



# **Making Telework a Federal Priority: Security Is Not the Issue**

**Cyber Security Industry Alliance**

**July 2005**

# Making Telework a Federal Priority: Security Is Not the Issue

CYBER SECURITY INDUSTRY ALLIANCE

JULY 2005

Telework provides flexibility in the locations where employees may perform their jobs. Some call it telecommuting, flexiwork, flexiplace, or enabling a remote work force. Telework lets employees work at home, at an alternate office closer to home, or at other defined locations. Telework may be performed on a fixed schedule, but may also be done at random. The idea was born decades ago and is now widely used in private industry. Telework is popular with employees because it frees them from the drudgery of commuting and provides flexibility for personal activities like a visit to the doctor or attending a child's school event. Many employers provide opportunities for telework because it helps keep workers happy and saves organizations money through higher productivity and reduced overhead. The byproducts of telework include cutting traffic congestion and pollution. For the Federal government, perhaps the most important aspect of telework is that it can greatly facilitate continuity of operations (COOP) in times of crisis. Adoption of telework in the federal government began in 1990 and is on the upswing, but the level seriously lags private industry.

This policy briefing is provided by the Cyber Security Industry Alliance (CSIA), an advocacy group for enhancing cyber security. It explains the story of telework and its benefits to workers and organizations. It describes technologies that enable telework, especially for securing the safety and privacy of sensitive information transmitted to remote employees. The briefing concludes with policy considerations for expanding the adoption of telework throughout federal government. CSIA analysis indicates that security is not an obstacle within the Federal government to expanding telework.

<b>Telework</b>	
<b>Problem Summary</b> .....	2
<b>The Telework Story</b> .....	4
<b>Continuity of Operations</b> .....	5
<b>Documented Benefits</b> .....	5
<b>Technologies for Telework</b> .....	7
<b>Considerations for Policy</b> .....	9
<b>Resources</b> .....	10
<b>About CSIA</b> .....	11

## Problem Summary

### Federal Commitment Is Low

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 latter enforcement “stick” was a provision last year by Rep. Frank Wolf (R-VA) for six federal agencies to be docked \$5 million in their respective FY’04-05 budgets if they did not meet minimum standards for telework. Rep. Wolf is chairman of a House Appropriation’s subcommittee. He has not released results of the provision, but has begun efforts to renew the provision for FY’05-06 and extend telework requirements and penalties to two other agencies. Rep. Thomas Davis (R-VA), Chairman of the Committee on Government Reform said in December 2004 he would consider drafting a proposal to extend Wolf’s provision government-wide, but he has not yet taken action.

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 are puny compared to wide adoption of telework by the private sector. The most recent U.S. General Accounting Office study of telework in May 2004 stated the percentage of eligible federal employees teleworking did not increase between 2002 and 2003, remaining at about 14 percent (see [GAO-04-950T](#)). By contrast, the number of employed Americans who performed any kind of work from home grew from 41.3 million in 2003 to 44.4 million in 2004, a growth rate of 7.5 percent, according to a [survey](#) by The Dieringer Research Group. A report on the top 100 places to work in IT by [Computerworld](#) in 2004 said 88 percent of these large organizations offered provisions for telework.

**Total Americans who work from home** grew from 41.3 million in 2003 to 44.4 million in 2004, a 7.5% growth rate.

The Dieringer Research Group  
2004 American Interactive  
Consumer Survey

### The Roadblock Is People, Not Technology

The 2004 GAO report stated: “Much work remains to ensure that federal employees have the opportunity to telework.” None of the obstacles cited by GAO 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 (in particular, many mid-level managers insist on having staff be physically present when they perform work)
- Lack of training and information on telework programs

Two major obstacles within the federal government stand in the way of expanding telework: 1) an agency that saves money by reducing overhead expenses such as office space must return these savings directly to the federal treasury, and 2) some managers prefer to have employees in the same physical location.

## **The Federal Government Is Missing Huge Benefits**

The benefits of telework are well-documented by private and federal studies. Telework saves energy, improves air quality, reduces congestion and stress on transportation infrastructure, improves job satisfaction and retention, boosts productivity, helps ensure continuity of federal business operations in the event of a disaster, and supports federal employee policies such as promoting a family-friendly workplace. Why should Congress have to intervene and encourage agency adoption of telework when benefits are so obvious? A brief history shows why the federal government must get more aggressive about telework to reap its huge benefits.

## The Federal Telework Story

Telework has a long documented history. The concept was born in the early 1970s. A statutory framework for telework in executive branch agencies of the federal government started in 1990. The framework includes requirements for agencies to take specified actions for telework, provides tools for supporting telework, and designates leadership roles by the Office of Personnel Management and the General Services Administration. OPM and GSA operate the Interagency Telework web site at [www.telework.gov](http://www.telework.gov). The site provides guidance for employees who think they might like to telework or are already doing so, for managers who supervise teleworkers, and for agency coordinators.

