable materials that are cost competitive in manufacturing. Other countries are already aggressively offering incentives to attract digital manufacturing investments and jobs.

Recommendations:

- Coordinate policy, regulatory and standards policy at the international, national, state, and local levels to harmonize and enable U.S. competitiveness.

- Prioritize 3DP research & development investments for manufacturing applications (i.e. materials, design software).

- Create incentives for federal government and industry participants to move from analog to digital manufacturing.

- Invest in education and training for the skills a future U.S. workforce will need (e.g., for 3DP: composite research, manufacturing expertise, installation and maintenance, troubleshooting and instructing operators).

6 https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#376eed27795f

- Ensure the inclusion of physical to digital interfaces in national cybersecurity frameworks, policies, regulations, and related development investments (e.g., applied blockchain models).

- In addition to the recommendations outlined above, policymakers should enable the broader economic discussion necessary to inform a more robust understanding of policy implications. A discussion should focus on some of the questions outlined below:

- What are the implications of Industry 4.0 to our national economy?

- What are the obstacles to scaling out 3DP and how can the government play a role in addressing?

- What specific steps should be undertaken, in what sequence, and over what timeline to be successful?

- What are the competencies required for a well-positioned workforce of the future?

- What are our gaps and plans to address as a nation?

3. Support continued development of blockchain technology and avoid regulation before the technology is matured.

Of the many changes coming to our markets and economy, technology embodied in the blockchain of distributed data will have significant impact on multiple markets. Already seen in the cryptocurrencies that have aimed to replace or change the financial markets, blockchain will impact multiple other markets. While bitcoin uses the blockchain method to maintain anonymity of coin holders, anonymity is a choice within the system and not a requirement.

Blockchain technology has the ability to be utilized in many ways. It is so nascent, however, that industry believes that there are a multitude of possible applications that have yet to be imagined, much less developed. These include:

- Applying it to the supply chain to check the origin and pedigree of parts.

- Improve the quality and statistical insights into the manufacturing process.

- Create anonymity in medical records that can improve the analysis of treatments, including the understanding of the role genetics plays in disease, while maintaining personal privacy of health records.

Blockchain is also starting to find application in the transportation sector and in smart contracting and additional uses will emerge the more broadly it is implemented. The democratization of data afford by blockchain technology will significantly impact markets throughout the economy.

Autonomous vehicles will share data with control systems and other vehicles. Blockchain can be used to maintain anonymity and privacy of individual travel. It can also serve to collect taxation for road use. Consider a system where each vehicle is charged a fee per mile for usage of a specific road. The fees collected can be used specifically for repair of that road. This results in the taxation for that road being directly paid by the users and it can be collected without attribution of the users.

Recommendations:

- Government should avoid regulating markets. Premature regulation of markets will hamper the development of the technology's maturation and applicability.

- Fund blockchain research at the pre-competitive level to accelerate the application and bring benefits to the market.

- Utilize the distributed ledger provided by blockchain applications to allow visibility and eliminate middlemen in markets.

- Avoid distorting the evolution of the market by artificially sustaining middlemen and instead allow the consumer and user to benefit from lower costs.

- Avoid taxing blockchain applications. Moving the government's use of blockchain forward, embracing its security, and not creating barriers to development and continued application will ensure that the technology's power can be fully utilized.

4. Nurture the development of machine learning through policy development and support for research, including the application of artificial intelligence (AI) capabilities to federal government uses not yet imagined.

As the National Science and Technology Council's 2016 report on AI noted, there is no single, universally accepted definition of the term AI: "some define AI loosely as a computerized system that exhibits behavior that is commonly thought of as requiring intelligence. Others define AI as a system capable of rationally solving complex problems or taking appropriate actions to achieve its goals in whatever real-world circumstances it encounters."[7] For the purpose of these recommendations, our working definition of AI focuses on a field called machine learning, which specifically refers to the study of systems that learn from data without being explicitly programmed. The field of machine learning includes specific sub-fields, such as deep learning or deep neural networks, which have been responsible for many of the recent advancements in fields as varied as healthcare and transportation.

The federal government has historically played an important role in the development of AI, including in the specific sub-fields and techniques noted above. The recent boom in commercial AI applications can be traced back to public investments in scientific research. Supporting such research is critical to ensuring further innovation. Additionally, the federal government has an important role in promoting the positive, responsible development of AI and ensuring society understands – and is prepared for – its effects. We believe the recommendations below can help inform a balanced, pro-innovation government approach to this technology.

Recommendations:

- **Support research:** The federal government has traditionally played an important role in supporting long-term fundamental research. In fact, today's success in the development and deployment of AI can trace its roots to federally funded research dating back several decades. The government has – and should continue – to support research into the application of these technologies to meet social challenges, drive economic growth, and address potential limits and shortfalls.

- **Convene talent to meet social challenges:** AI has proven to be an effective tool for making progress on complex problems at significant scale. The federal government faces these types of challenges in

7 Preparing for the Future of Artificial Intelligence, Executive Office of the President, National Science and Technology Council Committee on Technology, October 2016.

energy, transportation, environment, urban planning, public health, and many other fields. We believe the federal government can convene task forces to explore the use of AI in these areas and, more generally, to improve the government's ability to deliver citizen services.

- **Invest in public data:** Making government data more accessible and machine readable presents a significant opportunity to accelerate the deployment of AI toward solving societal challenges and enhancing public good. Specific recommendations are detailed in the Big Data/Analytics proposals contained in this report.

- **Promote education and diversity:** The federal government has encouraged public support for increasing access to, and diversity in, science, technology, engineering, and mathematics (STEM) education and careers. The federal government should continue this effort to ensure that more students from more backgrounds have access to computer science education. We strongly support the Computer Science for All Initiative, and encourage similar projects. Additionally, with increased progress in robotics and automation, innovative training, retraining, and continuing education programs should be developed, via close collaboration between the public and private sectors, to ensure the benefits of these technological advances are widely felt.

- **Ensure flexibility and facilitate deployment while developing AI policy and regulation:** Despite many recent advances in AI, the field and its applications are still emerging. As opportunities are arising, we encourage a nuanced regulatory approach that will facilitate innovative applications and enable society to reap the full potential rewards of AI. To the extent that new rules are necessary to address safety, security, interoperability, operations, or other areas, we support expert agencies taking the lead on regulation of specific use cases in their areas of jurisdiction. In consumer protection areas, it will be important to maintain a harmonized approach as they assess whether new rules are needed and, if so, how they should be integrated with existing approaches developed over time. We also believe that consensus-driven best practices and self-regulatory bodies will play an important role in ensuring the flexibility necessary to drive innovation while simultaneously developing appropriate safeguards.

5. **Accelerate the adoption and deployment of 5th generation mobile networks (5G) through investment in research and development and early adoption by the federal government to enhance mission success.**

Progress in telecommunications is essential for the nation's productivity and competitiveness. Today, a notable force in modernizing the underlying telecommunications infrastructure is the industry push toward "5G" wireless communications, which is a crucial step forward for future innovations like Internet of Things (IoT) technologies, autonomous vehicles and smart cities that will improve our lives and enable future advances and economic growth. In parallel, industry is assuming and developing application architectures that go beyond traditional two-tier (client-cloud) Web services and architectures toward newer concepts, for example, coupled software "microservices" and physically distributed, three-tier IoT systems. 5G requirements are being driven in part by these application-level advances. An important question for the government is how to take full advantages of such telecommunication trends, potentially leaping ahead in technological capabilities instead of lagging, while maintaining a "futureproofed" deployment stance.

