

Navy Dives Deep into Telework



In an era of dwindling supply and increasing demand for top personnel, the Navy wants to remain a leading employer of choice. To ensure that it can compete effectively with industry and other service branches – especially as more members of Generation Y enter the workforce – Navy officials are set to begin permanently offering telework and other flexible scheduling programs at qualifying commands as a tool to better attract and retain employees.

“This all came out of the fact that we began looking for innovative ways to make sure that our employees are able to be productive and that we as an employer are able to hold people accountable for results, rather than saying, ‘Hey, you’ve got to be standing tall at 0700 in the morning so I can see everybody’s smiling face,’” says Capt. Ken Barrett, director of the Navy’s Task Force Life/Work (TFLW). “That model

is just not going to work for us as we get further into the 21st Century.”

While the Navy is looking at several work arrangements, it definitely sees telework as an important component of its strategy and is moving forward quickly. A telework pilot was started and continues within the N1 Total Force branch, with surveys showing positive productivity increases and high satisfaction rates among teleworkers and supervisors. Barrett now expects a permanent program to be underway by early 2010, predicting that at least 65 to 75 percent of personnel will be able to telework at least some of the time.

In addition, the new chief of Naval personnel, Vice Admiral Mark Ferguson, now has the ability to telework from his home with the goal to work from there at least one day a week. This decision, says Barrett, “has sent a signal to our

CONTINUED ON PAGE TWO

Telework Security is “Very Doable,” Says Federal Expert

Ron Ross believes that there are enough security tools and protective layers available to make teleworking as safe as a traditional office environment, but not just because he happens to be a leading expert on network and infrastructure security. The senior computer scientist and information security researcher at the National Institute of Standards and Technology (NIST) also knows from experience. He is an enthusiastic teleworker who works out of his home office several days a week.

“I really do think that we have a sufficient number of controls available that can reduce the risk to a level that is tolerable for even the most nervous manager, and it’s important for them to realize that, so they can take advantage of all the good things that teleworking brings to the employee and to the organization,” he says.

The key to ensuring that telework has the right security in place is to set up the alternate work site and computing environment in the same way it is done at the headquarters office location. That means addressing information in its three states:

1. At rest or when it is located in a secondary storage device, such as a hard disk
2. In transit between the corporate site and the telework venue

CONTINUED ON PAGE TWO

Navy Dives Deep into Telework

CONTINUED FROM PAGE ONE

entire leadership that telework is something to be embraced. If he is willing to do it, others should too.”

In the meantime, TFLW is working with Navy technical personnel to make the telework environment more user-friendly, including putting shared folders on Defense Knowledge Online, the very secure architecture run by the Defense Information Systems Agency (DISA). Barrett expects that task to be completed this fall and to roll-out a Navy-wide instruction by late 2009.

“That would basically be giving the authorization for telework,” Barrett says. “Now, we are obviously doing it within our own enterprise, and other folks have been able to embrace it on their own without asking for permission, but being able to have that permission there, that top cover, so to speak, is certainly something that we want to be able to give to the commanders in the field.”

On the surface, the idea that the Navy, with its long deployments at sea and hands-on work requirements, would and could embrace telework seems incongruous. And Barrett himself initially thought it might be appropriate only for administrative positions. After hitting the road last fall with three of his lieutenants to get the sailors’ views at Naval bases in San Diego, Norfolk, Hawaii, Japan, and other sites, however, he realized that the work arrangement was not nearly as limited as he first believed.

The first person who brought up telework was an aircraft maintenance worker near San Diego, who inquired about having telework as an option. While the employee obviously needed to be physically on-site to do maintenance, his job also included the requisite scheduling, log-keeping,

and other paperwork tasks that he felt could be done, and done more quickly, off-site.

Now, Barrett says, he and his team see potential for all kinds of teleworking opportunities. Sailors could sign up for telework while working their shore jobs in between deployments, for example. People who work with top secret or secret information would not be eligible, but many of those personnel also tend to work with unclassified information, so during that time, they might be eligible to work from home.

The Navy concurrently is investigating and piloting other flexible arrangements, such as compressed scheduling, flexible work hours, and even career intermission, which would allow Naval personnel to take a break from their careers without losing their place in the promotion chain.

Ultimately, though, these work arrangements, along with telework, are all seen as more than a way to improve morale and benefit the work and personal lives of Naval employees. They will also enable the Navy to hang onto its best people and fulfill its mission as effectively as possible.

