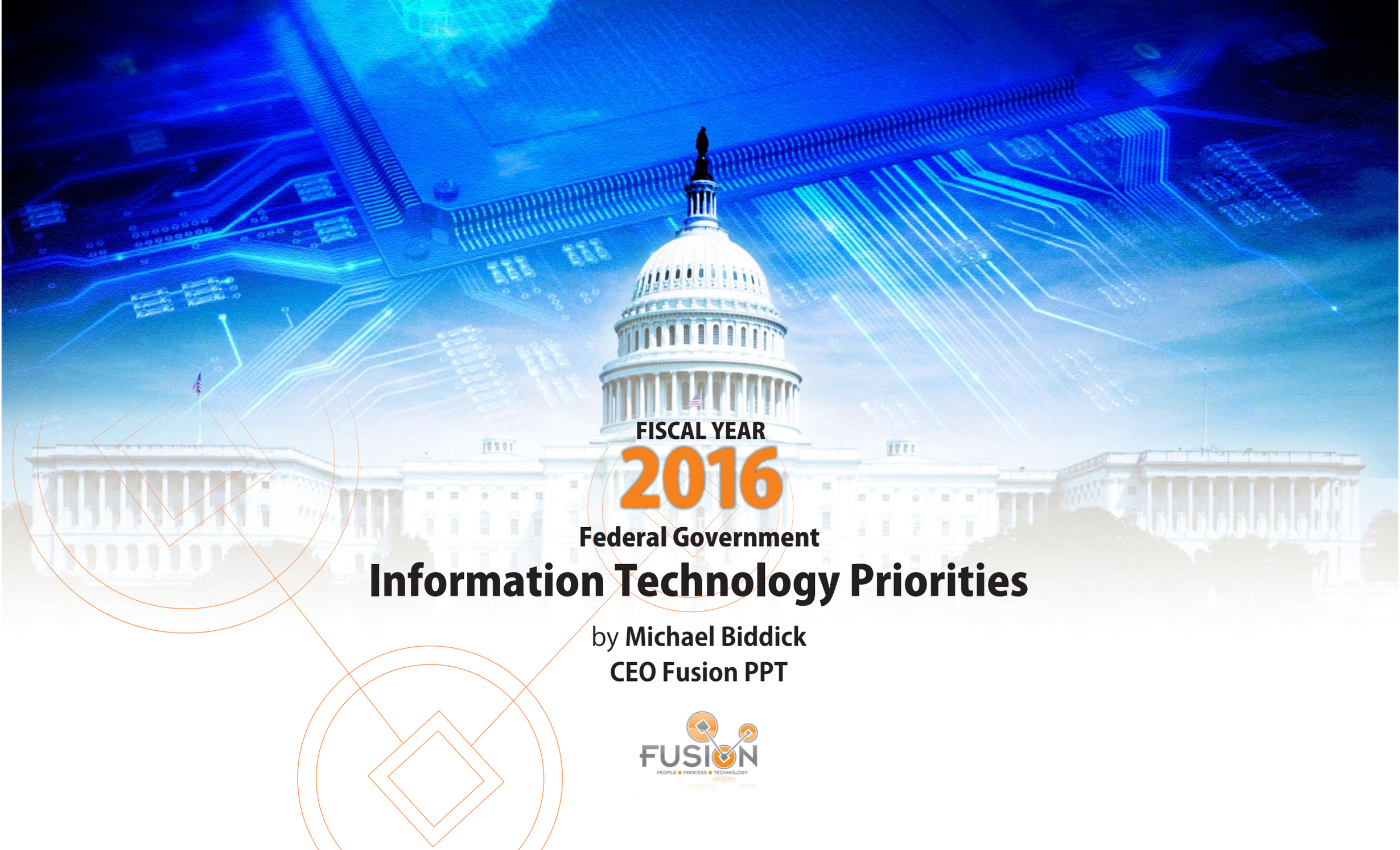


FISCAL YEAR

2016

Federal Government

Information Technology Priorities

by **Michael Biddick**
CEO Fusion PPT

FUSION
PEOPLE ■ PROCESS ■ TECHNOLOGY

Table of CONTENTS

Author's Bio 2

About Fusion PPT 3

The IT Juggernaut 4

Cybersecurity Gets Real 5

The Agile IT Environment 9

Big Data Getting Bigger 10

Cloud Computing 11

The Future of Federal IT 12

Michael Biddick
CEO Fusion PPT

Under Michael's leadership as CEO, Fusion PPT has achieved triple-digit growth becoming the premiere vendor-independent systems integration and consulting partner with their clients. Michael is responsible for the strategic vision, market strategy, project quality and is responsible for the company's overall performance. For nearly 20 years, Michael has worked with hundreds of government and international commercial organizations providing expertise in our Solutions. Michael has a unique blend of deep technology experience coupled with business and information management acumen that provide a balanced approach to our business. Prior to joining Fusion PPT, Michael spent 10 years with a boutique consulting firm and Booz Allen Hamilton, developing enterprise management solutions for a wide variety of both government and commercial clients. He previously served on the academic staff of the University of Wisconsin Law School as the Director of Information Technology.

Michael earned a Master's of Science in Information Systems from Johns Hopkins University and dual Bachelor's degrees in Political Science and Afro-American History from the University of Wisconsin-Madison.

Michael is a contributing editor at InformationWeek and Network Computing Magazines and has published over 50 articles on Cloud Computing, Big Data and Application Performance Management. Michael is also the author of the book "Federal Cloud Computing." Michael holds multiple vendor technical certifications, is a certified ITIL v3 Expert and a certified Barista.

ABOUT Fusion PPT

About Fusion PPT

We Simplify Enterprise IT.

Fusion PPT is an established leader in providing IT consulting and system integration services to organizations with challenging technology initiatives. Since our inception in 2009, we have contributed to the success of hundreds of projects, and most have spanned the globe in their reach and impact. Our ability to perform and add value in complex, diverse, and distributed environments has earned us a solid growth rate and a reputation as a trusted, capable, and results-oriented service provider.