One part of the answer could be to fully leverage and exploit underpinnings that are being offered in the form of Software Defined Networking (SDN) and Network Function Virtualization (NFV). A second part of the answer is to directly invest in telecommunications leadership around 5G. A final part of the answer is to develop a coherent strategy for rolling out SDN-based network innovations, in plausible large-scale networks such as deployed by the Department of Defense (DoD), Department of Transportation, and other agencies with a stake in IoT and services infrastructure.

In terms of background, just as processors and networks are pervasively virtualized in modern datacenters, so too can networks be virtualized. SDN technology provides this "network virtualization" and can serve to scale and secure modern networks in much the way that virtual machines (VMs) have been successfully used to scale and secure modern datacenters. Moreover, SDN is ideally embodied in software rather than realized in hardware, which provides the kind of agility that should be the goal of IT modernization, whether in government or industry. In conjunction with SDN, NFV technology can be used to realize the functions of dedicated hardware, again providing agility in terms of designing and deploying services. At trade gatherings such as the Mobile World Congress, vendors and operators are making an increasingly compelling case that SDN and NFV are critical building blocks of 5G – and those building blocks are becoming mature enough for enterprises (and federal government agencies) to deploy in their networks by way of adopting best practices.

For example, network segmentation (implemented not with physical segmentation but through SDN) is increasingly viewed as a best security practice in enterprise datacenters and is available today for use in federal government IT modernization efforts.

Going forward, technologies like SDN may also provide key building blocks to secure the emerging IoT. A key aspect of the IoT is the existence of edge devices (sensors and actuators) that cannot benefit from physical security and which are difficult to update when software becomes unavailable. Fortunately, these devices are rarely connected directly to the internet, but are proxied in a three-tier architecture by an IoT "gateway." This "gateway," viewed as an extension of the datacenter, should arguably be secured in conjunction with the datacenter, which implies the use of processor virtualization, SDN, and NFV to deploy functionality in those gateways to achieve key cyber hygiene principles: least privilege; microsegmentation; encryption of data at rest; multi-factor authentication; and, persistent/automatic software patching.

By working toward these goals with software defined, virtualized solutions, the federal government will simultaneously be deploying solutions that are inherently more agile and open to upgrade in ways that support a future-proofing goal.

Recommendations:

- Fully leverage software-defined networking, processing, and storage in IT modernization plans to achieve IT goals related to agility, security, and scalability.

- Recognize 5G is an opportunity for the US to regain leadership in telecommunications by investing in research and development and by early adoption of 5G capabilities by the U.S. government.

- Develop a strategy for rolling out SDN-based demonstrators and deployments within the federal government, recognizing that the DoD and the intelligence community are well-poised to point the way for others.

Future Trends
Additional Resources

ITAPS Future Trends Table of Resources #1

ITAPS Future Trends Table of Resources #2

Blockchain Explained - IBM

Artificial Intelligence - Microsoft

Cognitive Services - Microsoft

Blockchain - Microsoft

IT Alliance
for Public Sector
A Division of ITI

Partnerships

Topline Recommendations

1. **Identify and alleviate barriers and obstacles for effective collaboration, communication and partnering with industry that have historically hobbled concepts such as public-private partnerships (PPP) and work to address and dispel perceived prohibitions on engagement with industry. Ensure that senior career, and appointed agency and department leadership are properly instructed and educated to establish and sustain high-level support for the use of public-private partnerships and to deepen overall engagement with industry.**

2. **Establish a Center of Excellence for Partnerships for government and industry to identify opportunities to partner together, establish best practices and standards, train the federal workforce, and deploy identified solutions to address the challenges associated with federal information technology (IT) modernization.**

3. **Deepen existing relationships and create new opportunities for department or agency specific partnerships with the IT sector that can leverage and deploy best practices and solutions identified through the Center of Excellence to help formulate options to address the mission-specific challenges of federal IT modernization.**

Partnerships
Detailed Recommendations

1. **Identify and alleviate barriers and obstacles for effective collaboration, communication and partnering with industry that have historically hobbled concepts such as public-private partnerships (PPP) and work to address and dispel perceived prohibitions on engagement with industry. Ensure that senior career, and appointed agency and department leadership are properly instructed and educated to establish and sustain high-level support for the use of public-private partnerships and to deepen overall engagement with industry.**

   Efforts to effectively engage, collaborate and partner with industry have long faced varying degrees of opposition from within the federal government. This opposition has largely been based on perceived prohibitions, many of which are based in flawed interpretation of statue or regulation. To create an environment where collaborative partnerships between the federal government and industry can flourish, the administration should work to dispel the flawed interpretations and clearly establish that robust engagement with industry, with the objective of identifying technological options and solutions for federal IT modernization, is permitted and encouraged.

   Senior leadership can also be instructed on the benefits of PPPs and encouraged by White House guidance to promote and support the use of government-industry arrangements to the maximum extent practicable.

2. **Establish a Center of Excellence for Partnerships for government and industry to identify opportunities to partner together, establish best practices and standards, train the federal workforce, and deploy identified solutions to address the challenges associated with federal IT modernization.**

   PPPs can be defined based on "Contracting for the 21st Century: A Partnership Model" as:

   > "Relationships among government agencies and private or nonprofit contractors that should be formed when dealing with services or products of highest complexity. In comparison to traditional contractor-customer relationships, they require radical changes in the roles played by all partners."

   For purposes of federal IT modernization, we believe it means innovative procurement regulations, new compensation models and incentives, and payment and technology innovation rolled into a project-based delivery model that meets the demands of today's digital citizen who uses IT regularly and effectively to engage with society, including with their government.

   Creating PPPs between industry and the federal government will open the door to innovation and cost savings on a scale currently unattainable. This model will accelerate adoption of industry best-in-class practices and solutions at lower cost and reduced risk for the federal government. It is important that industry and the federal government both share the risks involved, establish clear service level agreements, and align accountability to take advantage of rapidly changing technology and best commercial practices, while addressing the federal government's unique IT security and privacy requirements.

   Centers of excellence traditionally take one of three delivery-based business models, or some combination of them, to deliver their value. The federal government will need to define which model or combination of models is best suited for its IT modernization needs and set common operational principles to guide the structure and direction of the federal center. The models and their attributes include:

Repository Model:

- Identify and curate best practices, methodologies, and tools to be used and provide maintenance, support, and subject matter expertise on those identified practices, methodologies, and tools.
- Serve in a consultative and training role.
- Conduct research and provide advisory functions.

Governance Model:

- Provide project planning support.
- Offer functions to assist with portfolio management.
- Enforce the application and use of methodologies once established.

Service Provider Model:

- Offer the development of turn-key solutions.
- Utilize center-specific resources for assistance with projects.
- Coordinate efforts and initiatives across the enterprise.