Additional statutes on telework were passed in the 1990s. The most significant legislation was passed in 2000 (P.L. [106-346](#)). Its provision by Rep. Wolf in Section 359 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.

Rep. Wolf stepped up his effort to put teeth into telework by inserting language into the omnibus appropriations bill approved on Dec. 8, 2004 (P.L. [108-447](#)). Its Section 622 requires the Departments of Commerce, Justice, State, and Judiciary; the Securities and Exchange Commission; and the Small Business Administration to certify to Wolf’s appropriations subcommittee that telecommuting opportunities are made available to 100 percent of the eligible workforce. The penalty for failure docks \$5 million from the FY’05 budget for each respective agency. Agencies are required to make quarterly reports on the status of telecommuting programs, including the number of employees eligible for and participating in those programs. The provision also requires designation of a “Telework Coordinator” to oversee, implement and operate telecommuting programs in respective agencies. The Government Accounting Office is currently gathering documentation for those certifications and reports. Rep. Wolf has initiated efforts to renew this provision for FY’06 and extend its requirements to the National Science Foundation and the National Aeronautics and Space Administration.

The structure of the Federal budget – not technology or management – may be the biggest obstacle to the expansion of Telework in the Federal government. We understand that there is little incentive for agency leadership to adopt telework, as any savings resulting from reduced overhead for office space are *returned* to the Federal treasury and cannot be applied elsewhere in an agency’s operations. Enabling agencies to realize such savings appears to at least require intervention by the White House’s Office of Management and Budget (OMB), and possibly a change current law.

There is an abundance of information in government and private-sector publications, studies, reports, and how-to resources on developing, implementing and managing telework. The Resources section at the end of this briefing provides web site addresses for a few important telework portals and publications.

## Continuity of Operations

On June 29, the Director of the Office of Management and Budget (OMB) directed all agencies to undertake a review of their telecommunications capabilities in the context of planning for contingencies and continuity of operations, including Federal Preparedness Circular (FPC) 65. FPC 65, which provides guidance for addressing continuity of operations (COOP), addresses telecommuting explicitly. The circular states planning requirements for viable COOP “should take maximum advantage of existing agency field infrastructures and give consideration to other options, such as telecommuting locations, work-at-home, virtual offices, and joint or shared facilities.”

The review is timely, particularly in the context of the recent bombings in London. The bombings closed mass transit systems, denying both government and private sector workers alike access to their offices for extended periods. Unfortunately, these incidents demonstrate that the terrorist threat remains and it is not unreasonable to assume that similar attacks could occur in Washington, with a significant impact on the Federal work force. A more flexible workforce that is prepared to work from virtual locations would certainly lessen the impact of an attack.

## The Benefits Are Well Documented

The GSA’s Office of Personnel Management described the benefits of telework for employers and employees in its May 2003 study, [\*Telework: A Management Priority – A Guide for Managers, Supervisors, and Telework Coordinators\*](#). The OPM report cites many sources of research in documenting the benefits of telework, such as improved quality of work/life, improved job performance, and improved retention. Among the benefits cited:

- Reduces turnover by average of 20 percent
- Trims 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.
- Is a top recruitment tool valued by prospective employees

Valued Benefit
<b>33% of CFOs said telework is the No. 1 incentive to attract top talent.</b>
<b>46% said telework is second only to salary as the top draw.</b>
Robert Half International

An untapped benefit of telework is business continuity in the event of a disaster. The International Telework Association & Council (ITAC) sponsored a public-private study of using telework for business continuity. Specific recommendations for public sector organizations are included in the executive summary of the ITAC report, [Exploring Telework as a Business Continuity Strategy: A Guide to Getting Started](#).

The Office of Personnel Management also has published a compendium of thirteen telework case studies. Each study, [Telework Works: A Compendium of Success Stories](#) provides anecdotal examples of successful experiences for employees who teleworked at least one day per week. The studied positions included budget analyst, contract specialist, librarian, human resources specialist, compliance officer, examiner, and others. There were three key findings. First, managers were willing to experiment. Second, motivated, self-starting employees initiated their entry to telework, worked out details and approached supervisors with a specific plan. Finally, managers and employees agreed on clearly defined expectations before starting a telework arrangement.

Rep. Wolf encourages agencies to allow eligible federal workers to telecommute at least one day per week. He notes that the Washington, D.C. metropolitan area is one of the worst areas in the nation for congestion on roads and highways. By allowing telework, the federal government can lead by example and help to lighten D.C. area traffic, conserve energy, and reduce air pollution.

Leaders in the private sector cite huge financial benefits from telework. AT&T Corp. formalized its telework program in 1992 and currently has more than 25,000 employees who work from home at least once a week. Telework saves the company more than \$150 million a year from better productivity, reduced real estate costs, enhanced retention and recruiting. It says job satisfaction is higher because teleworkers enjoy better work/family balance.

A new public-private partnership called *The Telework Exchange* provides agencies with online tools and value calculators to help determine specific benefits of telework. See [www.teleworkexchange.com](http://www.teleworkexchange.com).

