DIGITAL TRANSFORMATION IN FEDERAL GOVERNMENT

Securely Modernize and Mobilize Government IT to Advance Missions
ACHIEVING GREATER EFFICIENCY AND COST CONTAINMENT

With 80 percent of every Federal IT dollar spent on legacy systems, the Federal IT community is exploring new options to modernize and innovate—virtualization, cloud computing, Flash technology, software-defined options, shared services, and more.1 Concurrently, the always-on demands of a highly mobile government have agencies seeking to effectively balance productivity increases with information security requirements. Key to achieving the new evidence-based goal of running Federal agencies more like businesses are modern technologies that drive efficiency and contain costs.

Across Federal agencies, providing more effective and productive ways for citizens to engage and employees to work now depends on IT agility. The anticipated shrinking of the Federal workforce is expected to place additional pressure on IT leaders to achieve mission objectives while demonstrating value and investment return faster. Moreover, the need is becoming urgent to replace aging systems in the era of increasingly dynamic cyber threats.

“Technology is at the heart of every government program. We’ve reached a point where we need to invest the time and money necessary to transform the way we do business in the government. CIOs, and the rest of an agency’s leadership, need to play a key role in driving this transformation.”

STATE OF FEDERAL IT REPORT
JANUARY 29, 2017

This paper provides guidance about what’s needed to ensure Federal agencies can securely modernize and mobilize government IT to advance missions. It also illustrates how Federal agencies are using VMware solutions to seamlessly transition from legacy IT to modern infrastructure and clouds while continuing to consolidate data centers, reduce time-consuming operations and management (O&M) tasks, enable new modes of digital engagement, and transform cybersecurity.

Accelerate Digital Transformation in Government

Boost Agency Performance and Efficiency + Improve Citizen Service Delivery + Protect Data, Digital Assets, and Citizen PII

Modernize Data Centers + Integrate Public Clouds + Empower Digital Workspaces + Transform Security
FLEXIBLE AND EVOLUTIONARY APPROACH TO ADDRESS CHANGE

Federal data centers, housing an enormous wealth of legacy assets, have been the primary targets for agencies evaluating different cloud computing approaches. Following the 2010 directive to close inefficient and underutilized Federal data centers, many U.S. Federal government agencies turned to server virtualization—and VMware—to reduce their data center inventories.

While achieving optimization and cost savings targets, data center consolidation efforts enabled Federal IT leaders to maintain service-level agreements, secure data and apps, protect information, and support increasing end-user mobility. Today, the Data Center Optimization Initiative recommends cloud services and automated monitoring and management tools as optimal methods of achieving new consolidation, efficiency, and cost avoidance goals.

Recognizing that no Federal agency wants to start over, VMware accelerates digital transformation by enabling unprecedented freedom and flexibility in how agencies build and evolve their IT environments. The VMware Cross-Cloud Architecture™ enables Federal teams to run, manage, connect, and secure any app on any cloud. VMware’s secure digital workspace solutions provide anytime, anywhere, any device access to data and information, improving citizen engagement and workforce productivity.

“We needed to change from a physical, client-server, manual-touch business model to a totally virtualized, cloud-delivered infrastructure-as-a-service model. That would give us a platform on which we could efficiently automate development operations. It’s much easier to manage than separate compute and storage platforms, with all the connection issues that can entail. Having everything visible on one pane of glass is a huge improvement.”

IT DIRECTOR
U.S. FEDERAL AGENCY
During a recent House Oversight Committee hearing, the state of (U.S.) Federal IT was described as “a ticking time bomb.” In some cases, the national IT infrastructure relies on source code that is more than 50 years old. A software-defined data center (SDDC) model provides the foundation for an evolutionary modernization of core platforms that deliver more responsive IT operating models through automation and IT as-a-service capabilities.