Participation in the efforts of the center as an industry partner should be voluntary and open to business-unit stakeholders who have a corporate or civic interest in furthering the goal of federal IT modernization and the Center of Excellence. Such participation, however, should not create a dynamic where a business unit or executive of one company would dominate the direction and focus of the center. Instead, the center should match its direction to the overall strategic goals set forth by the federal IT modernization plan. Finally, unless otherwise determined for legal purposes, all models, processes, tools, techniques, concepts, and plans should be open and available for use by all stakeholders and participants.

3. **Deepen existing relationships and create new opportunities for department or agency specific partnerships with the IT sector that can leverage and deploy best practices and solutions identified through the Center of Excellence to help formulate options to address the mission-specific challenges of federal IT modernization.**

The common operating principles, and the guidance implementing them, should also restrict the creation of siloed, agency-specific, enterprise-level centers of excellence that will risk adopting redundant or conflicting capabilities. Any center established at the agency or department level should be focused on mission specific capabilities that do not easily transfer across the government-wide enterprise (e.g. – space based IT needs).

The same opportunities for stakeholders and industry business representative participation in the federal Center of Excellence should also extend to centers established at the agency or department level to focus on mission specific needs.

Partnerships
Additional Resources

How to Build More Impactful Centers of Excellence – Industry Week

Innovation Centers of Excellence: Next Practices in Innovation Management – Think for a Change

IT Alliance
for Public Sector
A Division of ITI

Purchasing & Contract Reform

Topline Recommendations

1. **Ensure that for all federal agencies, the primary goal of the procurement system must be to facilitate mission fulfillment at fair and reasonable pricing.**

2. **Maximize the use of data analytics by federal procurement officials to promote evidence-based procurement decisions based on the Total Cost of Acquisition.**

3. **Maximize the use of commercial practices and products when fulfilling agency requirements.**

4. **Leverage the global supply chain to maintain the nation's technological dominance.**

5. **Enhance market research to allow for additional opportunities for vendors to provide goods and services to the federal government.**

6. **Leverage "right-sized" common acquisition approaches driven by mission requirements, avoiding "one-size-fits-all" process solutions.**

7. **Promote ongoing statutory and regulatory review, including the sun-setting of relevant laws and regulations to require prompt review and analysis of their utility before legislative or regulatory efforts to reinstate them.**

8. **Embrace collaboration and dialogue with private sector stakeholders to promote innovation and program expertise, and to share experiences between the government and private sectors.**

9. **Explore the use of agile acquisition techniques to promote innovation.**

10. **Commit to career-based support for federal acquisition workforce personnel to promote professional development and technology fluency.**

11. **Drive cultural change by identifying and measuring key performance indicators for contract personnel, program managers, and organizations.**

12. **Evaluate current methods employed to achieve public policy objectives and determine whether alternate methods would improve efficiency.**

Purchasing & Contract Reform
Detailed Recommendations

Many panels have been convened over the years charged with addressing acquisition challenges faced by the federal government, and consistently, their recommendations for improving the system have centered on the identification and use of best business practices, coordinated acquisition management, simplification of procurement laws and regulations, increased competition, increased use of commercial practices, and the continued development of federal procurement professionals.

The main thrust of these panels and their recommendations has been to facilitate a transition from a procurement system based on acquiring goods and services using government-unique requirements under strict design specifications to one centered on the acquisition of commercial items to meet the federal government's needs. By so doing, the government recognized that for the Department of Defense (DoD) to maintain the technological superiority necessary to address new challenges and maintain national security, it needs to maintain a more rapid, unimpeded access to commercial technologies than other countries. As a result, Congress has passed several laws to facilitate commercial buying practices being incorporated by the government, including the Federal Acquisition Streamlining Act (FASA)[1] and the Clinger-Cohen Act[2], both of which were subsequently followed by the Service Acquisition Reform Act of 2003 (SARA)[3] and the Federal Information Technology Acquisition Reform Act (FITARA).[4]

FASA established a preference for commercial items by calling for the establishment of regulations for acquiring those items, which have been implemented as Federal Acquisition Regulation Part 12. Additionally, underpinning each of these laws is the Competition in Contracting Act (CICA) calling for "full and open competition."[5] These statutes and their implementing regulations have been in place for decades, and they have been integrated in the government and business acquisition community. Over time, the global political environment has continued to change, as has the globalized nature of the marketplace. This has transformed how companies do business and drive innovation by establishing value chains to design, develop, and market their products and services so they can be competitive and reach customers faster than ever before. At the same time, the acceptance of commercial products has expanded, growing in importance as the platform for continuing technological innovation.

1. **Ensure that for all federal agencies, the primary goal of the procurement system must be to facilitate mission fulfillment at fair and reasonable pricing.**

   The goal of the acquisition process should be to facilitate mission fulfillment by purchasing the best value goods and services in the most efficient, timely, and cost-effective manner that meets the federal government's competition requirements. It stands to reason that other policy drivers overlaid on the system, although undeniably worthy in and of themselves, would be immaterial if the government were unable to fulfill its core mission. Clarifying this goal unclutters the process and allows federal acquisition and program officials to focus on contributing value-added service to their organization's efforts.

   Implementing action:

   - Remove policy overlays on the federal acquisition process that do not facilitate or further

1 Pub. L. No. 103-355 (Oct. 13, 1994).

2 Pub. L. No. 104-106, National Defense Authorization Act for Fiscal Year 1996, Division E, as codified in 40 U.S.C. 1401 et seq. (Feb. 10, 1996).

3 Pub. L. No. 108-136, National Defense Authorization Act for Fiscal Year 2004, Title XIV (Nov. 24, 2003).

4 Pub. L. No. 113-291, Carl Levin and Howard P. Buck McKeon National Defense Authorization Act for Fiscal Year 2015, Title VIII, Subtitle D (Dec. 19, 2014).

5 Pub. L. No. 98-369, as codified in 41 U.S.C. 253 (July 18, 1984).

mission fulfillment as the goal of the acquisition system.

2. Maximize the use of data analytics by federal procurement officials to promote evidence-based procurement decisions based on the Total Cost of Acquisition.

As recognized by the National Defense Industrial Association (NDIA) in its 2014 study, "Pathway to Transformation,"[6] faced with the responsibility to manage processes and increasingly complex IT programs, the government's use of Big Data and other analytic tools with comprehensive metrics would enhance program performance and management. These metrics would allow the government to assess the Total Cost of Acquisition (TCA), i.e., all direct and indirect costs of acquisition, including the monetized cost of time, associated with differing approaches to acquisition. In addition to defining optimal acquisition solutions up front in the process, managers would be able to identify performance issues before they undermine a program, manage any needed implementation changes, and identify opportunities for success that can be shared. Focusing on the TCA recognizes that processes are tools to an end, not an end in themselves; thus, it allows the government to assess whether the benefit of any process is worth the cost. Any process not mandated by law that increases the TCA should be avoided.

Implementing action:

- The Office of Federal Procurement Policy (OFPP) should construct an analytic framework by which to measure the benefit of any process in the acquisition system. This framework must include an assessment of the TCA, as defined above, of any process.