Barrett notes that he talked to a lot of people during his Road Show last year, even those who had left the Navy. “We heard a lot of variations on this sentiment: ‘I would have loved to have stayed with this organization. I loved the job I was doing, but based on the career path and the timeline for me to move up, it was too rigid. If only you’d given me just a little bit of flexibility, I would have stayed.’ That kind of flexibility is something that other employers are beginning to offer, so we too have got to have those kinds of work options available if we are going to be an employer of choice, so when it comes time for those decisions to join up and then

whether not or to stay, they will choose the Navy.”

Telework Security is “Very Doable,” Says Federal Expert

CONTINUED FROM PAGE ONE



Ron Ross, senior computer scientist and information security researcher, National Institute of Standards and Technology (NIST)

3. In process, when the employee is actually using the information

To address each state, Ross recommends using what NIST terms a “Defense in Depth” strategy. He adds that his agency relies on this strategy in its own telework program and is so effective that Ross feels completely at ease working out of his home office. Components of this approach include the following:

- Establish and use a Virtual Private Network (VPN) connection between agency headquarters and the telework site, which relies on firewalls, encryption, and tunneling to ensure that information is fully protected while in transit across public networks
- Equip teleworkers with an authorized government-owned and -issued laptop or workstation so that it can be managed as an agency asset
- Rely on managed services so routine updates and upgrades on

CONTINUED ON PAGE THREE

To read the full text of the articles in this issue, visit

www.teleworkexchange.com

Telework Security is “Very Doable,” Says Federal Expert

CONTINUED FROM PAGE TWO

virus templates, security patches, and other optimal configurations can be pushed to the teleworker’s computing device automatically by the IT department (or contracted third-party vendor)

- Equip the laptop with an add-on biometric device, like a fingerprint reader, for secure access by the designated employee only
- Install a “session lock” on the computer so when the employee leaves his or her desk, the computer would go into sleep mode and the employee upon returning would have to log in using a password and (if applicable) a fingerprint reader to bring the computer back up
- Use full-disk encryption so if a laptop or hard drive is lost or stolen, the information cannot be accessed and would therefore be useless to an unauthorized user
- Conduct automatic backups to the agency site over the network so if something happens to the teleworker’s remote office or computer, the information would be readily accessible by other agency personnel
- Rely on personal identifiers, such as passwords and endpoint device authentication, to guard against any unauthorized access to the agency network

Managers who feel jittery at the idea of telework have a legitimate right to be concerned whenever operations are moved outside of the normal boundaries of an enterprise, Ross says. “It’s important for them to realize, however, that there are a variety of controls available to them,

and that the number and strength of those controls are really at the discretion of the organizations and the managers that are going to allow telework to proceed,” he states. “It does always get back to the individual manager’s risk tolerance, but I think if they take the time to see what’s available, they’ll see that telework can be done in a secure manner.”

Ross adds that anyone with questions can contact him or another NIST security expert. He also recommends consulting the recently-released NIST Special Publication 800-46, “Security for Telecommuting and Broadband Communications,” as well as Special Publication 800-53, “Recommended Security Controls for Federal Information Systems.”

The Teleworker Highlights

To view full text, visit www.teleworkexchange.com.

Let’s Talk Telework

Kathy Kadilak, President of Strategic Work/Life Solutions, answers questions about teleworking from *The Teleworker* readers.

COOP and Telework: A View from the Inside

As deputy division director of the National Continuity of Operations (COOP) Division for the Federal Emergency Management Agency (FEMA) within the Department of Homeland Security, Eric Kretz understands the value of telework to an agency that has to deal with the routine-altering ramifications of a sudden disaster, whether it is a local snowstorm, a pandemic flu, or a bioterrorism incident.

Kretz recently spoke with *The Teleworker* about the success and challenges that agencies see while trying to combine telework and COOP planning and what additional steps

telework program officials can take to help improve the effectiveness of COOP.

FDIC: Success Personified



Arleas Upton Kea, director, Division of Administration, FDIC

By any measure, the Federal Deposit Insurance Corporation (FDIC) makes telework look easy. Its program, established in 2001, now has more than 1,600 regular teleworkers across every grade level and division – and more than 2,600 of FDIC’s over 4,500 employees, including nearly 50 percent of its managers, teleworked at least one day during 2007. FDIC also permits bank examiners to choose to telework from home versus a field office when they are not in a bank, allowing the agency to reduce its real estate needs. The Corporation estimates that it will reap savings in rental costs in 2008 equal to approximately \$1,748 per “work at home” employee.