### Telework at AT&T

**30% of management** works outside traditional office

**Another 41% of managers** are regular teleworkers

**90% of salaried employees** are teleworkers

**Productivity up 12.5%** by teleworkers (1 hr. per day)

**\$150 million in annual benefit:** more productivity, lower overhead, enhanced retention and recruitment

AT&T Corp.

Annual surveys in [2004](#) and [2003](#) by

## TECHNOLOGIES FOR TELEWORK

Most major incidents that compromise sensitive information stem from weaknesses in human-based systems, not security technology. But even the best human-based systems need a solid foundation of security applications to protect systems and information used for telework. Security technology is not a roadblock. By using proper security technologies that are available now, federal agencies can prevent the typical incidents of accidental exposure of sensitive information that are reported by newspapers.

The National Institute of Standards and Technologies (NIST) provides detailed guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines were broadly developed from a technical perspective to complement similar guidelines for national security systems. Technologies for securing telework are described in Special Publication 800-53, [\*Recommended Security Controls for Federal Information Systems\*](#). NIST states:

“Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task – a task that demonstrates the organization’s commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.” (pp. 9-10)

Two types of security are crucial for securing telework. They include *network security* for intra-agency communications and connections used by teleworkers, and *physical security* for data on mobile devices. Devices for telework that require protection include notebook PCs, desktop PCs used at home, handheld personal digital assistants, telephones (regular, cell, VoIP), and desktop videoconferencing.

## SECURITY FOR THE NETWORK

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

## SECURITY FOR DATA ON MOBILE DEVICES

<b>Anti-virus</b>	Software automatically checks new files entering a PC for infection.
<b>Authentication</b>	Technology such as multiple-factor authentication (including tokens and smart cards), digital certificates and device authentication to verify identities of authorized users, web sites, and computers.
<b>Encryption</b>	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.
<b>Firewall</b>	Blocks unauthorized traffic from entering PCs from the Internet.

## CONSIDERATIONS FOR POLICY

CSIA urges the Administration and Congress to consider the following recommendations for federal telework policy.

### **1 – OMB should include Telework within the President’s Management Agenda for e-government**

The President’s Management Agenda (PMA) calls for expanding e-government and an effective IT workforce. The Federal government’s stated goal is to be the best manager, innovator, and user of information, services and information systems in the world. OMB acknowledges the opportunities to apply existing and emerging business best practices to government to achieve increases in productivity and delivery of services and information. Telework clearly falls within the PMA’s stated goals. We encourage the White House to call out Telework in the PMA.

### **2 – Build telework into continuity planning**

OMB should ensure that all agencies include telework plans in COOP. Telework will enable a more a resilient and flexible work force in times of crisis lessening the impact of contingencies.

### **3. – Provide endorsement by the highest levels of federal agency management**

Adoption and implementation of telework requires commitment by the employees and especially by the managers of federal agencies. Commitment from the top must be clear, forceful and sincere. Telework is more successful when managers live the balanced work-life ethic.

### **4. – Encourage state and local governments to adopt telework**

As a public sector leader, the federal government should be an operational role model for organizations in state and local government.

### **5. – Explore new benefits of telework**

Congress and Administration should continually look to new benefits from telework. CSIA will sponsor a public-private Town Hall Forum on “Making Telework a Federal Priority.” The forum will be held later this year in the Washington, D.C. metropolitan area.

## RESOURCES

### General

#### **U.S. Interagency Telework Web Site**

Operated by General Services Administration and Office of Personnel Management

<http://www.telework.gov/>

#### **International Telework Association & Council (ITAC)**

Non-profit association for Fortune 500 companies and U.S. agencies since 1993

<http://www.telecommute.org/>

#### **Telework Consortium**

Group working with public policy decision makers and pilot testing projects

<http://www.teleworkconsortium.org/>

### Organizational Guidelines

#### ***Telework: A Management Priority – A Guide for Managers, Supervisors, and Telework Coordinators***

GSA Office of Personnel Management (May 2003)

[http://www.telework.gov/documents/tw\\_man03/prnt/manual.asp](http://www.telework.gov/documents/tw_man03/prnt/manual.asp)

### Security Technology for Telework

#### ***Security for Telecommuting and Broadband Communications***

National Institute of Standards and Technology, Special Publication 800-46 (Aug. 2002)

<http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>

## About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Surety, Symantec Corporation, and TechGuard Security.

### **Cyber Security Industry Alliance**

2020 14th Street  
Suite 750  
Arlington, VA 22201  
(703) 894-CSIA  
[www.csialliance.org](http://www.csialliance.org)

© COPYRIGHT 2005 CYBER SECURITY INDUSTRY ALLIANCE. ALL RIGHTS RESERVED.  
CSIA IS A TRADEMARK OF THE CYBER SECURITY INDUSTRY ALLIANCE. ALL OTHER COMPANY, BRAND AND PRODUCT NAMES MAY BE MARKS OF THEIR RESPECTIVE OWNERS. 3: 3-07-2005