3. Maximize the use of commercial practices and products when fulfilling agency requirements.

Increasingly, the commercial market is the main driver of information technology (IT) research and innovation. Absent an appropriate statutory, programmatic, or policy driver, it is not in the federal government's interest to consume scarce resources undertaking unique activities and/or innovations that could be procured from the commercial market. Indeed, by utilizing streamlined commercial processes and purchasing commercial products and services, the federal government can leverage the research and innovation expenditures made by the private sector and thereby free scarce budget dollars for mission-critical needs. By leveraging competitive commercial procedures to fulfill its requirements, the government can maximize its access to cutting-edge technology, while also increasing downward price pressure and incentives for vendors to innovate. Current laws and regulations provide excellent guidance on the use of commercial processes and products. Specifically, they require agencies to utilize commercial products, terms, and conditions "to the maximum extent practicable."[7] By articulating this standard, these policies recognize that, although government and commercial entities have similar operational processes, the two sectors are not identical. Legal and policy drivers, as well as the mission of the government itself, may militate against its wholesale adoption of all commercial practices. What is left for consideration, then, is a strong preference for commercial processes and products, with a recognition that appropriate government interests must be balanced.

Commercial online marketplaces could provide opportunities for the federal government to facilitate and transform the acquisition of certain commercial items, representing significant opportunities for the government to leverage the commercial market and enjoy the benefits noted above. The use of such marketplaces has the potential to operate in a manner consistent with many objectives the federal government has been promoting for decades, including lowering barriers to entry for non-traditional firms and small businesses, reducing regulation, increasing the use of commercial terms and conditions,

6 National Defense Industry Association, Pathway to Transformation: NDIA Acquisition Reform Recommendations (Nov. 14, 2014).

7 Cf. 41 USC 3077; see FAR 12.301(a) and FAR 12.302(c).

and paying competitive commercial prices. Additionally, the government could have access to useful transaction data without imposing collection burdens on itself or contractors. Furthermore, allowing the federal government to access multiple, competitive online marketplaces affords agencies the opportunity, with minimal administrative activity and cost, to reap the full benefits of competition by opening channels to suppliers and by incenting multiple marketplace providers to lower transaction fees and improve their service to be attractive platforms through which those suppliers may be accessed.

As the federal government explores the use of commercial online marketplaces for certain commercial items, it will need to address a few operational considerations to assure that its actions do not undermine markets, the vitality of its supplier base, or its long-term ability to obtain fair and reasonable prices for the goods and services it purchases.

First, the federal government should determine what qualities commercial online marketplaces must exhibit to qualify for government use. If it seeks to award contracts for online marketplaces, rather than contract with a limited number of commercial online marketplace providers, the government should authorize the use by agencies of all commercial marketplace providers that meet certain criteria. These criteria should include qualities that provide assurances for government buying priorities, as examples, adequate competition among commercial marketplace platforms and suppliers on those platforms, and the assurance of fair and reasonable prices (e.g., product pricing and other terms, and marketplace provider transactions fees), among others.

A strong ecosystem of authorized and qualified online marketplace providers will help avoid the potential problems of a single or limited number of providers capturing the federal market by providing agencies access to the largest number of products across multiple commercial marketplaces, incenting competitive transaction fees from marketplace providers, and encouraging continuous service improvement. Thus, the federal government will need to assess the prudent use of only those government terms and conditions necessary to assure specific compliance with the law, to promote competition among online marketplace providers and suppliers selling through online marketplaces, and, if online marketplace services are utilized pursuant to awarded contracts (rather than directly through platforms), to fulfill its obligation to administer any contracts awarded. By way of example, the federal government will need the ability to prevent any direct and/or indirect “pay-to-play” terms/actions imposed by online marketplace providers on suppliers.

Additionally, the federal government will need to determine which categories of products and services should be authorized for purchase from commercial online marketplaces, and what controls need to exist for government needs (e.g., the pedigree of the product purchased). Moreover, the realities of online transactions raise the federal government’s interest in safeguarding its data and supplier data, including compliance with the government’s expectations for defenses from cyber-attack. With supplier and customer data residing in online marketplace provider networks, the federal government has an interest in restricting any use by marketplace providers of data obtained from suppliers to preserve the commercial competitive nature of online transactions. Finally, when the above considerations and interests are accounted for, should the federal government award contracts for online marketplaces, it should also allow contractors to use those commercial online marketplaces when providing government furnished property under the terms of a contract.

It is important to note that the foregoing discussion is not intended to limit the federal government’s means of accessing commercial online marketplaces. Indeed, to the extent that the federal government can articulate in policy, statutes, and/or regulations the standards that govern agency utilization of commercial online marketplaces and account for its interest, and utilize compliant commercial online marketplaces to the maximum extent practicable, we believe it should consider doing so.

Implementing actions:

- Undergo a federal government-wide review to determine the extent that commercial products, terms, and conditions are not used.

- Require contracting officers to provide a written determination as to why commercial terms and conditions were not utilized.

- Use online commercial marketplaces for the acquisition of certain commercial items in a manner that addresses the federal government's interests, as set forth above.

- Allow contractors to use commercial online marketplaces when providing the federal government furnished property under terms of a contract when the government's interests are addressed.

4. Leverage the global supply chain to maintain the nation's technological dominance.

For years, a key element of our nation's security has been the commitment to developing and fielding new technologies faster than any adversary.[8] To this end, the nation relied on, in large part, domestic innovation, and production. That dynamic has changed. The nation exists in a global economy with global research and development, global manufacturing, and global supply chains. These supply chains enable efficient delivery of a wide range of goods and services. Additionally, because allies and adversaries alike have access to this global marketplace, they can close the technology gap that underpins our nation's security. Thus, to maintain the United States' technological dominance, in addition to mitigating non-value-added procedures, the acquisition process should facilitate the federal government's access to the global market.

This access already occurs as a result of the Trade Agreements Act of 1979 (TAA), which mandates that only U.S.-made or designated country end products shall be purchased by the federal government. These designated countries are our international trade allies, countries with which the U.S. has negotiated extensive bilateral and multilateral agreements that include commitments to uphold the rule of law and to provide strong protections for intellectual property rights. Continued adherence to the TAA regime would expand the nation's research and innovation base and utilize the acquisition process to enhance joint engagement in defense of common national interests.

Implementing actions:

- To sustain our nation's technological superiority and the national security it underpins, federal government procurement processes should not be used to hobble access to the global marketplace.

- The Administration should continue to rely on the provisions in the Trade Agreements Act to facilitate the federal government's access to the most innovative and mission-critical technologies.

5. Enhance market research to allow for additional opportunities for vendors to provide goods and services to the federal government.

Departments and agencies generally are required to conduct market research into potential solutions and technologies prior to conducting acquisitions, but there is minimal legislative or regulatory guidance on how the federal government should conduct that research. As a result, government agencies sometimes conduct pro forma market research, such as visiting trade shows, conducting internet searches, or perhaps

8 Non-Traditional Commercial Defense Contractors, Gansler, Jacques S., Greenwalt, William C., and Lusty, William (UMD-CM-13-119), Center for Public Policy and Private Enterprise (Nov. 2013).

speaking with a select group of industry providers. It does not, however, engage in open discussions with a swath of industry regarding the need it is trying to fill. As a result, agency solicitations can be based on a self-selected and narrow view of what the requirement is and/or how to fulfill it and federal agencies do not gain the perspective of other providers, with potentially innovative and lower-cost solutions, that are not in the selected cohort.

