CYBER SECURITY
INDUSTRY ALLIANCE

Telework: Get the Facts

August 2006

Telework: Get the Facts

What is "telework" and who uses it?

Telework provides flexibility in locations where employees may perform their jobs and allows them to work at home, at an alternative office or other location. It is also called telecommuting, flexiwork, flexiplace or enabling a remote workforce.

Developed in the early 1970s, telework is widely used in private industries. Telework is popular with employees because it frees them from the drudgery of commuting and provides flexibility for personal activities. Employers also like telework because it helps to keep workers happy, increases productivity, reduces overhead and saves money. Society also benefits from reduced traffic congestion and pollution.

For the government, the most important benefit of teleworking is that it can greatly facilitate continuity of operations in times of crisis. Adoption of telework in the federal government began in 1990 and is on the upswing, but it seriously lags behind private industry.

What are the benefits of telework?

The benefits of telework are well documented. OPM described the benefits for workers and employers in its May 2003 study, *Telework: A Management Priority – A Guide for Managers, Supervisors, and Telework Coordinators*. This well-researched and documented report cites numerous benefits, including:

- Reduction in turnover by average of 20 percent
- Lowers absenteeism by 60 percent
- Potential savings to agencies of up to $10,000 per employee per year in reduced absenteeism and retention costs
- Boosts productivity up to 22 percent
- Enables compliance with Clean Air Act, the Family and Medical Leave Act, and Americans with Disabilities Act
- Top recruiting tool valued by prospective employees

Why doesn't the federal government use telework more universally?

The federal government has made little progress on telework despite fifteen years of pilot programs, presidential directives, legislative mandates and even the threat to cut funding for substandard efforts. The most recent U.S. Government Accountability Office (GAO) study of telework in May 2004 stated that the percentage of eligible federal employees teleworking did not increase between 2002 and 2003, remaining at about 14 percent (see GAO-04-950T). In contrast, the number of American employees who performed any kind of work from home grew from 41.3 million in 2003 to 44.4 million in 2004 – or 7.5 percent – according to a survey by The Dieringer Research Group.

The 2004 GAO report cited several obstacles to teleworking, but none involved technology:

- Lack of full funding to meet needs of telework programs
- No eligibility criteria established for teleworkers
- Lack of support from top management
- Resistance by managers (especially mid-level managers who insist on having staff physically present when they work)
- Lack of training and information on telework programs

What are the biggest telework obstacles for the federal government?

Two major obstacles within the federal government stand in the way of expanding telework:

- An agency that saves money by reducing overhead expenses must return these savings to the federal treasury
- Some managers prefer to have employees in the same physical location

The structure of the federal budget – not technology or management – is one of the biggest obstacle to the expansion of telework. There is little incentive for agency leadership to adopt telework because any savings resulting from it must be returned to the federal treasury and cannot be applied elsewhere in the agency's operations. Enabling agencies to realize such savings appears to require intervention by the White House's Office of Management and Budget (OMB) and possibly a change to current law.

How can telework help with the continuity of operations?

Ensuring the continuity of key government operations for an extended period is a central responsibility of the government; however, the reality is that today's contingency plans are only designed to withstand a few days. Essential government services can be interrupted by a range of events, including a terrorist attack, severe weather or a health pandemic. The ability for employees to work at alternate or virtual locations is key to ensuring continuity of operations (COOP) in emergency situations.

This is not just a simple case of severe weather and power outages causing employees of one agency to telework for a few days while systems come back online. For example, the potential impact of a flu pandemic is well-publicized, estimated by the White House to take as long as 18 months to run its course. During this time, employees will be unable to report to their offices due to office closures, quarantines or because they must stay at home to care for family members. The public will need timely, reliable information about ongoing developments and the medical community must have access to secure, reliable communications to ensure that they are able to save as many lives as possible. The federal government must be prepared for COOP in the event of such a long-term scenario. In addition to developing a telework plan, it is crucial that agency employees regularly use – and are comfortable with – the system before crisis strikes, ensuring a more seamless COOP when it is most needed.

On May 11, 2006, the GAO issued a report on COOP (GAO-06-713) that found that federal agencies lacked specific guidance on how to prepare to use telework during a COOP event and as a result, were ill-prepared to do so. The GAO pressed the Federal Emergency Management Agency (FEMA), which is responsible for overseeing and assessing the status of COOP capabilities of federal executive branch agencies, to coordinate with OPM to develop guidance on the steps that agencies should take to adequately prepare for the use of telework during a COOP event. FEMA has been receptive to some of these recommendations.

What legislation has been passed to require the federal government to implement telework policies?

Telework was first introduced in the early 1970s. A statutory framework for telework in executive branch agencies of the federal government was created in 1990. It included requirements for agencies to take specific actions, provided tools to support telework, and designated leadership roles by the Office of Personnel Management (OPM) and the General Services Administration (GSA). OPM and GSA operate the Interagency Telework Web site at www.telework.gov, which provides telework guidance for employees, managers and agency coordinators.

