GOVERNMENT USE OF MOBILE TECHNOLOGY

Barriers, Opportunities, and Gap Analysis

DECEMBER 2012

Product of the Digital Services Advisory Group and Federal Chief Information Officers Council

Contents

Introduction

Mobile technology has become a key driver throughout information technology. The growth of the tablet market, user demand for smartphone technology, and rapid mobile device innovation are driving the future of our end-user computing platform. The use of mobile technology provides opportunities for innovation, agility and flexibility in the workplace.

Departments and agencies (agencies) should establish sound policies that define their mobile strategy, while accounting for an ever-changing technological landscape. To that end, Executive Order 13571[1] (Streamlining Service Delivery and Improving Customer Service), issued April 27, 2011, directed Federal agencies, in consultation with the Office of Management and Budget (OMB), to take steps to improve the quality of Government services to the American people. Under that Executive Order, the Digital Government Strategy[2] was released in May 2012 with three objectives:

- Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device;
- Ensure that, as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure, and affordable ways;
- Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people.

The Information Security and Identity Management Committee (ISIMC), by direction of the Federal CIO Council, chartered a Mobile Technology Tiger Team (MTTT) to address Milestone Action 10.2 of the Digital Government Strategy: “Evaluate opportunities to accelerate the secure adoption of mobile technologies into the Federal environment at reduced cost.” To address 10.2, the MTTT created a methodology for gathering information from different agencies to identify the following key considerations for the use of mobile technologies in the Federal Government:

- Opportunities and barriers;
- Gaps; and
- Risks, threats, and vulnerabilities.

In accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 1 (Draft), *Guidelines for Managing and Securing Mobile Devices in the*

1 http://www.whitehouse.gov/the-press-office/2011/04/27/executive-order-streamlining-service-delivery-and-improving-customer-ser
2 http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf

Enterprise (Draft),[3] the MTTT developed a framework for security analysis of mobile technologies based on essential components critical to centrally managing and securing mobile devices.

The MTTT identified the profiles of typically supported end-users (employees, executives, partners, and the public), stakeholder services (applications, identity and authentication, connectivity, management, and device protection), and other considerations (cost, technical, work location, sensitivity of work, confidence in ability to support policy, and compliance with other policies) that are critical to accelerating the secure adoption of mobile devices at reduced cost. These factors helped frame the mobile security analysis necessary to complete Milestone Action 10.2.

To develop this deliverable for 10.2, the MTTT conducted a survey and interviewed 21 agencies (including agency sub-organizations) on their use of mobile technologies. A summary of the results of the MTTT's interviews and information gathering, and identification and verification of barriers and opportunities (including a gap analysis), are presented in this document. The information gathered provides leading indicators that will be helpful in the development of requirements and architecture documentation. More detailed survey results will be made available to the Federal Government community.

3 http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Methodology

The MTTT developed a five-phase methodology to assess mobility barriers and opportunities and perform the gap analysis for Milestone Action 10.2. These phases included the following:

1. Identify stakeholders;
2. Develop questionnaire;
3. Conduct interviews;
4. Analyze data; and
5. Prepare report.

The MTTT methodology gave each agency response equal consideration. The dependency on agency cooperation and availability, in addition to time and resource constraints, led the MTTT to focus on identifying high priority issues and leading indicators.

Mobility Barriers and Opportunities

The MTTT identified a number of challenges and enablers that impact agencies' ability to deploy mobile technologies to meet mission requirements. Barriers are operational and technical challenges that inhibit the ability to provide Government information *"anytime, anywhere, on any device"*. Opportunities represent technology enablers for the secure delivery of information and services in a manner that complies with Federal requirements and mandates.

The results of the study indicated that all but one of the agencies and sub-organizations interviewed have expanded, or are planning to expand, user options for mobile technologies beyond current implementations of laptops and mobile devices, often including newer models of smartphones and tablet computing devices. While the impetus for examining mobile solutions is frequently driven by user demand, mission drivers were identified which include:

- Enhanced mobility and quicker access to information for a user population that is dispersed nationally and internationally;
- Ability to provide previously unavailable services and applications to support mission operations in the field;
- Increased resilience regarding concerns about relying on a single smartphone vendor; and
- Interest in examining the potential of using non-Government Furnished Equipment (GFE) for cost savings.