Deep Technical Knowledge, Diverse Project Experience.

Led by veteran IT professionals and thought leaders in the industry, our team has amassed a depth and breadth of technical knowledge and experience that we are passionate about sharing with our clients. We attract and hire only subject matter experts and proven performers, and our culture fosters collaboration, innovation, and a nimble, team-based approach to help our clients achieve their objectives.

Big Firm Expertise, Smaller Firm Service & Agility.

As a privately held small business, Fusion PPT combines the best practices and expertise found at large consulting firms with a nimble, entrepreneurial, and client-focused service team. We reward and encourage fresh perspectives, creativity, and intellectual risk-taking, and this consistently produces more efficient and more cost-effective IT solutions for our customers.

Mission Focused.

At Fusion PPT, we take a partnership approach in all of our engagements, and our team functions as an integral part of the clients' organizations. We understand complex enterprises and the importance of networks, applications, and systems in delivering reliable mission-based services to stakeholders. Our staff is focused at all times on our clients' missions and ensuring that the services we provide and technology solutions we recommend are in complete alignment.

Value Beyond IT.

The "PPT" in our company name stands for "People, Process, and Technology," and it represents a core added value that our team offers – which is a deep understanding of what it takes to make technology investments pay off. Our expertise extends beyond physical and virtual systems. We address the critical success factors of people and process, defining success at the level of organizational impact and the incorporation of new systems into daily work flows and job functions. The fusing together of people, process, and technology is core to our methodology and it is core to technology projects being able to attain their financial and operational objectives.

Fusion PPT Company and Team highlights include:

- ISO 9001:2008 Certified Organization
- Privately Held Firm
- Led by IT Industry Experts and Thought Leaders
- Collaborative Subject Matter Expert (SME) Team Approach
- Agile, Entrepreneurial Staff
- Diverse, Complex Project Experience
- Proven Track Record of Successful Deployments
- Global, Enterprise-Oriented
- Multiple Contract Vehicles
- Depth & Breadth of Technology Expertise
- Commitment to Excellence
- Quality Focused
- Fusion PPT Innovation Lab

Corporate Information.