Virtualizing Beyond Compute
Agencies can begin an IT modernization and cloud journey with server virtualization based on proven, industry-leading VMware vSphere with Operations Management, which delivers compute virtualization with intelligent operations management. The solution is purpose-built to get the best performance, availability, and security from infrastructure and applications. From there, agencies can evolve to a fully virtualized SDDC architecture—virtualized storage with VMware vSAN, virtualized networking with VMware NSX, and virtualized security with NSX micro-segmentation—at their own pace. VMware’s software-defined solutions enable cost-effective data center modernization that meets the increased demand for agile application delivery, centralized IT management, and strengthened endpoint security.

Broadening IT Automation
VMware vRealize cloud management solutions allow Federal agencies to be both proactive and reactive when it comes to infrastructure changes. VMware solutions broaden IT automation across operations, saving time and removing complexity. With comprehensive visibility through a single dashboard, Federal IT can intelligently pinpoint, analyze, and even prevent potential issues in real time, before they affect end users. With cost metrics at their fingertips, IT teams can make decisions about where to run specific workloads at maximum efficiency. VMware management solutions enable IT teams to continuously monitor IT assets to enhance security, governance, and compliance, as well as better manage the life cycle of all infrastructure.

Running Modern Apps
By modernizing applications, agencies are better positioned to accelerate application delivery and respond to change. With VMware, Federal IT can build, test, and run modern applications through a container-optimized platform purpose-built for cloud-native applications, or deploy on production-grade OpenStack while retaining security, control, and performance of the data center. With VMware solutions, agencies can run critical business applications with high reliability, at lower cost.
INTEGRATING CLOUD

Today, U.S. government agencies are moving to cloud computing and away from their own data centers faster than private corporations. The primary reason is the same as the private sector: better economies of scale. Other reasons include prequalified, or FedRAMP, clouds that make adoption easier and DCIO policy advising, “agencies shall use cloud infrastructure where possible when planning new mission or support applications or consolidating existing applications.”

However, results of efforts to move to the cloud have been mixed—in a recent report, a high percentage of respondents (41 percent) describe their organization’s efforts to migrate to the cloud as mixed, problematic, or non-existent. Yet those initial efforts may not have maximized the value of hybrid cloud.

Embracing Hybrid Cloud

Many agency cloud strategies—depending on operational, mission, and security requirements—include the use of multiple clouds, both private and public. However, managing multiple clouds can be expensive, complex, and less than secure undertakings. VMware supports hybrid cloud architectures, satisfying strict data protection regulations and providing freedom from vendor lock-in.

Whether running on-premises or off, the Cross-Cloud Architecture enables consistent deployment models, security policies, visibility, and governance for all applications. Agencies can deploy workloads on OVH as easily as on Amazon Web Services or IBM SoftLayer.

“VMware provides a migration path for vSphere users today that makes it straightforward to integrate with existing management solutions and to migrate workloads back and forth between a FedRAMP accredited community cloud and their existing private-side cloud environment. Cloud computing and automation technologies are allowing us to do things more quickly, more efficiently, more consistently, more securely than we have ever been able to do before.”

COBY HOLLOWAY
VP CLOUD COMPUTING & BUSINESS TRANSFORMATION, SAIC

Figure 1. VMware Cross-Cloud Architecture
MOBILIZING GOVERNMENT EMPLOYEES

Delivering mobile services is critical to efficient government in the 21st century, and is an integral component of digital transformation. Citizens expect it, and IT administrators need it for efficient operation. VMware has eliminated the trade-offs between enabling on-the-go productivity and maintaining IT control. VMware solutions provide secure delivery and access to applications on any device, from any location, at any time, to advance missions and improve service delivery to citizens.

Secure Digital Workspace for Government
The VMware Secure Digital Workspace for Government—powered by VMware Workspace ONE™—is a transformative end-user computing solution for Federal agencies seeking to modernize IT, strengthen data security, ensure Continuity of Operations (COOP), and mobilize agency workflows to advance missions. It ensures agencies can secure desktops, apps, and devices across the SDDC while adhering to key government data protection requirements.