While there are many factors to consider when adopting any technology, the initial set of questions a Chief Information Officer (CIO) will ask falls into three main categories:

1. **Capabilities**. What capabilities or functionality and mission needs will be supported?
2. **Cost**. How much is the total cost of ownership (e.g., including planning, acquisition, and operations and maintenance costs)? and
3. **Security**. What are the relevant security requirements?

Although these areas have some overlap, the following sections discuss mobility opportunities and barriers for each of the three categories.

Category 1: Capabilities and Related Issues

Newer-generation mobile devices provide additional capabilities beyond voice, email, and calendar to present opportunities to enable a mobile workforce and deliver information and services to customers, partners, and the public, improving the ability to accomplish the agency's mission. These capabilities encompass a variety of commercially-available mobile devices, public and Government-developed mobile applications, a mobile application store, wireless connectivity options, and management of GFE (e.g., smart phones and tablets) and Government information.

Issues: The technical limitations of the product space of devices and management solutions can hinder the ability of agencies to develop and enforce the security and access policies required to implement mobile capabilities that fit their mission needs.

The MTTT identified technical limitations focused on the pace of technological change and relative immaturity of the product space, including mobile device management (MDM) solutions, mobile application stores, and the variety of device configurations. The issue of intermittent network connectivity was also raised as a barrier to delivery of web applications and a virtualized desktop, since both require a continuous network connection.

While agencies are already adopting Bring Your Own Device (BYOD) or similar policies within their organizations to support multiple device types, many agencies expressed concerns regarding the legal, privacy, and financial policies that need to be developed to support use of these new approaches. Furthermore they identified a need for guidance on the use of mobile devices in general, and specific guidance and decisions on BYOD reimbursement policies when Government work is performed using the device.[4]

A number of operational issues were also identified, with application store management and application vetting raised as top concerns. Other operational barriers identified were: infrastructure changes required to support mobile technologies; the challenges of migrating existing applications to mobile devices; and the lack of formal application development processes and guidelines for mobile application development.

Category 2: Cost and Related Issues

There is a cost associated with the deployment of any new technology. Exploratory or planning efforts should include a cost-benefit analysis to determine if the costs to acquire, operate, and maintain the technology are outweighed by the benefits projected to be realized from the technology. Agencies must perform a rigorous analysis to understand the costs associated with devices, data plans, applications, and supporting infrastructure, and quantify how the technology will improve their ability to accomplish their mission.

Issues: The lack of a Government-wide contract vehicle for devices and data plans was noted as a cost barrier. Some agencies are well into the planning stages for mobile technologies and will not delay deployment in anticipation of an acquisition vehicle. Another primary issue is the difficulty of performing a life cycle cost-benefit analysis to justify investment in mobile technologies. The rapidly changing maturity of the mobile marketplace and the relative immaturity of support infrastructure products may drive up costs as agencies have to support an increasing number of devices and products.

4 Under an earlier Digital Government Strategy deliverable, the Federal CIO Council and Digital Services Advisory group developed government-wide BYOD guidance based on lessons learned from successful BYOD programs launched at forward-leaning agencies: https://cio.gov/wp-content/uploads/downloads/2012/09/byod-toolkit.pdf.

Category 3: Security and Related Issues

Security enables mobile computing when it can provide strong user authentication, access controls and encryption protection for sensitive data and applications, bringing the data to the user and breaking down the barriers and limitations of fixed work locations. This requires that agencies determine information sensitivity and align it with appropriate security methods that will protect the information from unauthorized access and ensure that employees have access to the information needed to do their jobs.

Issues: Limited options for strong authentication and data encryption are the most significant short-term barriers to secure adoption of mobile technologies. As the pace of technology advancement continues to increase, standards and processes must be updated and new technologies developed to allow the continued use of Commercial Off-The-Shelf (COTS) products, giving government users access to the latest technologies to meet their missions without sacrificing privacy and security.

The lack of validated encryption modules to secure data on mobile devices impacts the ability to have sensitive information protected on these devices and creates challenges for agencies to comply with requirements and meet their mission needs. Many agencies expressed concern with the length of time associated with the validation process, typically performed by independent laboratories. Ultimately, market forces determine the cost of validation and speed in which encryption modules can be validated.