DUNS: 8307-42-792
CAGE Code: 5H6B4
Primary NAICS: 541611, 541512, 518210
Ownership: Private, 100% U.S
Size Standard: Small Business, under $14M
Certifications: ISO 9001:2008, ITILv3, PMP
D&B Open Ratings: 95% Customer Satisfaction Rating

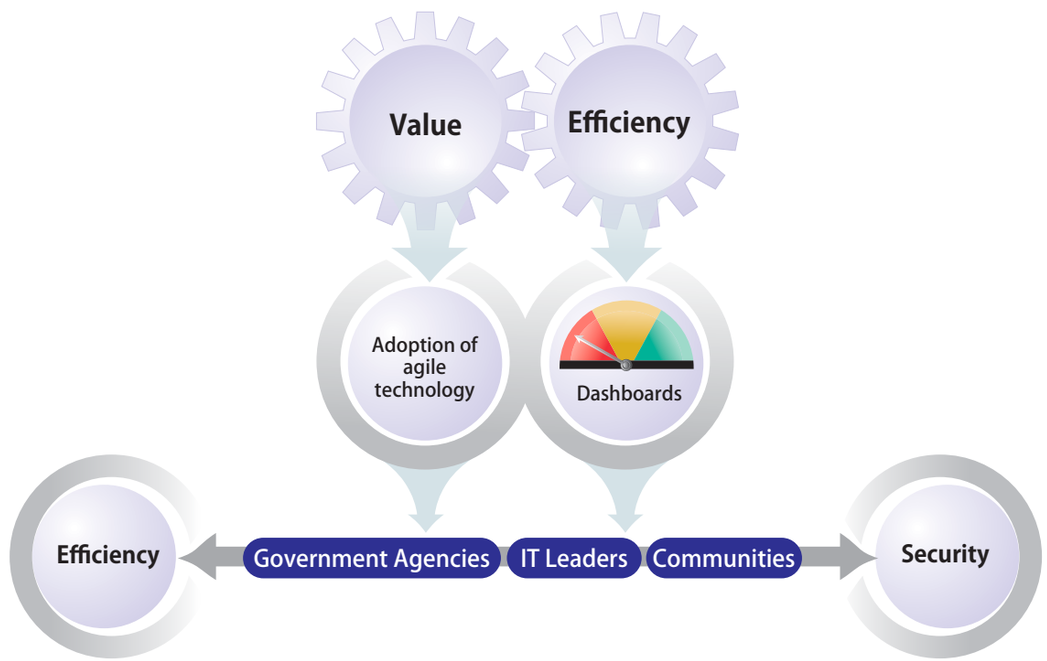
The IT Juggernaut

With the Federal Government IT budget continuing to hover below $80 billion, this February, the president requested a 1.8 percent increase over the $78.3 billion agencies estimate they'll spend this fiscal year – approximately a 10% percent increase over fiscal 2014 spending. At the same time the president released his budget request, partisan groups, legislators and government watchdogs criticized the overall spending on IT and value obtained from this spending compared to private industries.

While legislation and opinions originating from the White House have always focused on more efficient, effective and secure government IT spending, the third appointed Federal CIO, Tony Scott, continued to trumpet bold visions and federal IT transformation. Scott was appointed by President Obama in March of 2015 and explained how "driving value is also about driving efficiency" in his first speech. Some of his proposed ideas included "adoption of agile technologies" and "creating the right kinds of dashboards that will help us understand whether we're making progress or not."

A fundamental question to answer is: Are these bold visions trickling down to agencies and rank-and-file IT leaders within the government and contracting communities? Criticism around spending and efficiency also runs parallel to high-profile security breaches of some of the most sensitive government data reported over the past year. If this security issue is not addressed, breaches will continue to occur and increase in frequency.

In this annual Federal Government IT Priorities report, we'll examine where federal IT leaders should be focusing their time, the key challenges they must address in order to meet an increasingly complex IT environment, and how they can drive innovation across programs.



