



## FOR IMMEDIATE RELEASE

### Media Contacts:

Lauren Olsen  
Telework Exchange  
(703) 883-9000 ext. 118  
[lolsen@teleworkexchange.com](mailto:lolsen@teleworkexchange.com)

Deb Symons  
Utimaco  
(508) 543-1008 ext. 222  
[deb.symons@utimaco.com](mailto:deb.symons@utimaco.com)

## One Year After Veterans Affairs' Laptop is Stolen, Fed Data is Still AWOL

*Telework Exchange Study Reveals Encryption Shortfall, Security Education Opportunity, and Telework Advantage*

**ALEXANDRIA, Va., June 4, 2007** – Telework Exchange<sup>SM</sup>, a public-private partnership focused on telework in the Federal government, today announced the results of its latest study – “Feds Walking the Talk on Security? – One year after the VA laptop scandal, is Fed’s data still going AWOL?” Underwritten by Utimaco, a data security company, the study reveals that Federal data is significantly more mobile and still vulnerable. Thirteen percent of Federal employees do not have encryption on their newly-issued laptops. Pushing back the myths about telework, the study shows that Federal teleworkers are more secure than their in-office colleagues.

In June 2006, VA announced that the laptop stolen from an employee’s home contained personal information on roughly 26.5 million people, including 1.1 million active military members. The study, “Feds Walking the Talk on Security?” uncovers what has changed since the Veterans Affairs laptop scandal and what still needs to be addressed in agencies’ data security policies.

The study provides new insight on Federal agency employees’ knowledge of their agencies’ data security policies and out-of-office data security practices. Key study findings include:

### ***Are Feds More Mobile?***

The Federal government has embraced mobility. Forty-one percent of respondents note that they use a laptop for work. Out of these laptop users, 45 percent have switched to a laptop in the last year.

***Are Feds More Secure?***

The study highlights vulnerabilities in data security systems. Thirteen percent of new laptop users do not have encryption. Merely 48 percent of respondents said that their agency provided training after the VA laptop scandal, and 47 percent of agencies provided updated encryption and protection technology on computers. Sixteen percent of respondents said their agencies had no reaction.

***Data Security Achilles Heel – Teleworkers or Non Teleworkers?***

Teleworkers are defined as employees who work at alternative worksites during regularly scheduled work hours – on a full-time, part-time, or situational basis. Results indicate teleworkers remain in tune with agencies' data security procedures and training. Ninety-four percent of teleworkers have received security training, compared to 87 percent of non teleworkers, who work at the official workplace full time. In addition, 94 percent of teleworkers have anti virus on their work computers, compared to 75 percent of non teleworkers.

***Going AWOL***

Pointedly, the survey highlights a hidden majority of non teleworkers – the “unofficial teleworkers” – as the data security Achilles heel. “Unofficial teleworkers” are defined as employees who work at an official workplace full time, and also work at home on nights or on weekends. Fifty-eight percent of non teleworkers work at home on nights or weekends, unofficially. Out of these respondents who work at home, 63 percent use their own PCs. Fifty-four percent of non teleworkers carry files home and 41 percent log onto their agency's network from home. Agencies' data is moving in an uncontrolled environment. “Unofficial teleworkers” remain a high liability for Federal agencies.

***Recommendations***

Agencies need to audit the “unofficial teleworker” populations, enforce telework training practices similar to those who telework officially, and ensure that all employees are aware of how to handle data outside of the office environment – regardless of where they work. Agencies must make sure all desktops and laptops are protected and all data is encrypted.

“The study points to the inevitability mobility/security challenge,” said Craig Bumpus, general manager, Utimaco America. “Employees who work unofficially at home on nights and weekends are removing data from the office – either by mobile device or by hard copy files – and working in unauthorized locations. Agencies must take the necessary security precautions to protect

all computers and provide adequate training to employees on transporting data outside of the office.”

“Security of Federal data is not about bits and bytes – it’s about the brand of the U.S. government and Americans’ confidence in their government,” said Stephen W.T. O’Keeffe, executive director, Telework Exchange. “One year after the VA laptop crisis, America’s information is still AWOL. It’s time to get serious about security.”

The “Feds Walking the Talk on Security?” study is based on a survey of 258 Federal employees. Fifty-two percent of respondents are non teleworkers and 48 percent are official teleworkers. To download the full results of the study, please visit [www.teleworkexchange.com/datasecurity](http://www.teleworkexchange.com/datasecurity).

### **About Telework Exchange, LLC**

Telework Exchange is a public-private partnership focused on demonstrating the tangible value of telework and serving the emerging educational and communication requirements of the Federal teleworker community. The organization facilitates communication among Federal teleworkers, telework managers, and IT professionals. For more information on Telework Exchange, please visit [www.teleworkexchange.com](http://www.teleworkexchange.com).

### **About Utimaco Safeware AG – The Data Security Company**

Utimaco is the leading provider of data security solutions. The Data Security Company enables mid- to large-size organizations to safeguard their data assets against attacks and to comply with privacy laws by protecting their confidentiality and integrity. In response to twenty-first century threats Utimaco’s complete range of data security solutions provide full 360 degree data protection unlike point solutions which only partially cover the data security needs of enterprises. Only SafeGuard solutions protect and manage data during storage (data at rest), during transmission (data in motion) and during processing (data in use). Utimaco offers its customers comprehensive on site support via a world-wide network of certified partners and subsidiaries in Europe, the USA and Asia. Utimaco Safeware AG, with headquarters in Oberursel, near Frankfurt, Germany, is listed on the Frankfurt Stock Exchange (ISIN DE0007572406). For more information please visit <http://www.utimaco.com>.

**About Utimaco USA**

Based in Foxboro, Mass., Utimaco U.S.A. is a business unit of Utimaco Safeware, AG. The company provides technical, sales and marketing services throughout North America and Canada for Utimaco's extensive line of platform-independent, mobile, desktop, and network security solutions. Utimaco also has technology partnerships with market leaders such as IBM Lenovo, Microsoft, Card Systems, and Siemens. A full list of technology partners as well as reseller partners can be found at [americas.utimaco.com](http://americas.utimaco.com).