Additional statutes were passed in the 1990s. The most significant legislation was passed in 2000 (P.L. 106-346), which included a provision by Rep. Frank Wolf (R-VA) in Section 359 that required each executive branch agency to establish a telework policy "under which eligible employees of the agency may participate in telecommuting to the maximum extent possible without diminished employee performance." It was largely ignored by agencies.

In 2004, Rep. Wolf added an enforcement provision (P.L. 108-477) in Section 622 that would dock $5 million from the respective FY '04-'05 budgets of six agencies if they did not meet minimum standards for telework. In September 2005, GAO issued a report on *Agency Telework Methodologies* (GAO-05-1055R) that reviewed five of these agencies (one was dropped from the list) to certify that telecommuting opportunities were made available to 100 percent of the eligible workforce. The findings were varied and inconsistent, resulting in a GAO recommendation that Congress should determine ways to promote more consistent definitions and measures related to telework and also continue to encourage agencies to promote telework. To our knowledge, Congress has not taken action in pursuit of these recommendations.

Are there any telework success stories in the federal government?

There are some federal success stories. Employee unions have praised telework programs at the Internal Revenue Service, the Trademark Division of the Patent and Trademark Office, the Federal Communications Commission, and the Tax and Trade Bureau of the Treasury Department. But overall, federal efforts to adopt telework have lagged behind the private sector.

Are there real strategies to help agency managers to make it work?

OPM's *Telework Works: A Compendium of Success Stories* profiles thirteen case studies of employees who teleworked at least one day per week in a variety of job positions. There were three common threads for success:

- Managers were willing to experiment
- Motivated, self-starting employees initiated their entry into telework, worked out details and approached supervisors with a specific plan
- Managers and employees agreed on clearly defined expectations before starting a telework arrangement

On August 3, 2006, OPM released new rules to guide managers and employees involved in telework programs. Although general, the guidelines emphasize the need for good communications between managers and employees and the importance of establishing expectations and performance management practices.

Will telework compromise the security of federal agencies?

Security is not the issue and should not prevent adoption of telework. Although most incidents that compromise sensitive information stem from weaknesses in human-based systems, proper security technologies should also be implemented to protect systems and information used for telework. By using technologies that are available today, federal agencies can prevent the typical incidents of accidental exposure of sensitive information that are reported in the news.

Two types of security are crucial for securing telework: *network security* for intra-agency communications and connections used by teleworkers, and *physical security* for data on mobile devices. Telework devices that require protection include notebook computers, desktop computers used at home, handheld personal digital assistants, telephones (regular, cell, VoIP), and desktop video conferencing. The following tools help to secure telework:

Security for the Network

- Firewall – Blocks unauthorized traffic from entering servers from the Internet
- Intrusion Detection/Prevention – Technologies that monitor network traffic content for infections and block traffic carrying infected files or programs
- Policy Management – Enforces security rules and regulations of IT systems, including every remote endpoint device used by teleworkers
- Virtual Private Network – A secure network for an organization that transmits data through the public network
- Vulnerability Management – Processes to find and remediate cyber vulnerabilities on mobile devices

Security for Data on Mobile Devices

- Anti-virus – Software automatically checks new files entering a PC for infection
- Authentication – Technologies used to verify identities of authorized users, Web sites and computers
- Encryption – The process of encoding data so that only the intended recipient can read it by using a pre-defined algorithm and a secret piece of information, whether data is in transit or at rest
- Firewall – Blocks unauthorized traffic from entering computers from the Internet

The National Institute of Standards and Technologies (NIST) also provides detailed guidelines for selecting security controls for information systems supporting the executive agencies of the federal government. These technologies are described in Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*

What does CSIA recommend the Administration and Congress do about telework?

CSIA urges the Administration and Congress to consider the following recommendations:

- OMB should include telework within the President's Management Agenda for e-government
- Build telework into continuity of operations planning
- Provide endorsement by the highest levels of federal agency management
- Congress should incentivize agencies to pursue telework by removing financial barriers
- Encourage state and local governments to adopt telework
- Explore new benefits of telework

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include Application Security, Inc.; CA, Inc. (NYSE: CA); Citadel Security Software Inc. (CDSS:OTC); Citrix Systems, Inc. (NASDAQ: CTXS); Entrust, Inc. (NASDAQ: ENTU); F-Secure Corporation (HEX: FSC1V); Fortinet, Inc.; Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); McAfee, Inc. (NYSE: MFE); Mirage Networks; PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR); Surety, Inc.; SurfControl Plc (LSE: SRF); Symantec Corporation (NASDAQ: SYMC); TechGuard Security, LLC; and Vontu, Inc.

Cyber Security Industry Alliance
2020 North 14th Street, Suite 750 • Arlington, VA 22201 • (703) 894-CSIA • www.csialliance.org