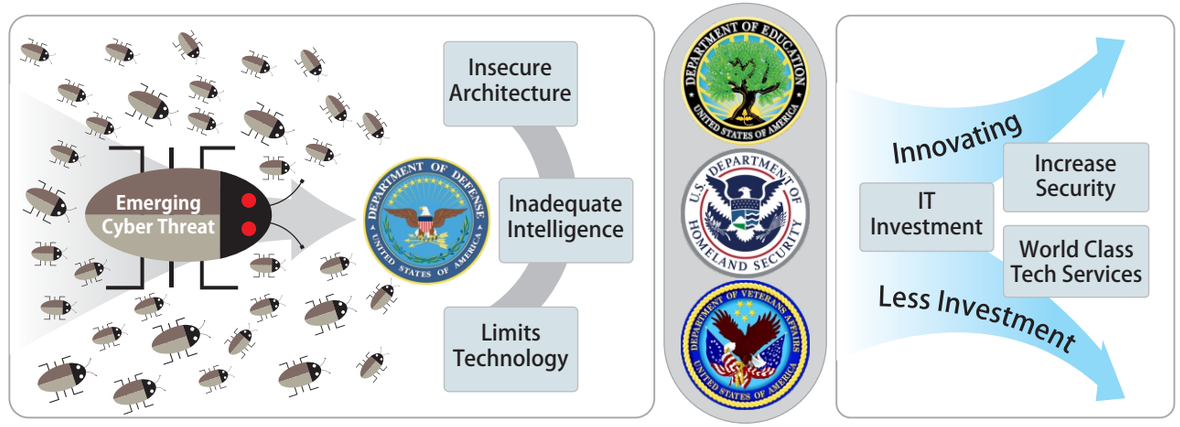
Cybersecurity Gets Real

In 2013, agencies received new guidance from the executive branch in the form of Executive Order 13636: Improving Critical Infrastructure Cybersecurity. This Executive Order warned that "the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." Despite the mandates, some of the most significant cyber security attacks against government data in our time have occurred over the past year.

In June of 2015, the Office of Personnel Management announced the personnel data of more than twenty-one million Americans. The OPM reported that tens of thousands of Standard Form 86s (SF-86) – which are required for all service members and civilians seeking a security clearance – were stolen. The SF-86, a 127-page document, requires information about family members, friends and past employment, as well as details on drug and alcohol use, mental illness, credit ratings, bankruptcies, arrest records and court actions. The OPM indicated that every person who underwent a government background check during the last 15 years was most likely affected.

OPM stated that hackers stole "sensitive information" that included addresses, personal health and financial records and other private details of 19.7 million people who had been subjected to a government background check, as well as 1.8 million others, including the victims' spouses and friends. This theft was separate from, but related to, a breach revealed last month that compromised the personnel data of 4.2 million federal employees, OPM reported.

Other high-profile attacks reported over the past year include the White House network, State Department network, United States Postal Service, GAO and the Healthcare.gov website. Those are only the entities that have been detected and reported. According to a report issued by MerriTalk, the number of cyber incidents reported by Federal agencies to the U.S. Computer Emergency Readiness Team rose from 48,562 in fiscal year 2012 to 67,168 in fiscal year 2014, an alarming 38% increase over two years.



Cybersecurity Gets Real

In a report released in March, The Defense Science Board, a civilian committee that provides scientific and technical advice to the Pentagon, stated that the DOD is not prepared to defend against sophisticated, international cyber attacks. The report pointed to "inherently insecure architectures," inadequate intelligence, and the sheer limits of technology in defending against emerging cyber threats. It encourages the DOD's CIO to work with branches of the military to create an enterprise security architecture that includes minimum standards for ensuring a "reasonable" level of defensibility and increasing the probability that attacks are detected.

Over the last three years, cyber security has rocketed to the top of all priorities for Federal Government IT leaders. No other IT aspect is more important to control than the security of federal data and preventing access to critical command and control systems of critical infrastructure.

To address these significant cyber security concerns, the FY 2016 OMB budget, released by the White House in February, focused on bolstering existing cybersecurity programs and increasing infrastructure agility, while decreasing waste. The budget request included $14 billion to support cybersecurity programs, including “Continuous Diagnostics and Monitoring of Federal systems, the EINSTEIN intrusion detection and prevention system, and Government-wide testing and incident response training to mitigate the impact of evolving cyber threats.”

While an ongoing theme in the budget recommendations was innovating “with less,” some agencies, such as the Veteran's Administration, Department of Education and the Department of Homeland Security, submitted requests for significant budget increases. Evidence-based policy, promoting experimentation and evaluation was also new, but measured in terms of proposed investments. The three major focuses of the budget consisted of increasing value in IT investments, increasing security to protect federal information and resources, and conveying world-class tech services.

