Boosting Telework in the Federal Government

How VMware Workspace ONE empowers federal agencies to meet performance, cost savings, and emergency preparedness goals

VMware Workspace ONE empowers remote workforces with a digital workspace experience that delivers access to any app on any device without compromising security.

Telecommuting eligibility in the Federal Government has continued to rise since the signing of the Telework Enhancement Act in 2010. According to the sixth status *Telework Report to Congress*[1], since the Act's signing approximately 43 percent of federal employees are eligible to telework.

As agencies continue to adopt this strategic organizational program to modernize government and meet not only performance and cost savings but also emergency preparedness goals, they need a strategic IT partner with both technology capabilities and deployment expertise to help. VMware Workspace ONE® provides secure access to SaaS, web, mobile, and virtualized applications and desktops to enable government employees to securely access the applications they need from any device, and any location.

Securely Modernizing and Mobilizing Government

VMware accelerates telework plans and service delivery by integrating access control, application management, and multiplatform endpoint management to deliver a consistent digital workspace available from agency- or employee-owned devices. Workspace ONE is an intelligence-driven digital workspace platform that empowers federal employees to securely access government resources, data, and applications anytime, anywhere, and on any device—transforming workflows and advancing missions.

1. U.S. Office of Personnel Management. "Status of Telework in the Federal Government Report to Congress, Fiscal Year 2018."

vmware®

"Based on a very conservative estimate, the federal telework program is likely saving taxpayers over $800 million a year."

KATE LISTER, PRESIDENT OF *GLOBAL WORKPLACE ANALYTICS*, A RESEARCH-BASED CONSULTING FIRM [WHOSE *TELEWORK SAVINGS CALCULATOR* WAS VETTED BY THE GAO IN A 2016 REPORT TO CONGRESS]

Workspace ONE features simple, single sign-on (SSO) access to cloud, mobile, web, and Windows apps in one unified catalog, and includes powerfully integrated email, calendar, file, and social collaboration tools that engage employees. Agencies can confidently empower government workers to use their personal devices or agency-provided devices, with IT enforcing fine-grained, risk-based conditional access policies that also take into account device compliance information—delivered by Workspace ONE Unified Endpoint Management (UEM) technology.

Workspace ONE automates onboarding including laptop and mobile device configuration, and delivers real-time application lifecycle management that bridges legacy client-server apps to the mobile cloud era. The platform is powered by VMware Workspace ONE® Intelligence and uniquely combines workspace data aggregation and correlation to deliver integrated insights and automation that help agencies manage complexity and security without compromising workforce experience.

Ramping Up Government Workforce Productivity and Security

In addition to supporting agencies complying with the Telework mandate, Workspace ONE is an ideal approach for agencies to adopt a remote-first culture while gaining the following benefits.

Improved onboarding and employee experience

Driven by the *President's Management Agenda*, government IT is currently executing on a multi-year plan for building and maintaining a modern, secure, and resilient technology foundation. This plan addresses the challenges of attracting and retaining the best talent, improving service delivery to achieve mission outcomes at optimal cost, and reducing cybersecurity risk.

From special access cards—also known as personal identity verification (PIV) cards—for physical building access to multiple layers of authentication protocols for data access, government employees face a variety of productivity hurdles on a typical day. The approach an agency takes to onboarding employees can directly impact their willingness to stay, and be crucial to hiring and retaining the best talent.

A recent *Digital Employee Experience survey* by Vanson Bourne for VMware reveals that as much as 73 percent of respondents across industries worldwide strongly agree that flexibility of tools (technology, apps, and devices) that they use at work would influence their decision to apply for or accept a job. It's hard to imagine government workers would be any different. In a world where agencies are now directed to become more competitive with commercial enterprises for employees, agencies will have to match, or even exceed, the employee experience offered by alternative prospective employers.

Day One is a new hire's first impression of working life at an organization—offering a glimpse into its structure and culture. Agencies can spur excitement and build loyalty from the start by providing both new and current employees with seamless access to resources, teammates, and required training and documentation.

Streamlined COOP and DCOI compliance

Federal agencies can leverage digital workspaces to improve Continuity of Operations (COOP) plans to ensure that essential federal functions continue during emergency situations. With Workspace ONE, an agency can get a head start in ensuring that the availability of desktop and application services for employees is never affected by disasters or during times of uncertainty when employees can't get to offices. With critical services hosted in data centers or the cloud, an agency can permit users to access desktops and applications from anywhere, anytime. Because the solution has

COOP and business continuity/disaster recovery (BCDR) capabilities built in, it serves as an everyday testbed for COOP, eliminating the need for agencies to frequently test the infrastructure for disaster recovery.

Moreover, the VMware digital foundation includes cost-saving virtualization technology that helps agencies dramatically reduce the number of data centers they need, in compliance with The Data Center Optimization Initiative (DCOI), which requires agencies to optimize and consolidate data centers to deliver better services to the public while increasing return on investment to taxpayers.