A more productive form of market research would be for federal acquisition officials to expand how forthcoming they are about their potential needs. If federal agencies provided advance and public notice of their potential requirements (through draft Requests for Proposals (RFP's), draft Statements of Work (SOW's), etc.), all industry providers could review them, ask questions, offer previously unidentified options and innovations, and provide feedback to the agency regarding it needs. This approach would allow providers who are not contacted by an agency the opportunity to participate in the process, and thus, would enhance market research.

Implementing actions:

- Federal agencies should issue draft RFP's, SOW's, etc., on a publicly available government point-of-entry and provide detailed information on the products they are seeking and the project that is being developed. Doing so would allow vendors to discuss the draft at an early stage of the acquisition process and allow agencies time to reconsider the requirements. Such efforts should afford adequate and reasonable time for industry to review the proposal and offer feedback.

- Such notices should also be brand and technology neutral and identify the federal government's salient functional and performance requirements.

- Federal agencies should be required to publish their market research results (e.g., prevailing industry practices; availability of commercial solutions; customary industry terms, conditions, and warranties; historical acquisition information; capabilities of small businesses) so that all stakeholders have insight into the basis for the government's decisions.

6. Leverage "right-sized" common acquisition approaches driven by mission requirements, avoiding "one-size-fits-all" process solutions.

Multi-award, Government-Wide Acquisition Contracts (GWACs), authorized pursuant to Section 5112(e) of the Clinger-Cohen Act, provide the federal government the opportunity to leverage its buying power and obtain administrative and cost efficiencies. The potential benefits of these vehicles, however, can be attenuated by inappropriately duplicative contracting vehicles. Conversely, inappropriately centralized GWACs risk subordinating legitimate mission drivers that may justify duplicative contracting vehicles. In any case, care must be taken to avoid the waste associated with assuming that the federal government can be viewed as one enterprise, or that a one-size-solution-fits-all. Again, first and foremost, federal acquisition should be driven by agency mission requirements, and sometimes, a level of duplication may need to be accepted to promote this overarching policy driver. For this reason, efforts directed toward common acquisition should allow for agency flexibility in meeting defined mission objectives and policy objectives.

Some have suggested the use of tools, like category management, to achieve right-sized acquisitions for common goods and services. Such tools can be useful, provided they are implemented properly. Specifically, mission drivers should be served most efficiently by these tools, and whether their use is proper must be assessed against defined metrics that identify the TCA. Moreover, it is not enough simply to use the nomenclature of industry with respect to such tools. That nomenclature and the tools

used by the federal government must have the same meaning, purpose, and practice understood by the government's supplier base to assure an integrated approach to a given procurement without conflict.

Implementing actions:

- Recognizing that the goal of the acquisition process should be to facilitate mission fulfillment, the federal government should avoid efforts to drive "one size solution fits all" approaches to contracting.

- Prohibit any mandate requiring the use of a specific contracting solution.

7. Promote ongoing statutory and regulatory review, including the sun-setting of relevant laws and regulations to require prompt review and analysis of their utility before legislative or regulatory efforts to reinstate them.

The federal acquisition reforms of the 1990s followed a critical substantive review of procurement law and policy. This so-called Section 800 Panel led to upwards of 250 statutes being reviewed, amended, or repealed, streamlining the acquisition process. Since that time, a multitude of laws have been passed and regulations and circulars promulgated, adding an element of complexity to the system. Congress, again, has undertaken the establishment of a panel, the Section 809 Panel, to conduct another review like that of its predecessor.

Generally, to mitigate conflicts, duplication, and inefficiency costs for the federal government and industry, it could be useful to define periodic reviews of laws, regulations, and circulars to determine their suitability for amendment or repeal, and, in this process, include the sun-setting of relevant laws and regulations after a date certain to require prompt review and analysis of their utility before legislative or regulatory efforts to reinstate them. To that end, the aforementioned NDIA study proposed a similar such review with the proviso that nothing be retained that is not justified expressly. [9]

Although this review is for the executive branch, which cannot amend laws unilaterally, it can amend its own regulations and make recommendations to Congress regarding laws it feels suitable for amendment or repeal. In any case, we note with appreciation the regulatory review already undertaken by this administration.

Implementing actions:

- Continue the existing regulatory review, integrating input from the Section 809 Panel, and repealing all regulations not required by statute or executive order.

- Implement a schedule to sunset new and existing regulations that will require prompt review and analysis of, and justification for, their utility before reinstating them.

- Work with Congress to adopt, where appropriate, the sun-setting of relevant acquisition laws and include a requirement for the prompt review and analysis of, and justification for, their utility before reinstating them.

- Mandate, as part of any information collection (IC) required by regulation, that prior to any collection the requesting agency determine whether the federal government already collects or possesses the same or similar data, or if the data is available from a public source. If the same or similar data is identified, the agency should be prohibited from requesting a waiver from the Paperwork Reduction

9 National Defense Industry Association, Pathway to Transformation: NDIA Acquisition Reform Recommendations (Nov. 14, 2014).

Act. Instead, the Office of Management and Budget should direct the agency to identify what steps and resources are necessary to access the data for purposes of satisfying the IC requirement, rather than devoting additional resources to the development of a new information collection mechanism and/or creating additional regulatory compliance burdens on an impacted stakeholder community.

8. Embrace collaboration and dialogue with private sector stakeholders to promote innovation and program expertise, and to share experiences between the government and private sectors.

The acquisition reforms of the 1990s sought to encourage dialog between the federal government and the private sector. Dialogue, occurring up front in the acquisition process, could enhance market research, promote accuracy in the requirements definition process, enhance competition, reduce disputes, and promote efficient contract administration. This practice seemed to have fallen off over the years, which prompted the Office of Federal Procurement Policy to issue a series of "Myth Busters" memos clarifying its utility and appropriateness.[10] Such encouragement should continue and innovation collaboration channels, whereby business innovation and program expertise and lessons-learned can be shared between the federal government and private sectors, should be explored.

Additionally, the federal government should consider revisiting the rules around Organizational Conflict of Interest (OCI). Clearly, the government has a legitimate interest in mitigating OCI, as such conflicts can reduce credibility in the procurement system. At the same time, OCI rules may impede standard commercial practices related to system development. Thus, the federal government should assess whether these rules can be modified to address the evolution of commercial practices while accounting for the government's interest and ability to acquire goods and services. In addition, the federal government may wish to explore alternative procurement approaches, like competition for both evaluation and implementation or the use of "two-step-like" techniques, that enhance incentives for firms to help the government in such planning and assessment activities.

Implementing actions:

- The Administration should encourage the federal acquisition workforce to increase appropriate communications with industry through inclusion of related performance metrics in each official's performance evaluation.

- The Administration should incentivize officials financially and through career advancement to enhance appropriate levels of communications, and it should reward, with similar incentives, collaborative behavior between industry and federal government personnel in the acquisition process.

