Nextgov

Suss Consulting Inc.
When you need results SM

Securing Your Agency's Mobile Devices for the Cloud

Presentation to the Nextgov Webinar
March 28, 2013
By Warren Suss
President, Suss Consulting, Inc.

Suss Consulting, Inc.
801 Old York Road • Suite 305 • Jenkintown PA • 19038 • 215.884.5900
www.sussconsulting.com

Technology Policy and Marketplace Environment

- Agencies shift to cloud and mobile technologies in response to top-down policy pressure and bottom-up user demand

- Technology is rapidly changing, budgets tightening, and policy still evolving

- Approach to managing risks for cloud and mobile must be different than the approach for more mature, hard wired technologies

Mobile Policy

- **"All existing Federal requirements for data protection and remote access are applicable to mobile devices."**
  - OMB Memorandum 12-20, dated September 27, 2012 states the following in paragraph 25 (p. 13).

- **The Problem?**
  - "Additional guidance regarding the use and management of mobile devices will be developed as appropriate."
    - NIST "Guidelines on Hardware-Rooted Security in Mobile Devices," (SP 800-164)
    - NIST "Guidelines for Managing and Securing Mobile Devices in the Enterprise (SP 800-124)

Department of Defense

- **Department of Defense Commercial Mobile Device Implementation Plan**
  - Cost management and governance
  - Security

- Aggressive set of targets for information assurance

Approved Identity and Access Management

v.

The Nature of Mobile Computing

A Period of Flux

- Tough technical challenges and policy decisions

- **The DoD "Commercial Mobile Device Implementation Plan"**
  - Protect Controlled Unclassified Information using approved Public Key Infrastructure (PKI) credentials (i.e. Common Access Card or CAC card)

  - **The Challenge:** only one CAC card sled available for only one commercial mobile device (Blackberry)
    - Experiencing an extreme drop in popularity

Gap between existing policy guidance and practical realities of available solutions in the marketplace

"The adoption of mobile devices by federal users, especially smartphones and tablets, is catching on like wildfire. Every week, there are more and more people in meetings with smartphones and tablets. We're in the midst of massive, almost uncontrolled adoption of mobile technology."

– Senior Agency IT Official

The Reality?

Many IT executives do not have good data on and control over the devices they're supposed to be managing.

Security of Cloud Computing

- **Federal Risk and Authorization Management Program (FedRAMP)**
  - Standardize and streamline cloud Certification and Accreditation (C&A) processes
- **DoD Cloud Computing Strategy**
  - "…externally provided cloud services, i.e., commercial services, to expand cloud offerings beyond those offered within the Department."
    - Intention to leverage FedRAMP
- **Both in early phases of deployment**

Concerns about security are the leading factor holding back more rapid adoption of cloud services by both corporate and federal users.

Example

From an agency IT official:

"We just finished our migration from internally supported and provided email into a cloud mail solution and an array of services associated with that. It is not housed inside the department. In the past, when I had my laptop, I used to dial into my VPN to get the message encrypted. Now, any user can take their Android, go straight into the Internet to get to their email. They're bypassing my previously established security solution."

Nightmare Scenarios

- Virus-infected smartphones accessing cloud email
- Bypassing VPNs
- Misplacing mobile devices with sensitive attachments
- Virus-infected smartphones broadcasting to foreign agents

The Bottom Line:

We need immediate investments in mobile security solutions

Recommendations

- Use a risk based approach
- Keep your eye on a dynamic marketplace
- Prioritize security over other administrative challenges
- Speed and power count
- Consider field trials
- Assess total cost of ownership
- Stay flexible

Questions?