Disaster Recovery: Tailor Programs and Practice, Practice, Practice

Pandemic preparedness and Continuity of Operations (COOP) planning are all top-of-mind priorities for Federal government professionals, and many employees are uncertain what to do when regular operations

CONTINUED ON PAGE FOUR

To read the full text of the articles in this issue, visit www.teleworkexchange.com

The Teleworker Highlights

CONTINUED FROM PAGE THREE

are interrupted. According to Steve O'Keefe, executive director of Telework Exchange, recent research shows that 45 percent of Federal employees do not have personal guidance from their agencies on how to handle a disaster and more than 40 percent feel their agency is not prepared to continue business operations in the event of a disaster.

Given this context, a panel of disaster recovery and COOP experts assembled at the Symantec Government Symposium 2008 on July 31, 2008, in Washington, D.C. to discuss how agencies can better prepare for operating in extended emergency situations and how telework can – and should – be an integral component of their preparedness planning.

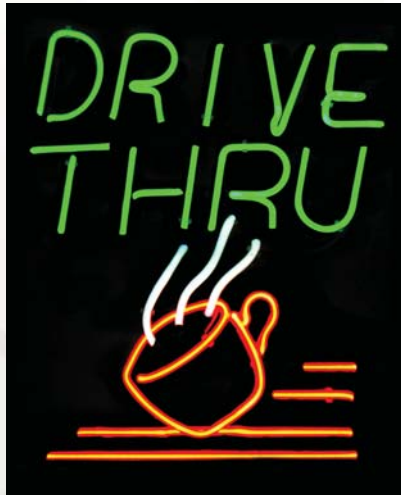
Teleworkers Benefit from Wireless

The majority – 83 percent – of Federal IT executives believe that wireless Internet can be used securely. As a result, Federal agencies are increasingly allowing employees to use the technology to realize productivity and continuity of business operations gains. Further, teleworkers are much more aware of and compliant with their agency's related security policies than non-teleworkers, according to a recent study conducted by Telework Exchange and Sprint.

IRS Planning Move from Telework Pilot to Program

When the Internal Revenue Service (IRS) decided to kick off its Virtual Office pilot initiative in July 2007, the initial goal was to "find out what we didn't know about telework," according to Greg Zurmühlen, then acting deputy, Real Estate and Facilities Management. To do so, the agency invited 150 volunteers in three business lines to begin working at home four days a week.

Telework News Update



Virginia Governor Encourages Telework

Gov. Timothy Kaine announced in mid-July an initiative that will allow 120 gubernatorial appointees to telework and he directed all state agencies to do what they could to follow his lead. Kaine cited rising fuel and commuting costs, traffic congestion, and environmental concerns as the drivers behind the new policy, which he described as an "opportunity to create a culture of conservation." Almost immediately, more than 60 employees within the Kaine Cabinet and office began teleworking or using alternative schedules for part of their work week.

Telework Tax Credit Proposed

In mid-July, Congressman Earl Blumenauer (D-OR) introduced new legislation for consideration by the 110th Congress, with Representatives Ellen Tauscher (D-CA) and Christopher Shays (R-CT) as original cosponsors of the "Transportation and Housing Options for Gas Price Relief Act of 2008" (H.R. 6495). This bill focuses on the impact of increasing gas prices on U.S. consumers and proposes a number of initiatives associated with alternative forms of transportation to reduce dependency on gas

consumption. Among the programs outlined, the Gas Price Relief Act proposes creation of a Telework Tax Credit "for qualified teleworking expenses for employers and employees." This telework incentive program is intended to encourage broader adoption of telework nationwide and reduce millions of gallons of fuel used by commuters. For more information on H.R. 6495, please visit www.teleworkexchange.com.



Fall Town Hall Meeting Details

Where: Ronald Reagan Building, Washington, D.C.

When: October 15, 2008
Registration begins at 7:30 a.m.
Program runs from 8:30 a.m. - 4:30 p.m.

Contact

Please contact Meghan O'Neil for more information.

E-mail:

moneil@teleworkexchange.com

Phone: (703) 883-9000, ext. 125

For additional details please visit

www.teleworkexchange.com/townhallmeeting.

The Teleworker

Phone 703.883.9000 | Fax 703.883.9007 | **Enquiries:** Cindy Auten 703.489.1185

Write to Us: 921 King Street | Alexandria, VA | 22314 | **Info:** info@teleworkexchange.com