9. Explore the use of agile acquisition techniques to promote innovation.

Increasingly, the dynamic nature of IT innovation conflicts with the timeframes and processes associated with federal government procurement. Large, complex government programs can involve static, upfront technology requirements assessments that drive program implementation over time. Consequently, should the federal government need to change its approach in response to this technology evolution, it may face significant administrative effort (and associated cost), and to the extent that it failed to exercise sufficient clairvoyance when it drafted its requirements up front, its options to respond to technology

10 See Memorandum from Daniel I. Gordon, Administrator for Federal Procurement Policy, to Chief Acquisition Officers, Senior Procurement Executives, Chief Information Officers, "Myth-Busting": Addressing Misconceptions to Improve Communication with Industry during the Acquisition Process (Feb 2, 2011); Memorandum from Lesley A. Field, Acting Administrator for Federal Procurement Policy, to Chief Acquisition Officers, Senior Procurement Executives, Chief Information Officers, "Myth-Busting 2": Addressing Misconceptions and Further Improving Communication During the Acquisition Process (May 7, 2012); Memorandum from Lesley A. Field, Acting Administrator for Federal Procurement Policy, to Chief Acquisition Officers, Senior Procurement Executives, Chief Information Officers, "Myth-busting 3": Further Improving Industry Communication with Effective Debriefings (Jan 5, 2017).

evolution may be limited. To address this challenge, the federal government could consider piloting technology and innovation acquisition activities in a manner akin to that referenced in the TechFAR, where it identifies objectives in short-run increments, solicits and accepts solutions, and adjusts accordingly. This approach is knowns as Agile Project Management. Such an approach could allow the federal government to explore solutions, even experiment, and accept the failure that sometimes comes with innovation, without incurring significant upfront expense.[11]

Implementing actions:

- The Administration should require the use of Agile Project Management in federal acquisition pilots for innovative IT projects.

- Create and use a performance evaluation metric that rewards the use of innovative acquisition tools by acquisition personnel.

10. Commit to career-based support for federal acquisition workforce personnel to promote professional development and technology fluency.

The federal acquisition process is complex, as is the technology acquired, which itself evolves rapidly. This technology must be reduced to requirements that are understood and that promote competition. Given the critical missions served, the increasing demand for technological fluency, and the overarching importance of their function to the nation, the federal acquisition workforce must be professionally supported and compensated to assure a continuity of expertise. To this end, the federal government should be updating and enhancing acquisition workforce education, areas of specialization, and professional development. Further, it should continue to identify opportunities to leverage current acquisition workforce development channels, such as the Federal Acquisition Institute and the Defense Acquisition University. Use of social media should be encouraged to facilitate message delivery and connect to a broader audience than is currently being reached. Additionally, video descriptions are becoming the norm in high tech positions in the public sector, and these allow the candidates to better understand the position and show the public their value.

Implementing actions:

- Require that program managers and contract officers receive ongoing training and guidance with respect to both technology and key acquisition practices, including requirements specific to the acquisition of commercial items, market research and competition.

- Set minimum IT graduation requirements for all federal acquisition personnel and require advanced training for those in the IT career path.

- Mandate that program managers must participate in an industry-government personnel exchange program to achieve career advancement.

- Require federal acquisition personnel to receive training on appropriate communication with industry in the acquisition process and evaluate them on their effectiveness.

11. Drive cultural change by identifying and measuring key performance indicators for contract personnel, program managers, and organizations.

11 See also "Government Technology Opportunity in the 21st Century," TechAmerica Foundation, Vol. 1, July 2010 at Sec. 2.2 ("Promote Agile/Incremental Development").

The professionalism expected of contract and program managers cannot thrive in a risk-averse environment, as the federal government relies on these individuals to exercise discretion, which always involves an element of risk. Thus, for the federal government to expand opportunities for professionals to exercise discretion, in addition to balancing the levels of discretion against technical and program experience, it needs to recast the work environment to accept rational risk-taking. In this regard, critical professional behaviors expected of those exercising discretion should be manifested in the Key Performance Indicators (KPIs) that are realistic, understandable, and meaningful against which those professionals will be evaluated. In addition, these KPIs should reward mission fulfillment.

Likewise, indicators need to be established and followed by the organizations in which these professionals perform. Those organizations, and senior management, must be held accountable to adhering to cultural practices via measurement tools like scorecards, that like KPIs, are developed with realistic, understandable, and meaningful common metrics to assess performance. Strong management practices such as these, we believe, are fundamental to creating cultural change in government.

Implementing actions:

- Federal agencies should utilize KPIs for contract personnel that reward innovation, mission fulfilment and attention to total cost of acquisition through indicators such as market research, extent of communications with industry, competition, and appropriate use of commercial items and practices.

- The Administration should develop an agency acquisition scorecard that provides clear metrics, such as use of commercial terms and conditions, use of innovative acquisition tools, etc., to assess the performance of each federal agency procurement system.

12. Evaluate current methods employed to achieve public policy objectives and determine whether alternate methods would improve efficiency.

The federal acquisition system is currently used to implement many laudable public policy goals. Throughout the system there are various tools in place to ensure small businesses can participate in the federal marketplace, encourage that a robust industrial base is created and sustained, and ensure compliance with environmental laws as well as labor laws. While these goals should be in place, it is unclear whether the mechanisms are in fact the best way to achieve public policy goals. For instance, many companies regardless of whether they serve as government contractors must observe laws already in place on wages for employees, workplace safety, nondiscrimination and the handling and treatment of materials and manufacturing processes to protect the environment. Requiring certification of these from federal contractors for compliance to the same statutes is duplicative and creates two systems for compliance, thereby increasing the costs and burden for both the federal government and businesses.

Additionally, with regards to small businesses, it is unclear whether the programs in place are creating a healthy industrial base and mobilizing the nation's full productive capacity as the Small Business Act originally intended. Until recently, small business goals had been primarily focused on the percentage of dollars awarded to these firms and not whether agencies have been spreading the dollars among all industries,[12] or the percentage of small businesses that are able to graduate from the program and thrive in an open marketplace. If the goal is to ensure small business participation in the federal marketplace and a thriving industrial base, then the tools to promote those goals should target the factors necessary for such an achievement (i.e. revenue, job creation, and growth) rather than solely focusing on the dollars awarded to these businesses.

12 Pub.L.No. 114-92, National Defense Authorization Act for Fiscal Year 2016, Sec. 868 (Nov. 11, 2015).

Implementing actions:

- OFPP, in conjunction with the Federal Acquisition Regulations Council, should conduct an assessment of public policy requirements overlaid on the federal procurement system that are not directly related to mission fulfillment.
    - OFPP should review both the benefits of the polices to the nation and the impact of these overlay requirements on the federal procurement system, including the cost of compliance, the delay in acquisition, duplicative requirements, and the efficiency of the federal procurement system to address non-procurement related policy goals (essentially, the TCA) – and, based on this assessment – make specific recommendations as to which requirements that are not related to mission fulfillment should remain or be removed from the FAR.
    - The evaluation should include a cost-benefit analysis of benefits of public policy objectives and their impact on the federal government's ability to procure and leverage optimal solutions.
- Require federal agencies to evaluate both the tools currently used to meet a stated public policy and whether they meet the intended goals. The focus of these efforts, however, should be to improve the industrial base and not meet arbitrary numerical goals, like participation rates.
- Eliminate compliance requirements and certifications where existing statutes and regulations already mandate compliance, e.g., labor compliance regimes and certifications for federal government procurement when they duplicate requirements already applicable to the private sector.

