Secure Mobility

AFCEA Cyber Committee

I. Approach

Mobile technology is a pervasive driver for innovation, agility, and flexibility in the workplace for both the U.S. Government and industry. The AFCEA Cyber Committee approached this review of secure mobility by monitoring the outcome Federal CIO Council's assessment of U.S. Government agencies use of mobile technology. A Mobile Technology Tiger Team (MTTT) was created to "Evaluate opportunities to accelerate the secure adoption of mobile technologies into the Federal environment at reduced cost." [1] The MTTT developed a questionnaire to gather information from 21 agencies throughout the Federal government. The AFCEA Cyber Committee considering this a valuable tool modified the questionnaire for surveying key industry representatives. This report documents the survey demographic and key findings.

II. Survey Demographic

The demographics were broad to include large system integrators, internet service providers (ISPs), Federally Funded Research and Development Centers (FFRDC), non-for-profit, and retail. Likewise, the sizes of these organizations ranged from modest in size to Fortune 100 companies with staffing exceeding 10,000 employees. One noticeable trend was that larger organizations tended to support a broader range of device platforms. Conversely, smaller organizations embraced the use of BYOD to presumably offset operational costs.

III. Key Findings

a. Business Objectives

A majority of companies surveyed have established telework policy. Virtual Desktop Infrastructure or Virtual Applications were the most common choice as a means to protect the data in transit and while displayed on a personally owned or other devices not owned by the organization. All of the organizations surveyed responded acknowledging that they are currently using or planning to use their devices to process sensitive information in support of their business objectives. This demonstrates that mobile devices are further expanding into and in some conditions serving a replacement of the traditional workspace.

b. Cost

Cost is a driving factor for most businesses to adopt any technology. Making an efficient affordable solution that addresses the void and satisfies a business need is vital. To gain the perspective of the organizations we asked what cost barriers they have encountered for deploying mobile technologies in their environment and gave them choices for Data Plans, Operational Support, Licensing and another option they could custom fill. A majority of organizations stated that data plans were at the top of the list driving up costs. Others noted operational support being the main roadblock while some even had no cost barriers whatsoever. The responses were very scattered and the data plan concern was the real only similarity. Understandably a main component of cost can be associated with a technology refresh rate. A 24 month refresh rate was the only commonality among responses.

c. Authentication/Protection Mechanisms

The authentication and protection mechanisms used to secure mobile devices and the information varied in offerings. Typically user name and password was standard practice, with exception of two organizations. These exceptions required either the use of PIN or VPN only. It is noted that the organization using PIN only is known to have a mature cyber security program. Others authentication services included Personal Identity Verification (PIV) card, biometrics, and token. Only one organization reported the use of both PIV card and biometrics in addition to their use of user name and password. Although the survey's data limited, an assumption maybe drawn that either this organization is evaluating multiple authentication and protection mechanisms or has established that requires enhanced authentication to access high value data.

d. Type of Device/Management

Device management was as varied as the types of devices in use. In nearly every case, a mobile device management service was in use and managed from within the company. Although few had reported that the BlackBerry Enterprise Server is in use, it was no longer the exclusive MDM use. This is consistent with the survey data that revealed that most organizations are supporting a combination of multiple platforms (Android, iOS, Windows, and BlackBerry). There were two exceptions where the organization exclusively used iOS devices. In those cases, the organizations relied on the Service Provider to provide the MDM service. Of these two organizations, one expressed high confidence in its ability to support both company issued and BYOD devices. While the other was less confident in the ability of the Service Provider to meet their policy needs.

e. Biggest Challenges

The majority of industry responses identified the legal and privacy challenges to implementing mobile devices within their organization. Configuration limitations on devices were cited as a close second. The diversity of device types make technical configuration difficult to map to policy was stated as other challenges. The Federal CIO Council study revealed gaps in security and privacy, policy, and legal issues as well as in supporting multiple devices and the cross-platform infrastructure.

IV. Summary

The mobile workforce's ability to access information and computing power improves information sharing, communication, and action response time for greater mission effectiveness. The potential for business enablement, specifically in how employees and partners interact provides an opportunity to rethink the way how business is conducted. The "untethered" mindset of operating an enterprise at the edge forces the need for ubiquitous connectivity. This freedom introduces new risk open new vulnerabilities that must be addressed through the introduction of a mobility strategy. The organizations surveyed demonstrated varying levels of maturity and confidence in the development of both a strategy and policy. As would be expected, confidence reached its highest point from those organizations that offer mobile security services as line of business to others. As mention within this report, MDMs were in use at most organization, allowing for the monitoring, management, and remote support of mobile devices deployed across the enterprise.

In conclusion, the rapidly change landscape of mobile devices, operating systems, services, and applications offers both great opportunity and peril. The development of a comprehensive strategy and

the promulgation of understandable and usable policy is a key to success. Included within the strategy is knowledge of share risk and the implementation of commonsense network and device security hygiene.

The questionnaire is attached as reference.

References

1. Digital Services Advisory Group and the Federal Chief Information Officers Council, **Government Use of Mobile Technology: Barriers, Opportunities, and Gap Analysis**, December 2012. https://cio.gov/cioc-blog/
2. Questionnaire on Mobile Technology – attached.

