



P&R CIO Newsletter

SERVING THE P&R COMMUNITY

VOLUME 3, ISSUE 2



WINTER 2011

Telework: A Flexible Work Environment and New Security Challenges for the Federal Government

Points of Interest:

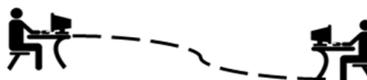
- Secure Telework
- Cloud Computing and Federal IT
- Green IT at P&R

Less than a year after snow storms paralyzed the Federal government, President Obama signed the Telework Enhancement Act into law, requiring agencies to increase the number of eligible telework employees and establish telework policies. In addition to setting new policies, the legislation also established interactive training programs for teleworkers and telework managers and set guidelines for the appointment of a telework managing officer in each agency, who must be senior official with direct access to the agency head. Following the President's announcement, the Office of Personnel and Management (OPM) also announced a new telework policy for federal workers who are unable to make it into the office due to inclement weather or emergencies, allowing employees with telework agreements to participate in unscheduled telework as needed. These new telework policies are expected to help the Federal government reduce costs incurred when government functions are closed or severely limited and to provide employees with work-life balance.

According to the Telework Exchange, a public-private partnership focused on expanding telework adoption, there are

five key steps that agency leaders can take to help create a successful telework program:

- Step 1:** Change the Mindset – Build Management Support
- Step 2:** Define Essentials to Demonstrate Return on Investment (ROI) and Overcome Resistance
- Step 3:** Management Training – Measure Productivity
- Step 4:** Telework Technology – Supply Secure, Effective, and Affordable Solutions
- Step 5:** Enhance Continuity of Operations (COOP) – Deploy Telework for Business Continuity



As addressed in Step 4 of the Telework Exchange's five step plan, the tools used to implement a new telework policy should provide a sufficient level of security, commensurate with the significance of the data produced and handled by the organization. Agencies should determine what types of resources will be necessary to implement telework for their current employees, and they must ensure that the solutions selected will be able to handle any foreseeable internal growth. Policies in this new environment should be written to address any and all security concerns, espe-

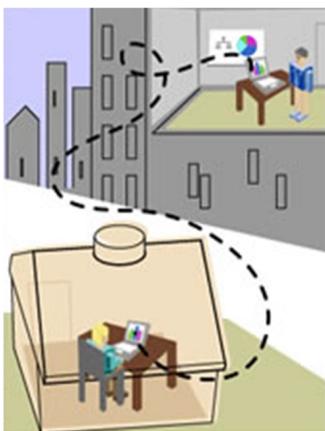
cially to ensure that each and every teleworking employee is trained on how to safely telework. The OPM recommends that agencies allow employees to telework regularly to familiarize them with the concept of working remotely.

As you explore the new Telework Enhancement Act, keep in mind that the government provides free antivirus software for all employees, including contractors, which can help prevent many security issues when teleworking. VPN connections may be used and/or regardless of location, wireless connections should always be secured with the highest possible level of security. Also, computers should be updated with the latest software patches for operating systems and applications. Implementing these measures is an easy way to provide the most secure and convenient work environment possible.

For more information on teleworking, visit www.telework.gov.

Sources:

- <http://www.teleworkexchange.com/pdfs/Telework-Exchange-From-Bill-to-Building-Release.pdf>
- <http://fcw.com/articles/2010/11/18/congress-passes-telework-policy-bill.aspx>
- <http://www.opm.gov/oca/compmemo/dismissal.pdf>



Cloud Computing: The Future of Federal Information Technology



The phrase ‘Cloud Computing’ is quickly being adopted by organizations around the globe, including the Federal Government. Cloud computing allows an organization to offload the burden of many Information Technology (IT) services to a third party who provides application and data hosting via the Web. With demand for IT services increasing as budgets are cut across the board, cloud computing provides a viable and cost-effective alternative.

Federal agencies are already positioning

themselves for organization-wide utilization of cloud computing services. The Federal Chief Information Officer (CIO) Council created the Federal Risk and Authorization Management Program (FedRAMP) in November 2010 to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. This process will allow joint authorizations and continuous security monitoring ser-

VICES for multi-agency cloud computing systems, and FedRAMP-certified vendors will enjoy shorter wait times for security authorizations and Authorities to Operate (ATO). The Department of Defense (DoD) is a prime example of the Federal Government’s use of the cloud. It recognized that centralized computing can provide cost savings to Combatant Commands, Services, Agencies, and Field Activities, especially when faced with scalability issues; in response to this opportunity,

the DoD created the Rapid Access Computing Environment (RACE) cloud computing solution operated by Defense Information Systems Agency (DISA).

Organizations cannot look solely at the convenience of cloud computing without considering all necessary aspects of data security. Vendors should provide the same level of security that would be provided for those servers and applications if hosted on-site. As with all technologies, advantages and disadvantages including cost and risk must be weighed against each other, and these factors will vary greatly for every organization.

Sources:

- <http://fcw.com/CloudComputingSnap>
- <http://cio.gov/pages-nonnews.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP>
- <http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf>

Green Information Technology (IT) Moving Forward at P&R

Green IT, also known as Green Computing, is the movement towards a more environmentally friendly and cost-effective use of power and production in technology.

Green IT is more environmentally sustainable by taking into account the use, manufacturing, and disposal of computers, servers, and associated hardware — such as printers, monitors, and storage devices — and trying to limit their environmental impact.

As the Federal Government moves towards data center consolidation, the crux of Green IT is to efficiently and effectively utilize IT with minimal or no impact on the environment by converting new structures and systems to this more conservative mode of operation. As consolidation continues, agencies are exploring the pros and

cons of some common Green Computing concepts such as virtualization and telecommuting, featured earlier in this newsletter.

Personnel and Readiness (P&R) is doing its part to stay on top of Green IT innovation. In October, P&R Information Management (P&R IM) attended the Virtualization, Cloud Computing, and Green IT Summit in Washington, D.C. Guest speakers included Mr. Ira (Gus) A. Hunt, Chief Technology Officer (CTO) of the Central Intelligence Agency (CIA) and Mr. Henry Sienkiewicz, Chief Information Officer (CIO) of Defense Information Systems Agency (DISA). The Summit hosted panel discussions on topics

ranging from power management strategies to the anatomy of a cloud. In addition to keeping abreast of cutting edge Green Computing efforts, the P&R IM Green IT team also organizes and hosts a Green IT Working Group and distributes regular communications to P&R and Defense Human Resource Activity (DHRA) Green IT representatives. These communications include information about Green IT best practices, tips, and events that P&R and DHRA agencies can incorporate into their everyday operations.

If you would like more information about Green IT at P&R IM or on the speakers and Green IT sessions from the Virtualization, Cloud Computing, and Green IT Summit, please contact the P&R IM CIO team at CIOsupport@osd.pentagon.mil.