Increased employee productivity

Individuals with access to telework are more engaged, more satisfied with work, and more likely to remain at their agencies than employees who are unable to telework, according to 2017 Federal Employee Viewpoint Survey (FEVS) data. Telecommuting also cuts the cost of lost productivity.

According to the most recent Telework Report, agencies are seeing these employee-related benefits:

- 63 percent of respondents attribute telework to an increase in performance
- 65 percent of federal teleworkers have an increased desire to stay at their agency due to the policy
- Securities and Exchange Commission (SEC) saved $870,000 per year in transit subsidies[2]

Zero Trust is a modern security approach that eliminates the concept of implicit trust and considers all resources external.

Workspace ONE enables agencies to maximize employee engagement and productivity by providing a personalized experience and Day One access to any app on any device. Agencies can boost productivity and delight employees with secure, password-free SSO access to the wide variety of applications deployed today and those planned for tomorrow—SaaS, mobile, Windows, virtual, and web apps—on any phone, tablet, or laptop, all through a single app catalog.

Moreover, IT staff can aggregate and correlate data across the entire digital workspace to *drive insights, analytics, and powerful automation* of common IT tasks that improve user experience, strengthen security, and further reduce IT cost.

Enhanced security

Security concerns are among the top reasons agencies are slow to adopt telework. Sensitive data must stay secure as it travels beyond agency firewalls. VMware Horizon® 7 virtual desktops keep all data, including desktops and applications, inside the agency data center without storing any data on the user's endpoint.

Government data is among the most targeted for cyberattacks, coming under ever-increasing threats from nation-state actors, according to the *2020 Cybersecurity Outlook* Report by VMware Carbon Black. A recent investigation by the Associated Press also reveals hackers targeting U.S. defense contractors with complex phishing attacks against employees working on some of the most forward-leaning, advanced technologies.

Security infrastructure in most agencies was developed in a perimeter-bound environment—where everything (users, devices, and applications) inside the network was treated as trustworthy. That's no longer effective in today's diverse IT environment. Government workers may be increasingly moving beyond government buildings; applications may reside on government or public clouds, not on-premises data centers; and employees may be using a wide variety of personal- or agency-

2. Forbes Media LLC. *"Trump Versus Telework: Federal Policy Retraction Will Cost Government Millions."* Laurel Farrer, 2020.

owned mobile devices. In this environment, the idea of implicitly trusting users, apps, or devices no longer applies.

A modern security approach, Zero Trust eliminates the concept of implicit trust and considers all resources external. It relies on continuous verification of devices, users, and apps before granting access to government resources. Agencies can require two-factor authentication for employees trying to gain access to information from smart devices, while contractors may be approved for application access through desktop and application virtualization technology to ensure that sensitive information does not reside on endpoints.

Agencies also can require personal devices to register with IT to ensure that basic security hygiene, such as patch levels and passcodes, can be established. Agencies can adopt bring-your-own-device (BYOD) policies that require agency personnel to manage all devices. With a new Zero Trust approach to security, government agencies can dramatically reduce the risk of a data breach and data loss as a result of hacked or phished credentials or through malware that exploits older or unpatched systems.

Workspace ONE combines intrinsic security across devices, users, and apps to simplify the enablement of Zero Trust access control. Industry-leading modern management enables IT staff to ensure that device compliance requirements, including patching and endpoint security settings, are met. Auto-remediation of non-compliant devices ensures workers have the opportunity to meet compliance standards and continue to access agency resources.

Risk-based conditional access policies can enforce multi-factor authentication (MFA) for access to the Workspace ONE application catalog with the ability to require step-up authentication for high-risk applications. Integration with device compliance policies enables device trust information also to be factored into the access policies. Desktop and application virtualization enable employees and contractors to remotely access an agency-managed virtual desktop from anywhere, on any device. As each desktop runs in the agency data center, no information is stored on endpoint devices, keeping agency information secure.

VMware Workspace ONE Is Telework Ready

Workspace ONE empowers the digital workspace for federal employees, supporting numerous standards and directives:

- Secure anywhere, anytime access from any device for all desktops and applications.
- Supports all federal standards and regulations governing telework, including Personal Identity Verification (PIV), Department of Defense Common Access Cards (CAC), and SIPRNet Hardware Token access cards. Authentication options vary based on customer's specific configuration. For more information on security certifications, visit *https://www.vmware.com/security/certifications.html*.
- Supports NIST 800-53 with FedRAMP Moderate and DISA IL 2.
- Can assist organizations with Homeland Security Presidential Directive 20: National Continuity Policy (HSPD-20) for Continuous Operations.
- Certified to Common Criteria EAL 4+ for VMware vSphere®.
- Enhances organization COOP plans.
- Supports the President's Management Agenda to attract and retain top talent.

LEARN MORE

Contact *VMware Federal* to learn more about how your organization can deploy VMware Workspace ONE to meet performance, cost savings, and emergency preparedness goals in compliance with the Federal Telework Enhancement Act.