Questionnaire
On
Mobile Technology

AFCEA Cyber Committee

Version 1.0

November 2012

This page intentionally blank

PURPOSE

Executive Order No. 13571, issued April 27, 2011, directed Federal Government agencies, to take steps in consultation with the Office of Management and Budget (OMB) to improve the quality of Government services to the American people. As a result, the strategy document "Digital Government: Building a 21st Century Platform to Better Serve the American People" was created.
The AFCEA Cyber Committee, Subcommittee on Mobility is interested in industry's efforts to meet the challenges of mobility.

OBJECTIVE

The objective is to gain information and help address three aspects of the target audience mobile programs 1) opportunities 2) barriers and 3) setting the stage, for evaluating and developing a strategy on mobile technology. It is the assumption that mobility programs within the Federal space share some of the same issues as those in commercial sector.

REFERENCES

Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service," April 27, 2011
"Digital Government: Building a 21st Century Platform to Better Serve the American People" (Strategy), Office of the Chief Information Officer of the United States, May 23, 2012

MOBILE SECURITY

GENERAL INFORMATION

1. What is the size of your organization?

- ☐ Over 10,000 employees
- ☐ 1,000 to 10,000 employees
- ☐ 500 to 1,000 employees
- ☐ 50 to 500 employees
- ☐ Under 50 employees

2. Which business sectors does your company represent?
Service, Manufacturing, Technology, etc.

3. How much of your business is International?

- [ ] 80 to 100 %
- [ ] 30 to 80 %
- [ ] < 30 %
- [ ] None

4. Do you have a Telework policy? Yes No

SENSITIVITY OF WORK

1. Are you currently using or planning to use sensitive information on mobile devices in support of your business objective?

WORK LOCATION

2. What categories of users and work locations will you support?

AUTHENTICATION

3. What types of strong authentication are in use for or being investigated for mobile devices? Are they readily available solutions?

Mobile Device:

- [ ] User name and password
- [ ] PIV card
- [ ] Token
- [ ] Biometrics
- [ ] Other:

Mobile Application:

- [ ] User name and password
- [ ] PIV card
- [ ] Token
- [ ] Biometrics
- [ ] Other:

CONNECTIVITY

4. What forms of connectivity do or will you allow for mobile devices? (Cellular, USB, Bluetooth, Wi-Fi, Near Field Communications, etc.) Why?

5. Have you or will you modify the infrastructure to accommodate mobile devices? (networks, operational support, etc.)

☐	Yes
☐	No
☐	Uncertain
Please explain:	

PROTECTION

6. How will you protect mobile devices and the information being used? (for example, device integrity and data protection)

☐	Virtual Desktop Infrastructure or Virtual Applications
☐	Mobile Device Management Solution
☐	Encryption (data at rest and data in transit)
☐	Dual persona
☐	Other:

MANAGEMENT

7. How do you plan to manage mobile devices?

Specifically, what platforms will your program manage?

☐	Blackberry
☐	Apple iOS
☐	Google Android
☐	Windows Mobile
☐	GFE vs. BYOD
☐	Other:

8. Are there specific applications you are currently using or would like to use when managing mobile technologies (beyond office applications such as Word, Excel, PowerPoint, E-mail, and PDF)?

TECHNICAL LIMITATIONS

9. Have you found technical limitations to implementation of mobile technologies? (for example, legacy applications, constant network connectivity, requirements for secure voice, and infrastructure) How are you mitigating those limitations?

10. Of those listed in the answer to question 9, what are your biggest technical hurdles?

- ☐ Legacy Application
- ☐ Constant Network Connectivity
- ☐ Infrastructure Change
- ☐ Other:

APPLICATIONS

11. How will mobile device applications improve your ability to accomplish the business objective?

CONFIDENCE IN ABILITY TO SUPPORT POLICY

12. What is the level of your confidence in being able to meet your mobile device security policies?

For Company Issued:

- ☐ Very confident
- ☐ Confident
- ☐ Slightly confident
- ☐ No policy available

For BYOD:

- ☐ Very confident
- ☐ Confident
- ☐ Slightly confident
- ☐ No policy available

13. What are the biggest hurdles for establishing and implementing policies for mobile devices? Any known issues in the ability to support those policies? Please check all that apply:

- ☐ No policy
- ☐ Legal and privacy challenges
- ☐ Configuration limitations for devices
- ☐ Other (please specify):

COST

14. What cost barriers have you encountered for deploying mobile technologies in your environment? Please check all that apply:

- [ ] Data plans
- [ ] Operational support
- [ ] Licensing
- [ ] Other (please specify):

15. How are you handling "Technology Refresh" for mobile devices?

PILOT PROGRAM INQUIRY

What pilot mobility implementations or test beds do you currently have underway or planned? Please provide a summary description of each pilot program to include following information:

Department or Agency:	
Mission Supported:	
Number and type supported:	*(for example, executive, mobile office worker, field agent)*
Types of mobile devices used:	
Mode(s) of connectivity to main infrastructure:	*(for example, virtual desktop integration, virtual private network over the internet, dedicated virtual network, etc)*
Special applications supported:	
Mobile device management used and application store restrictions:	
Device configuration settings or restrictions:	
User device authentication methods used:	
Protections for data at-rest and in-transit:	
Start and dates for pilot:	