



# Government on the Go – Preparing for Telework

---

GTC Conference

May 14, 2009

Deloitte & Touche LLP

# Disclaimer

This publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

# Security and Data Vulnerability

## The Telecommuting Dilemma

---

- Clearly, there are security and data protection issues with teleworking
- Both **employees** and **agency leadership** have a responsibility to apply strong security and privacy practices to teleworking
- Agencies responsibilities:
  - Establish clear policy that defines the types of functions permitted to telework ... not all jobs are appropriate for telecommuting
  - Ensure teleworkers understand the security ramifications and have the knowledge to comply with security and privacy requirements.
- Employees responsibilities:
  - Ensure that home telework environment complies with security and privacy requirements.
  - Comply with Acceptable Use Policy, participate in annual information security training, and report security incidents to the Information Security Officer.

## Acceptable Use Policy – State Administrative Manual (SAM)

---

- Policy Statements Under Acceptable Use Section of SAM Security Policy:
  - Users of state computer assets must be authorized in accordance with, and abide by the requirements of the **Enterprise Access Control Standard**.
  - Before receiving authorization to use computing assets which have access to or from the Internet, Telework users shall formally agree to abide by the **Enterprise Internet Acceptable Use Standard**.
  - Before accessing state IT infrastructure from a remote location, Telework users shall formally agree to abide by the **Enterprise Telework Standard**.

# State Administrative Manual (SAM)

## Telework Standard

---

- The Telework Standard Requirements include\*:
  - Secure Configuration of Network Devices & Connections
  - Security of Telework Devices
  - Maintaining Software Updates
  - Limiting Telework User Privileges
  - Telework User Account Passwords
  - Protection from Unauthorized Physical Access
  - Secure Application Configurations
  - Security Maintenance and Monitoring
  - Training of Telework Users
  - Securing Home Networks
  
- ❖ *Teleworking Standard draft is in process. Agencies can refer to [www.oispp.ca.gov](http://www.oispp.ca.gov) for the State's overarching security and privacy policies and standards*

## Deloitte LLP's Experience with Teleworking

---

- Deloitte LLP has over 44,000 employees in the U.S. across audit, tax, consulting, and financial advisory services
- The nature of our work entails that, at any given time, a significant number of employees may be working away from the office
  - These professionals are not considered teleworkers who require a formal telework agreement (however they must abide by Deloitte's general security and privacy policies)
- A formal telework agreement is required for professionals that have made a formal request for a flexible work arrangement
  - The formal agreement provides professionals with the flexibility to work up to 50% of their normal work week from home
  - Professionals must be at a certain level and number of years experience and have received performance evaluations that “exceed expectations”
  - Formal telework arrangements must be formally reviewed and approved by supervisors

# Questions?

---

# Deloitte Contact Information

---

## **Russell L. Jones, Partner**

- Security and Privacy Practice
- Enterprise Risk Services
- Deloitte & Touche
- Tel: 415.783.5054
- Email: [rujones@deloitte.com](mailto:rujones@deloitte.com)

## **Suna Taymaz, Sr. Manager**

- Security and Privacy Practice
- Enterprise Risk Services
- Deloitte & Touche
- Tel: 415.783.5583
- Email: [staymaz@deloitte.com](mailto:staymaz@deloitte.com)

# Deloitte.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Member of Deloitte Touche Tohmatsu

Copyright © 2009 Deloitte Development LLC. All rights reserved.