



GOVERNMENT

Telecommuting and the Federal Government

What's driving government telework

Telecommuting or telework has been gaining momentum as a leading employment practice at all levels of government: federal, state, county and municipal. Four trends are driving adoption in government:

- **Legislative mandates:** Public Law 106-346, passed in 2000, requires that all federal Executive agencies to establish policies that allow telecommuting "to the maximum extent possible without diminished employee performance."
- **Public attitudes:** Public policies urge governments to "go Green" to cut carbon emissions and commute miles.
- **Disaster planning:** Agencies are required to prepare for disasters, with Continuity of Operations (COOP) plans to keep key governmental functions running in a disaster.
- **Financial benefits:** Telework can be a cost-effective way to reduce government expenses, particularly in leasing office space for government workers.

In addition, the 2009 stimulus package will boost government employment, especially in federal agencies. That means more space to house more workers—unless agencies encourage telework as a cost-effective alternative to leasing more office space. Indeed, in 2007 a CDW Government study found telework adoption in the Federal government outpaces private-sector adoption by a 3-1 margin.

The same economic conditions that spurred the federal recovery plan are squeezing state and local governments in a different way. When Utah's governor in August 2008 announced a four-day work week for most government

agencies, he cited energy consumption, employee recruitment and retention, and reducing the environmental impact of state government in the one-year trial.

However, other cash-strapped states are exploring shortened weeks as a way to save money, both for themselves and for state workers who save 20% of commute costs by working a day fewer. In California, the governor closed certain state offices two Fridays a month in a cost-cutting move, reducing employee pay as well as work days.

Pioneers go beyond the basics

Beyond these broader trends, individual agencies are adopting telework programs with multiple motives. Seeking savings on real estate and greater efficiency, Loudoun County, Virginia, has issued notebook PCs to building inspectors to allow them to handle inspection duties without returning to the office. When current leases expire, the county hopes to save money by leasing less office space. Loudoun County uses SonicWALL® virtual private network (VPN) for security.

During the congestion and interruption of the 2008 Republican National Convention in Minneapolis, Hennepin County government maintained "business as usual" operations by relying on its telework program.

In Washington, D.C., the U.S. Patent and Trademark Office saved on office leasing while it went on a hiring binge in 2006-07, adding 1,200 examiners. Instead of leasing a ten-story office building to handle the new workers, USPTO counted on its telework program, one of the most successful in government. Among the 54% of USPTO employees eligible to telework, almost 83% do so, many full-time. USPTO also

Champions of Telework Use SonicWALL

In Loudoun County, secure remote access for building inspectors is only part of a larger telework program. Using SonicWALL technology, the county's telework program by September 2008 had more than 430 workers (some 18% of those eligible) participating an average of two days per month. The county has upped the goal for 2010 to 25% of employees teleworking 2.5 days per month.

The county found in 2006 that turnover rate among teleworkers was 10.4% lower than the overall county turnover rate, and teleworkers averaged 5% less unscheduled leave than the average. The county's telework program is estimated to save 125,300 vehicular miles traveled and 3,676 hours of commuting time each month. To support its telework program, the county is switching to laptop computers.

The Internal Revenue Service, another SonicWALL customer, first implemented a telework program known as "Flexiplace" in 1995. By 2006, it had grown to an estimated 28,000 participating employees, with a goal of 40,000 teleworkers. The system added a broadband option (previously it supported only dial-up) and saw costs drop \$9.5 million as participation continued to grow.

The IRS also reported telework produced real estate savings and proved a plus to recruiting, especially younger workers. The IRS telework operation proved its value in 2006, when flooding closed IRS headquarters for six months. Telework contributed to keeping agency operations up and running during and after the incident. An IRS report said that issuing more laptops to employees would have lessened the flood's impact even more. The IRS also contracts with an outside agency for up to 350 disabled call center agents who work from their homes.

SonicWALL customer General Services Administration (GSA), in its role as landlord for many federal agencies, is also a key promoter of telework. The agency oversees 14 drop-in telework centers in the greater Washington, D.C., area for both federal and private sector employees. GSA also has an aggressive goal of having 50% of eligible employees telework by the end of 2010; in November 2008, the figure was 38%. GSA had to negotiate with its employee unions on the terms of its telework program.



adopted a practice dubbed “hot desking” or “hoteling” by keeping 200-plus desks for teleworkers to use on required office visits.

Security tops technology requirements for telework

Security that allows remote workers to access government applications and data through an Internet connection is a key element in any telecommute program. Secure remote access is best provided by virtual private network (VPN) based on the SSL standard. SonicWALL provides a line of SSL VPN products for different sizes of installation. Some federal agencies have VPNs based on a different technology called IPsec, which has certain downsides for large telework programs.

Security also must extend to the teleworker’s site, particularly if the employee is using a wireless network. For greater security, many agencies require employees to use an agency-issued laptop, though a secure home computer may suffice for some agencies.