Last December, Congressed passed four new cybersecurity bills that the president signed into law. The National Cybersecurity Protection Act of 2014, S. 2519, codifies the Department of Homeland Security's existing National Cybersecurity and Communications Integration Center (NCCIC), which is a focal point for information sharing. The Federal Information Security Modernization Act of 2014, S. 2521, amends the 2002 Federal Information Security Management Act to centralize Federal Government cybersecurity management within the Department of Homeland Security, and also delegates implementation authority for defense-related and intelligence-related information security to the Secretary of Defense and Director of National Intelligence. The third bill focuses on strengthening the Federal Government's cybersecurity workforce and improving hiring procedures and compensation ranges for cybersecurity positions at the Department of Homeland Security, while the last bill mandates an assessment of its cybersecurity workforce every three years, in addition to developing a strategy for enhancing the recruitment and training of cybersecurity employees.

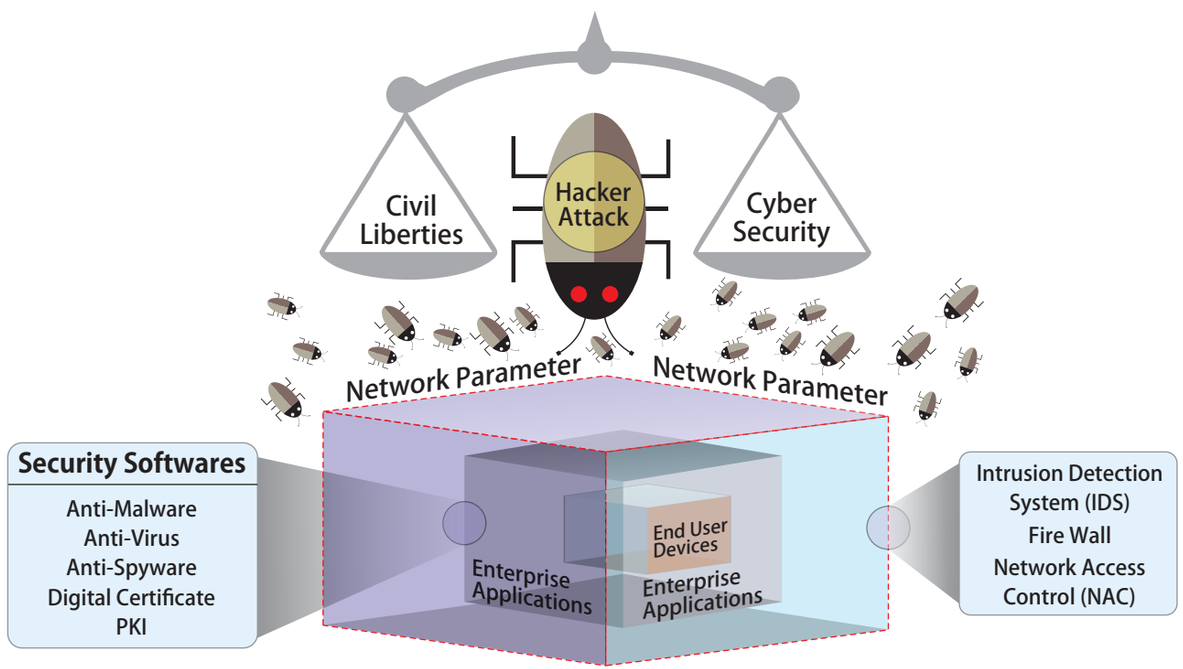
First introduced in April, the Cybersecurity Information Sharing Act of 2015 is currently stuck in Congress and faces opposition from many privacy groups. Within the provisions, it “Permits private entities to monitor and operate defensive measures to prevent or mitigate cybersecurity threats or security vulnerabilities on their own information systems and, with authorization and written consent, the information systems of other private or government entities. Authorizes such entities to monitor information that is stored on, processed by, or transiting such monitored systems.” While legislators and privacy groups try to strike a balance between civil liberties and cyber security protection, hackers continue to succeed in penetrating information systems and

Cybersecurity Gets Real

stealing government data. The plethora of Congressional bills, Executive Orders and management priorities makes cybersecurity not just an objective, but also a national priority. Still, this big-picture priority exists in conjunction with current cybersecurity threats that agency CIOs face on a day-to-day basis. A disconnect remains between lofty leadership cybersecurity objectives and compliance with current certification and accreditation policies and procedures, still mired in bureaucratic processes. It can take up to a year to receive authorization to operate (ATO) from a new system in the federal network. In most cases, these authorizations are still paper-based, with continuous monitoring layered on top.