Current devices and standards for Personal Identity Verification (PIV) authentication to mobile devices pose challenges given the difficulty in using two-factor authentication methods on mobile devices. Most agencies expressed strong interest in using derived credentials, pending release of standards and guidance on use. NIST understands these issues and has been developing guidance to help with the implementation of PIV authentication mechanisms and the use of derived credentials.[5]

Currently, it is challenging to configure mobile devices to meet security requirements across multiple platforms and operating systems. The lack of consistent configuration guidance for mobile devices and their rapid refresh cycle make it difficult to develop operating system hardening configurations for mobile devices.

5 In July 2012, NIST released for comment the Revised Draft Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification of Federal Employees and Contractors. FIPS 201-2 introduces the concept of a PIV-derived credential to accommodate the use of mobile devices that cannot work with contact card readers. Going forward, NIST will be working with ISIMC to ensure alignment with this approach, which will also be reflected in NIST Special Publication 800-157, Guidelines for Personal Identity Verification (PIV) Derived Credentials. When final, FIPS 201-2 and NIST SP 800-157 will help agencies meet the Federal mandate and help make progress to meet these challenges.

Gaps

The study highlighted a number of important gaps in various areas which need to be addressed to enable more effective use of mobile technologies to meet Government missions. These gaps include:

- **Security and Privacy**. Gaps exist between Federal security and privacy requirements and the availability of products that implement the required protections:
  - User authentication: Lack of a robust user identity authentication mechanism that complies with Federal mandates and maintains mobile device ease of use;
  - Data encryption: Growing need for validated, secure and efficient cryptography suitable for mobile devices;
  - Application security testing and evaluation: Lack of automated tools for efficient assessment and authorization of mobile applications;
  - Device Sanitization: Lack of agency processes and tools to follow requirements on device sanitization.
- **Policy and Legal**. There will need to be a continued focus on ensuring that existing policies accommodate agency needs in mobility:
  - Guidance and best practices for mobility: More robust engagement mechanisms should be created to help share best practices for mobile devices and supporting tools across the Federal enterprise;
  - Business and technical requirements: Lack of identified mission use cases and technical requirements that are consistent across the Federal landscape;
  - Legal: Lack of legal precedence, policies or guidance established on electronic discovery of information on mobile devices related to mixed official and personal use for both GFE and BYOD (e.g., compensation, liability for data or equipment loss, etc.).
- **Application and Infrastructure**. Gaps exist between the goals of supporting multiple devices and the cross-platform infrastructure needed for applications and devices:
  - Legacy applications: Lack of compatibility and ease of use accessing legacy applications from mobile platforms has hindered access to data and the overall transition to mobility;
  - Infrastructure for MDM and application distribution: Lack of cross-platform compatible industry solutions that satisfy Government authentication, security, and management requirements;
  - Network connectivity: Lack of adequate wireless data network through Wi-Fi or cellular data to always allow networking capabilities for the mobile worker relying on mobile applications.

As a result of this study, several key areas and themes emerged which require focused attention in the near term:

1. **Mobile Device Management**. Improvements in tools and processes are necessary to support enterprise-level configuration management and controls for Federal agencies.
2. **Application Services**. Better tools and processes are needed to accredit and distribute applications required for Government missions, leveraging commercial market cycles, and commercial and Federal application stores. NIST will release guidelines soon to provide a methodology for testing and vetting third-party applications that are distributed through various app stores.
3. **Identity Access Management**. The use of the PIV standard for user authentication is not well supported by existing products. Implementation of FIPS 201-2 and NIST SP 800-157 will require focused attention to ensure proper implementation and market support for user authentication tools.
4. **Improved Governance and Standards**. The Federal Government must work collaboratively with industry to bridge the security gaps present in today's smart phones, tablets, and other mobile devices, while continuing to identify policy and legal issues that may need to be addressed to accommodate these new technologies and better fulfill agency mission requirements.