Other technical requirements include broadband Internet access and electronic (not paper-based) workflows for work processes that can be executed remotely. Many teleworkers already have monitors, keyboards, fax machines and scanners at home to use for telework.

For telework, hosted applications (Software as a Service) provide certain advantages, since the same application is used in the agency offices or the home office. Teleworkers may require additional technical support from the agency help desk, although some agencies are using “virtual desktop” technology for remote support. While not required, Web conferencing and collaborative applications help teleworkers work efficiently and remain in the office flow.

Telework piggybacks on Continuity of Operations

Most government agencies have Continuity of Operations (COOP) plans to keep essential services operating in a disaster, such as severe weather conditions. These often-mandated disaster recovery programs come with funding. Fortunately

“Significantly, the number of agencies who have integrated telework into Continuity of Operations (COOP)/emergency planning increased to 60 percent, up from 42 percent in 2006. This improved level of readiness will be critical to the country to help avoid significant disruptions in essential government services during emergency situations.”

Office of Personnel Management,
2007 report on telework in government

for telework, the same secure remote access technologies that power COOP also can be used for telework. Disaster recovery requires frequent testing to be sure both equipment and personnel are operational, and a telework initiative can serve as an every-day testbed for resiliency of COOP.

How agencies gain from telework

The greatest opportunity for savings from telecommuting is in lower costs for real estate and operating costs of government offices. Agencies also gain workforce benefits from telework. Studies find higher retention rates for teleworkers, and thus lower agency training costs for new employees. The National Association of State Chief Information Officers found that the telework option aids in recruiting younger (Gen Y) workers.

Some studies reveal that telework boosts productivity, although the evidence is anecdotal, not conclusive. The National Science Foundation, which runs a major telework program, found that 87% of managers who supervise teleworkers said in a survey that teleworkers’ productivity increases or stays the same.

Other agency benefits include lower absenteeism and greater job satisfaction. In addition, telework can accommodate workers with disabilities.



Lower commute costs, lifestyle gains benefit workers

Telecommuters cut their commute costs, pocketing funds to spend in more satisfying ways. The flexibility of telework—drop the kids at school or work after they go to bed—provide greater work-life balance and control of their time for teleworkers.

The challenges of telework

Isolation from colleagues is one downside of telework, depending on how both the telework and office culture adapt. Middle managers often fret about managing remote employees—indeed, that's the top concern for agencies, according to research by the Telework ExchangeSM, a public-private partnership focused on telework. Training for managers and teleworkers helps facilitate the shift to goal-oriented management. Online training is available for both managers and teleworkers. Government supervisors also have seen complications arise in working with employee unions, but the largest independent union of federal employees, National Treasury Employees Union, has backed telework legislation. One issue: The power to choose the jobs and employees for telework.

How SonicWALL cleans up telework with Clean VPN

SonicWALL delivers dual protection for telework based on its Clean VPN approach to security. It delivers not only secure SSL VPN remote access but also protects the integrity of VPN traffic with high-performance Unified Threat Management (UTM). A SonicWALL Clean VPN allows agencies to safely extend their networks for anywhere, anytime access and thus increase productivity, collaborate with Web 2.0, efficiently manage workforce shifts, reduce operational costs and work green.

Telework and other remote access activities expose the network to network hacks that can compromise security. In addition, VPNs are also subject both inbound malware attacks and outbound data leaks, as teleworkers and other remote users increasingly work on personal laptops, mobile devices, home PCs or public Internet kiosks at airports or hotels outside the direct enforcement of IT policy. By securing the integrity of both VPN access and VPN traffic, the SonicWALL Clean VPN offers necessary defense-in-depth protection to control access based on how trust is established for users, their devices and the traffic itself for a truly secure remote access.

To protect applications and resources against unauthorized access, SonicWALL Clean VPN uses enforced authentication, data encryption, granular access policy and gateway threat protection. It then connects authorized users with appropriate resources seamlessly and in real time based upon device interrogation, user authentication and access policy, while employing an access method and interface appropriate to the specific endpoint.

SonicWALL Secure Remote Access

SonicWALL Secure Remote Access offers government organizations and agencies uninterrupted network access during times of natural disasters, terrorism, fires, power outages, etc. These SonicWALL SSL VPNs (virtual private networks) offer secure remote access to mission-critical resources from virtually any end point, a key requirement of telework.

- **SonicWALL Aventail E-Class SSL VPN Series**
- **SonicWALL SSL VPN Series**
- **SonicWALL Virtual Assist**

NSA Network Security/Unified Threat Management

SonicWALL delivers comprehensive anti-virus, anti-spyware, intrusion prevention protection and application control over internet, extranet and internal government networks.

- **SonicWALL E-Class NSA Series**
- **SonicWALL NSA Series**
- **SonicWALL TZ Series**

For more information on SonicWALL's broad range of simple, cost-effective security solutions designed to improve network efficiency, please visit our Web site at www.sonicwall.com.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