To effectively address these cyber security threats, government IT leaders need to take several concrete steps to prevent additional security breaches. First, government leaders must rationalize their application and data, and eliminate redundant applications. This is often exercised as a component of an application inventory process. With the right tools, application discovery and dependency mapping can be accomplished in a short amount of time. Second, Enterprise Architecture is needed to align security and application innovation, in order to ensure the appropriate security controls are in place at the enterprise level. Third, investments are needed for continuous monitoring and security tools that test the infrastructure.

One of the most vexing areas for many organizations to tackle is choosing the mix and correctly implementing security tools. We think about three layers of the IT environment that are critical to protect: the network perimeter, enterprise applications and end-user devices. We also work to embed automation to prevent issues, in contrast to simply reporting on issues.



Cybersecurity Gets Real

At the network perimeter, intrusion detection systems (IDS) detect potential threats to the network and can be deployed as network or host applications. The primary responsibility is reporting potential incidents to the security operations team. Network Access Control (NAC) products enforce security policies and handle access authentication and authorization based on their ability to recognize users, devices or their specific roles. IP blacklisting can be effective if very broad, while data loss prevention (DLP) tools can monitor and track issues from potential insider threats. Firewalls, one of our primary security tools, also possess advanced capabilities that include application-awareness features.

At the server enterprise level, security software is needed to protect against a wide range of threats. Anti-malware tools help security administrators identify, block and remove malware. Both anti-virus and anti-spyware software can be deployed to help IT departments focus their anti-malware policies to identify known and unknown malware sources. Newer identity-based security technologies manage authentication and authorization through such methods as digital certificates and public key infrastructure (PKI) solutions.

From an end-user device standpoint, mobile device management (MDM) monitors and controls security configurations, policy enforcement and patch pushes to mobile devices. They can also remotely lock lost, stolen or compromised mobile devices and wipe all stored data, if needed. For desktops and laptops, web browsing policies and anti-virus/anti-malware tools are essential.

The Agile IT Environment

One aspect that makes addressing security more challenging for federal agencies is the complexity of many application environments. The disastrous rollout of the Healthcare.gov site will live on as a lasting example of these shortcomings and complexities. As one response to the shortcomings of the Healthcare.gov project, GSA created an organization called 18F (located on 18th and F Street in Washington, D.C.). This government consulting organization focuses on "lean startup methods, open source code, and contemporary programming languages." One of their key objectives has been to promote the transition from waterfall frameworks to agile ones.

Overall, Agile values interactions over processes, among other things, and time to delivery is quicker. Because small components are completed sooner and stakeholder feedback is received faster, changes can be made in a shorter time frame.

At the end of July, the House Oversight and Government Reform Committee berated the lack of progress agencies have made in making government IT more efficient. Federal agencies are still over budget, behind schedule and making duplicated efforts that waste billions of dollars. Rep. Darrell Issa stated experts estimate as much as $20 billion in Federal IT funding is wasted every year. However, other studies show that waste could be as high as $40 billion compared to private sector spending. While agency IT leaders are faced with balancing this broad range of priorities, congress is struggling to provide effective IT governance across the massive federal bureaucracy.

Earlier this year, Federal Chief Technology Officer Megan Smith highlighted the importance of building large and complex projects, one incremental piece at a time. Speaking to the ACT-IAC Igniting Innovation audience, she noted "Let's not 'spec' the whole huge thing out. Let's do the minimum thing and then get it out there and start iterating with the community.". The General Services Administration released an agile-only contracting vehicle to allow agencies to buy services based on the faster turnaround speed. In contrast to traditional proposal efforts, contractors have been asked to submit examples of code that could be evaluated during the award process.