IT Alliance
for Public Sector
A Division of ITI

Talent/Recruiting/Training
Topline Recommendations

1. **The Administration must develop a vision for the public sector workforce that emulates what is found in the private sector, including the private sectors view of talent as a lifecycle.**

2. **To recruit the best talent, the Administration should:**

   - **Apply design thinking**
   - **Utilize a social branding strategy**
   - **Deploy better selection tools**
   - **Expand university recruiting strategy**
   - **Grow joint development and management with industry and academia**
   - **Introduce early professional tracks**
   - **Restructure the working environment**
   - **Partner with industry on leadership development**
   - **Deploy a succession planning tool**

3. **To retain talented individuals in the public sector the Administration must address the following:**

   - **Remove key impediments including:**
     - **Bureaucracy**
     - **Perception of low impact**
     - **Working environment and attractiveness**
     - **Address instability that arises with recurring administration changes**
     - **Investment in modern technology and procurement rules**

   - **Build credibility of the workforce by engagement by private sector, such as:Developing sprints with the corporate sector;**
     - **Exchange programs with private industry and government; and**
     - **Online training.**

4. **To ensure the current workforce has the skills needed to work on modern systems, the Administration should:**

   - **Identify digital skills gaps and propensity to upskill through cognitive tools**
   - **Certify the attainment of STEM skills**
   - **Create digital learning platforms with boot camps**

Talent/Recruitment/Training
Detailed Recommendations

As we began to develop recommendations on information technology (IT) modernization, the importance of talent emerged as a constant theme and priority in virtually every work stream. Industry continually pointed to the need for a competent, capable, and knowledgeable federal IT workforce as a key to the success of other workstreams. While there are many that fit the bill currently in the public sector, the need for additional staff that is not only proficient in the various IT technologies, but also has experience in the private sector, became a recommendation from these work streams.

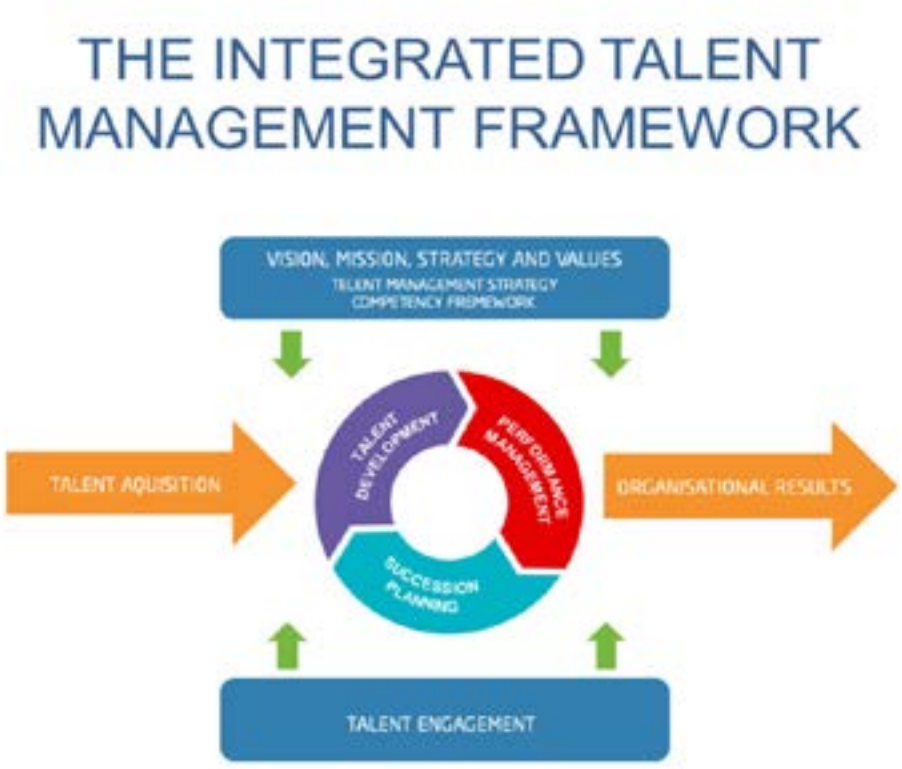
1. **The Administration must develop a vision for the public-sector workforce that emulates what is found in the private sector, including the view of talent as a lifecycle.**

   The first key in developing the workforce needed to modernize IT is developing a vision of the characteristics of the workforce and how it should operate. We recommend that this vision of the federal talent model should emulate the private sector in terms of recruitment, performance, evaluation, and retention incentivization. This vision should then be incorporated into each portion of the talent lifecycle, as shown in the chart below. The mission of recruiting federal talent needs to utilize more social media (such as use of LinkedIn), with video job descriptions, and for less senior jobs, interns with enthusiastic mentors.

   The goals of federal recruiting should meet the objectives of good employee experience, ability to retain, and, value for the dollar. Where the last seems to be counterintuitive, the ability to pay for a quality person is a two-way street that is often overlooked today. The mission within the federal venue should be to provide a wage that is competitive and receive a work product that is commiserate with that pay. Many within the private workforce have been cognizant of the work product requirement, but it has not been the same within the public sector workforce. This performance criteria, and the publishing of these criteria, would elevate the job desirability, as well as provide an understanding of what is expected of a prospective employee when they are ready to move to the public sector. This will help to renew the sense of pride in performing this public service.

   A good employee experience is paramount to the retention of the workforce. This experience can be as simple as Fridays off in the summer, which is already a policy in some departments, or as elaborate as forgiveness for student loans after a certain period of employment with, perhaps, the possibility of accelerated payback if the evaluations of the person are over 110% for an extended period. This achieves two of the goals: 1) it provides for an incentive to perform better; and 2) it assists the person and creates other tangible benefits, as their personal credit rating could be improved if they were eliminating debt effectively.

Private-sector Approach to Talent Lifecycle [1]



Additionally, by hiring better employees and retaining them, the operational efficiency of the department can be expected to improve. The department will see savings in training, time off reductions and higher-quality work products, which will allow for the mission to be accomplished more quickly. Furthermore, it should be noted that talent management should not be siloed into different efforts, but rather the government should address it as a lifecycle, similar to the chart referenced above, that each employee goes through in their career in the private sector. While many of these recommendations are discussed in a topic area, the topics areas themselves are intertwined under such an approach. Thus, each recommendation could fall into another area or be modified to address another topic.

Topic 1: *The United States government workforce is 2.1 million people, of whom 113,000 are IT employees. How can build an effective, evolving modern technical workforce? How should the government improve its recruiting of technical talent?*

Summary Point of View: Improve federal government recruitment, create new social branding, provide selection tools, and implement the adoption of agile processes for improved candidate and team experiences. Reimagine the working environment with modernized work spaces, work design, and career tracks built around digital skills.

» *What best practices can be adopted from private-sector human resources in branding, relationship building, and creating a compelling value proposition for pursuing a career as a technologist in*

1 See Centre for Executive Education, Integrated Talent Management (ITM) Framework—Winning the War for Talent 2.0 at http://www.cee-global.com/talent-management/.

government?

The federal government can improve its approaches by implementing the following recommendations:

- **Apply Design Thinking:** Design Thinking and Agile methodology will enable the federal government to take advantage of digital tools and move with speed to deliver solutions that have been pre-tested with inputs from constituencies.

- **Utilize a social branding strategy:** We can build a new, compelling branding strategy to attract top-tier talent into the federal government. Branding has allowed the private sector to accelerate our transformation and it has impacted the whole talent lifecycle from attracting, onboarding, retaining, and growing our talent. We are using a branding strategy combined with social solutions in our organization to successfully enhance the candidate experience.

