



Media Contacts:

Lauren Olsen

Telework Exchange

(703) 883-9000 ext. 118

lolsen@teleworkexchange.com

Federal CISOs Give Telework the Green Light

Telework Exchange Federal CISO Study Reveals Strong Interest in FISMA-Compliant End-Point Certification

ALEXANDRIA, Va., August 27, 2007 – Telework ExchangeSM, a public-private partnership focused on telework in government, today announced the results of the “Remote Control – Federal CISOs Dish on Mobility, Telework, and Data Security” study. Underwritten by HP, the study dispels myths of telework and security incompatibility – 94 percent of Federal Chief Information Security Officers (CISOs) do not consider official telework programs a security threat. Managing security in an increasingly mobile agency computing environment, 63 percent of Federal CISOs flag securing mobile devices as their number-one priority. Calling for a standards-based approach, some 83 percent of Federal CISOs express strong interest in a Federal Information Security Management Act (FISMA)-compliant mobile end-point certification.

Key study findings include:

- **Feds are Increasingly Mobile:** Eighty-three percent of Federal CISOs report an increase in laptop use in the last year and 17 percent of Federal CISOs say laptops represent half of their agencies’ computers
- **Keeping Mobile Data Secure is a Top Priority:** Sixty-three percent of Federal CISOs say securing mobile devices is their top data security priority
- **Telework is Not the Enemy:** Federal CISOs are integral to telework programs – 88 percent have input in their agencies’ telework programs. Knowledgeable in telework and security infrastructures, 94 percent of Federal CISOs say official teleworkers do not pose a security threat

- **FISMA Insight:** Eighty-three percent of Federal CISOs say telework or mobile computing does not hamper their abilities to meet FISMA requirements. An overwhelming majority – 83 percent – recommend a FISMA-compliant mobile end-point certification
- **Next Steps:** Federal CISOs recommend data security training for all employees, an audit of the full population of employees who work from locations other than their primary work sites, and a solution to ensure all telework-eligible employees are working within an official program

“Based on numerous study results, we find that while security is top of mind and should be top of mind for agencies, it should not hinder telework adoption,” said Stephen W.T. O’Keeffe, executive director, Telework Exchange. “Telework is the paragon for government operations. Now is the time to stop pointing the finger at telework as a culprit and instead embrace the program as a standard operating practice.”

“Although data security is top priority, according to Telework Exchange’s study, 94 percent of Federal CISOs surveyed said official teleworkers do not pose a security threat to their Federal agencies,” said Eric Brennan, director, PSG Solutions Marketing, HP. “This is further evidence that when agencies establish telework programs with proper security training, support, and equipment, Federal employees can safely benefit from more work/life balance, freedom, and cost-savings from reduced commute times.”

The “Remote Control – Federal CISOs Dish on Mobility, Telework, and Data Security” study is based on a survey of 35 Federal CISOs. There are 117 CISOs in the Federal government. To download the full study results, please visit www.teleworkexchange.com/cisostudy.

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.