As agencies work to move towards more agile projects, the key to the approach is using vital elements of Agile; specifically requirements, design and testing, and working collaboratively and simultaneously so that deliverables are produced in a shorter period of time. Development sprints should consist of one- or two-week increments and include a user-functionality test case document. Meetings should be held on a daily basis on all test sites. The most successful agencies will implement Agile as a pilot across a single application or project and further refine it to fit the specific needs of the organization.

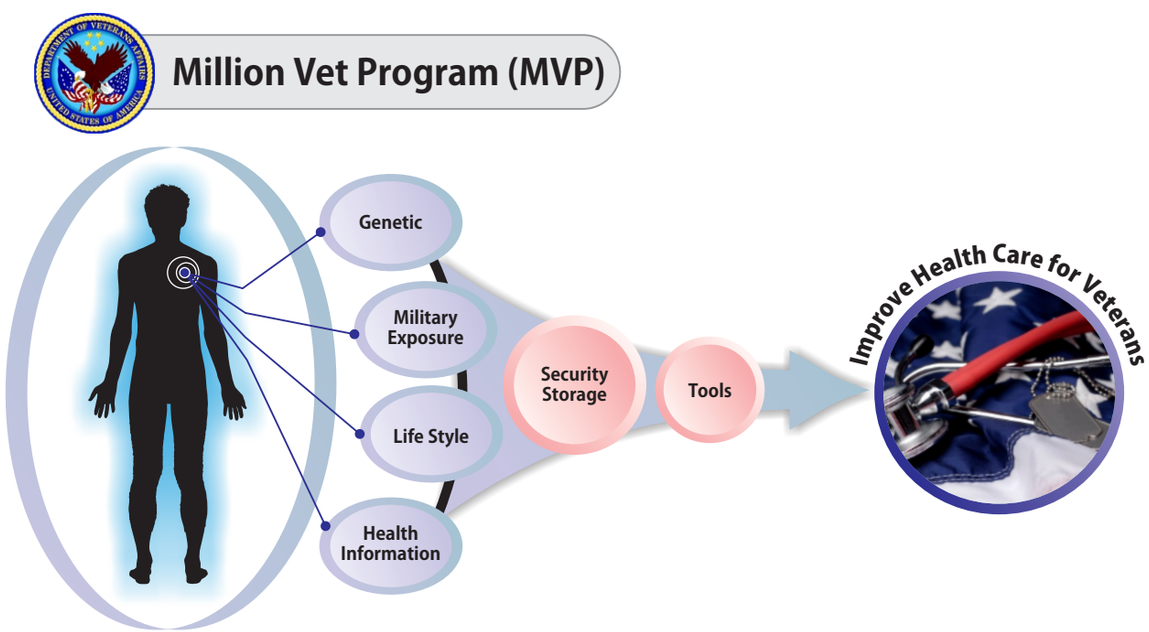
Big Data Getting Bigger

One of the reasons applications need to be delivered faster is to deal with an increasing amount of data that is produced within the Federal Government. Dealing with massive amounts of data is not new. All Federal agencies are responsible for creating and maintaining documentation on their organizations' functions, policies, decisions, procedures and essential transactions. However, a large shift over the past few years has been the desire to make a portion of this data more available to the public, as well as data produced through sensors, cameras and remote monitors that did not exist a decade ago.

The Open Government Initiative (data.gov) offers up datasets to the public that are generated and held by the Federal Government. Data.gov provides descriptions of the federal datasets (metadata), information about how to access the datasets, and tools that leverage government datasets. These data catalogs will continue to grow as datasets are added. Currently, over 140,000 datasets exist online. The government also publishes usage information. For example, over 165,000 people visited data.gov in June and the site averaged 60,000 monthly downloads over the past year.

The Veterans Affairs (VA) Research and Development program launched the Million Veteran Program (MVP) to understand how genes affect health and ultimately improve health care for Veterans. MVP will establish “one of the largest databases of genetics, military exposure, lifestyle and health information.” Aside from processing capability, secure storage and tools to analyze this type of data are needed to ensure that these types of aggressive projects provide value.

At the same time, the VA struggles with basic claim services. For example, at the VA's Little Rock Regional Office, it had “over 1,000 file banks full and overflowing with files and over 102,000 paper files." Director Lisa Breun stated "At the peak, it was taking us⋯over eight months to complete a veteran's claim and a lot of that was because it was paper. We've gone from over eight months to finish a claim to less than four months." That's still a significant amount of time that could be better spent in more critical areas.