The Digital Workspace helps prevent the crippling of government agencies in the event of natural and man-made disasters in compliance with the Telework Enhancement Act of 2010 and COOP. These are two examples of ways in which VMware solutions can be used to

• Provide personnel with immediate and flexible access to apps and data anytime, anywhere, on any device.
• Reduce the cost and complexity of desktop management.
• Scale and provision apps quickly, including pushing apps across device fleets and blocking unauthorized apps from an internal app store.
• Speed migration to Windows 10.

Faster App Deployment
VMware solutions also enable government IT to reduce application lifecycle management, delivery, upgrade, and maintenance costs. With a just-in-time model that disaggregates IT-managed applications and user-installed applications from the OS, IT teams can dynamically deliver apps in seconds.

Enterprise Mobility Management is critical for an agency under the U.S. Department of Defense. Realizing that manual data collection was no longer efficient in the disaster response and recovery process, the agency partnered with VMware AirWatch® to secure its fleet of mobile devices and applications—improving response times, service delivery, and mission success.
ADOPTING A TRANSFORMATIVE SECURITY PLATFORM

Combating increasing and dynamic cybersecurity threats is challenging for every agency. Both legacy and evolving government IT environments pose risks. VMware’s end-to-end cybersecurity solutions extend security from the data center to the endpoint device with identity-based access management, network and application micro-segmentation, and real-time detection and enforcement of security-hardening guidelines, configuration standards, and compliance requirements.

A Ubiquitous Software Layer to Combat Dynamic Threats
VMware provides a transformative security platform that enables Federal IT teams to address today’s dynamic threat landscape through a ubiquitous software layer across infrastructure and endpoints, independent of the underlying physical infrastructure or location. The platform provides visibility into interactions between users and apps, and the context to understand them. It also supports the insertion of additional third-party security services for intelligent protection.

Granular Protection with Micro-Segmentation
Legacy models of only securing the network perimeter are inadequate methods of protecting personally identifiable information and national secrets. Once malware has managed to make it inside a data center, it can move laterally from workload to workload. VMware NSX features micro-segmentation that introduces stricter, micro-granular security—isolating networks from one another and automatically applying appropriate security policies down to the app level.

End-to-End Security
VMware AirWatch unified endpoint management solutions integrate identity, application, and enterprise mobility management to safeguard data across any device or application—including native, web, remote, virtual, and Windows desktops. Identity-based conditional access and role-based policies allow for control of entry points and interactions across apps, devices, and locations. Federal IT teams can protect and encrypt data in transit and at rest, support two-factor authentication across web, cloud, and native apps using CAC and PIV cards, derived credentials, certificate-based login, biometrics, and third-party authentication services such as Symantec and RSA SecurID, and maintain compliance across the infrastructure.

VMware solutions support U.S. government authentication and security requirements, including CAC and PIV card access, Common Criteria, FedRAMP ATO, FIPS 140-2 compliant 256-bit SSL encryption, and DISA STIG for mobile device management.

Figure 3. VMware’s ubiquitous software layer across infrastructure and endpoints
TEAMING WITH VMWARE TO SECURELY MODERNIZE AND MOBILIZE

Fragmented and siloed legacy infrastructure and processes have served Federal agencies for decades. Today, they inhibit innovation and challenge data security. VMware offers a pragmatic, value-added path that helps Federal agencies securely modernize and mobilize IT. VMware is poised to continue to help government IT achieve efficiency and cost containment objectives with cloud infrastructure and digital workspace solutions that drive digital transformation.

Capital and Operational Savings
VMware virtualization technologies have saved organizations billions of dollars in capital expenses. With the software-defined data center, VMware is reimagining data centers by extending the paradigm of resource abstraction to all infrastructure domains, across on-premises and public cloud environments, while the digital workspace improves employee workflows, driving the digital-first agenda.

Digital Transformation Acceleration
VMware solutions help government agencies evolve—accelerating agility, streamlining infrastructure management, adopting modern approaches, and furthering innovation—all while keeping information secure.

Learn more
www.vmware.com/government

2. Government Computer News. “Can We Afford Not to Innovate?” March 10, 2017
Learn more
www.vmware.com/government