- **Deploy better selection tools:** Deploying a cognitively enabled set of recruitment tools will reduce time to hire and deliver an enhanced candidate experience. Currently, it takes months for the federal government to hire and many critical roles remain unfilled. A better pipeline can be built with top talent using a candidate management system, including candidate self-service tools to find matches to open positions, such as law enforcement, cyber security, medical professionals, and executive leadership positions.

» *Are corporate/university leaders willing to engage in enabling the federal government to recruit on-campus and how can they work with government to build awareness of the public service option?*

Yes. This can be facilitated by:

- **Expanding university recruiting strategies:** Federal government agencies need to develop a more robust university recruiting strategy, not just during the period before graduation, but throughout the school year, to better target talented and committed students for internships.

- **Grow development and management opportunities with industry and academia:** This would include sponsoring projects with semi-private or government entities, along with new and existing research lab entities. By establishing strong university relationships, the tech sector has recruited experts from universities, complementing traditional recruiting processes.

» *How does the private sector ensure it builds an adequate pipeline – from junior to senior professionals – and how can this be adopted for the public sector?*

- **Introduce early professional tracks:** Attract the best talent to boot camps and 1-2-year structured experiential rotation programs for data scientists, developers, security experts, and functional disciplines. In addition, apprenticeships will attract motivated candidates who have not completed a university degree.

- **Restructure the working environment:** In the private sector, we have moved to digital workplaces that are characterized by less hierarchical organizational structures that are networks of collaborative teams. Leaders leverage internal social media and styles that are more transparent, working together in open space collaborative offices. This creates an environment for rapid learning and expertise sharing that is very attractive to early professional hires.

- **Partner with industry on leadership development:** Instead of sending high potential leaders to

third-party programs, which has limited impact on leadership quality, consider a joint leadership development program with private industry where high potential participants can learn together. This should be conducted with on-campus offerings and participating companies and agencies.

- **Deploy a succession planning tool:** Commission a succession planning system utilizing cognitive capability to access talent, interagency and bureau wide, to enable unfettered slating of candidates for broad government experiences. Provide cognitive assistance to enable better information, limit bias, find expertise, and select candidates. Cognitive interventions will guide both the applicant, as well as the hiring executive, on fit for role vis-à-vis market and industry based circumstances. Science-based assessments will test for several variables beyond performance and potential.

Topic 2: *What steps will help to develop a tradition of public service in the technology industry similar to others (e.g. law, medicine, science, and finance)?*

Summary Point of View: Enhance the tradition of public service through intentional design of short-term assignment sprints with the private sector, solving the toughest problems in government, establishment of a trusted talent exchange program with agencies, a joint leadership development program with corporate leaders, and post-corporate career deployments into government via transition programs.

» *What are the key impediments from the private sector perspective to public service?*

- **Bureaucracy:** Perceived, or otherwise. This can limit career impact and career advancement.

- **Perception of low impact:** This perception lingers and proliferates within and outside of government. Most industry IT experts who have succeeded after coming into government, however, state that the mission impact they can deliver is vastly greater in terms of rewards and achievement versus in the private sector. Addressing challenging issues such as immigration or healthcare has been cited as the number one factor as to why they stay; this approach is used as a recruiting tool by agencies.

- **Working environment and attractiveness:** The federal government should consider adopting a more commercial workplace culture, including collaborative workspaces, more flexible hours, and flexible work options, all with the goal of achieving defined output and work deliverables.

- **Recurring administration changes:** Administrations and/or policy can cause instability in mission and perceived job growth and/or security, a reality that requires intervention in perceptions. Establishing comprehensive government-wide change and communications strategy can help mitigate the impact on the federal workforce.

- **Investment in modern technology and procurement rules:** The government needs private sector participation and investment in modern technology to provide cost effective services to the American taxpayers and its public and commercial partners. Current procurement rules limit agencies' ability to buy technology "as a service" and pay for it over a 5- to-10-year period. By leveraging alternative compensation models or partnership with private sector investment agencies can fully focus on their missions and approach IT modernization as a service they buy, not on whether they have funds for a multi-year investment in the current year's budget.

» *How can senior level support (such as CEO or executive engagement) from the private sector build credibility with the path among employees?*

Federal agency leaders could sponsor collaborative exercises with private sector companies to

solve tough challenges facing their government teams. In addition, agencies should consider talent exchange programs and creating a career off-ramp for corporate leaders to transfer their critical skills to government employees.

- Collaborative 'Sprints' with the private sector: This model can be focused on team projects working to solve problems by bringing together private sector talent with federal talent. Joint teams from the private sector and government can complete pro bono projects together to add problem solving expertise, and stimulate further interest in public-private partnership and ultimately public-sector employment.

- Exchange programs between private industry and government: A flexible exchange program can promote collaboration among technical and management experts and leaders in federal government and their counterparts in private industry, and focus collective talent in tackling the toughest technical challenges today facing both sectors.

- Online training. Working with the business community, the federal government should develop a set of online course materials, and mentorships designed to offer skill training and support for existing staff.

Topic 3: *What are the best practices for transitioning and retraining staff working on traditional systems to modern systems?*

Summary Point of View: Upskill the workforce from traditional to modern through the application of cognitive technologies that match inferred skills to requirements by certifying STEM skills, deploying advanced cognitive solutions to retain key skills, and introducing a digital learning platform along with the use of digital skills boot camps.

» *What large scale private sector retraining programs have been successful and how can government learn from them?*

Best practices for talent transformation of existing skills across large organizations include the following:

- **Identify digital skills gaps and propensity to upskill through cognitive tools:** Cognitive tools that match inferred skills to requirements across the government can be used, allowing for the management of gaps through both training and on the job experiences. The private sector has developed cognitive capabilities to help identify those reskilling candidates who have the highest chance of success based on profile, skill adjacencies, and propensity to learn.

- **Certify STEM skills:** Through certification, the organization can identify visible skills gaps and recognize skills impediments to achieving certifications. Digital credentials create a registry of verified skills that the market values most, including cognitive, cybersecurity, agile and design thinking.

- **Digital learning platforms with boot camps:** Learning and retraining is a strategic competitive advantage in private industry and government alike. Many leading private sector firms have institutionalized new digital learning platforms for their employees. Cloud-based solutions provide distributed learning capability anytime and anywhere, through desktop or laptop and fully enabled mobile devices. The private sector also offers external boot camps for candidate selection and employee re-tooling by way of certifying entities. The focus of these activities is on technical skills that have been identified to be successful in the new digital economy.

Talent/Recruiting/Training
Additional Resources

6 Steps to Acquiring & Retaining Talent - Overture Institute

5 Things Successful Companies Do to Retain Top Talent

The Chemistry of High Performance: Understanding the Periodic Table of Elements, Chapter One—Finding People - Oracle

Talent Acquisition Optimization - IBM

IT Alliance for Public Sector
A Division of ITI

Corporate Participants

Associate Participants

A.M. Fadida Consulting
Cyrus Analytics LLC
Hogan Lovells
Jefferson Consulting Group
Orlie Yaniv Strategies
Ralph Chandler & Associates
Rogers Joseph O'Donnell VJA
Touloumes & Associates
VJA Lexis