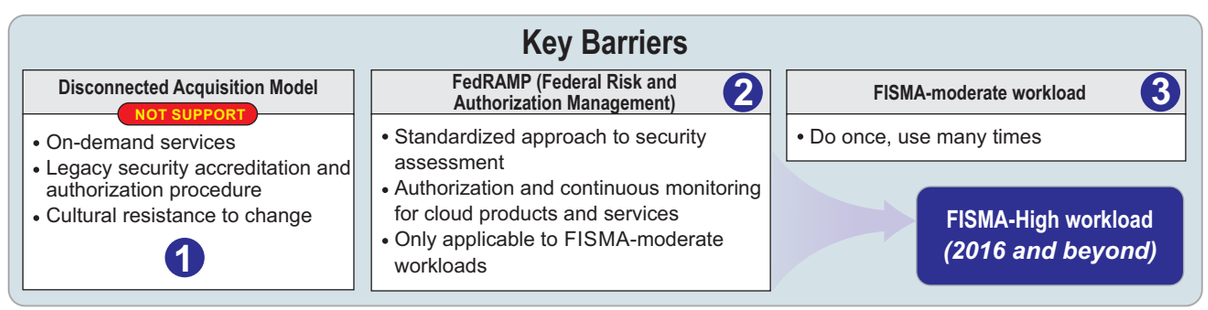
Cloud Computing

The Government's current IT environment has been characterized by "low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times." Delivered correctly, commodity IT services hosted in a cloud computing environment have the potential to play a major role in addressing these inefficiencies and improving government IT service delivery.

Large agencies have more resources, but also a more complex and diverse IT environment. Smaller agencies have simpler IT environments, but far fewer resources. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly and efficiently, despite resource constraints and highly complex environments.

Now over five years old, The Federal Datacenter Consolidation Initiative's (FDCCI) goal is to "reduce the cost of data center hardware, software, and operation, increase the overall IT security posture of the government, and shift IT investments to more efficient computing platforms." Agencies that are participating in the Federal Data Center Consolidation Initiative show an estimated 3,800 data center closings by the end of 2015. These consolidations will free up 1.7 million square feet of land, as well as save $3.3 billion. Many agencies are still struggling to migrate legacy applications that do not support virtualization, and dealing with a skill gap in terms of optimizing virtualized applications. The cost, complexity and political wrangling over who actually controls these applications has made the road to cloud computing a bumpy one.

The three key barriers that persist in greater cloud computing adoption continue to be a disconnected acquisition model that doesn't support on-demand services, legacy security accreditation and authorization procedures, and cultural resistance to change. The key mechanism for addressing this security challenge has been the Federal Risk and Authorization Management Program, or FedRAMP. This program provides "a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services." Currently only applicable to FISMA-moderate workloads, this approach uses a "do once, use many times" framework that saves an estimated 30-40% of government costs, as well as time and staff required to conduct redundant agency security assessments. Currently, the FedRAMP program is drafting standards for FISMA-High workloads to enable more sensitive workloads to exist in public cloud environments in 2016 and beyond.



The Future of Federal IT

While individual priorities can be charted, the reality is that all of these initiatives intersect into a unified IT strategy. From the user perspective, having accessible data, secure applications and a robust infrastructure all are basic functions of government IT. With limited budgets, government IT leaders need to innovate just to survive and handle the increasing reliance on IT. Because government business can't be accomplished without it, IT is no longer a niche for application developers.

While government leaders establish priorities, agency IT organizations are still struggling to provide basic access to applications, support for laptops and commodity IT activities. While many pockets of innovation exist throughout the government, the one-size-fits-all priority list is a challenge for diverse agencies that have different missions, budgets and objectives to serve citizens and their users.

A much more aggressive stance is needed on security, especially in the use of heuristic tools. As the complexity of the security tool environment increases, CISSOs need to consider how the correlation of these data elements can be combined and automated to prevent hacks. A stronger shared environment such as the cloud can strengthen security, as the resources are pooled within a larger community of users. These types of innovation are not only about technology, but center on the deep-seated cultural perspectives of individual agencies.