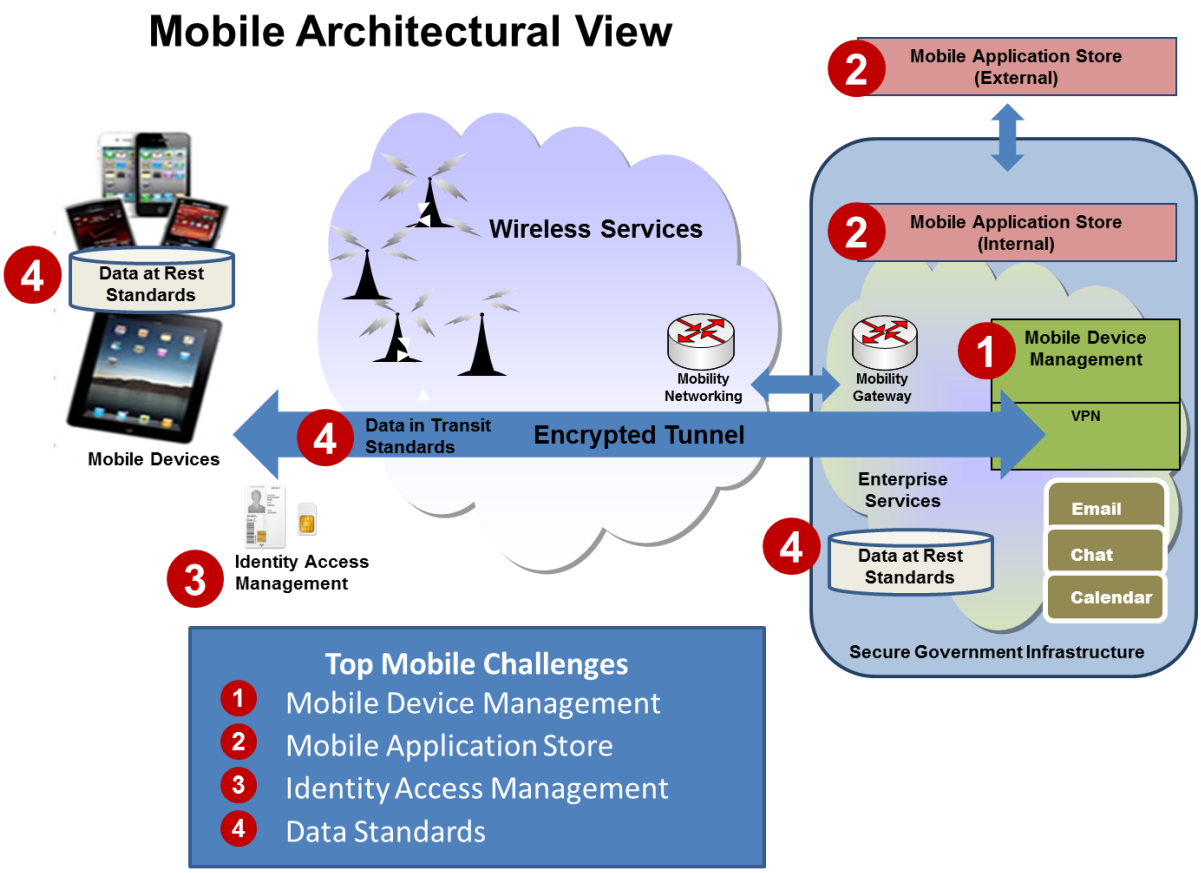

Figure 1

Figure 1 depicts the key areas or themes that have emerged from this study to address Milestone Action 10.2 of the Digital Government Strategy. These four challenges are the major areas which agencies have consistently identified as primary concerns for mobility. Mobile Device Management (MDM) involves improvements in tools and processes necessary to support enterprise-level configuration management and controls for Federal agencies. Mobile Application Store (MAS) consists of application services which include better tools and processes to accredit and distribute applications for Government missions, leveraging commercial market cycles, and commercial and Federal application stores. Identity Access Management (IAM) and data standards include user authentication and encryption solutions that meet Federal requirements.

Conclusion

Agency senior executives understand that the use of mobile devices and tools is an immediate challenge, not one on the distant horizon. Agencies are already moving ahead with implementation of mobile technology and some are currently accepting the risks of the gaps identified in this report. Based on input from agency interviews along with the assessment framework and gap analysis, several key recommendations were made to streamline the secure adoption of mobile technology. These recommendations include:

- Define requirements for MDM and MAS around various use cases. Requirements will help reinforce mission-related use case selections and priorities, assist in procurement activities, and address the urgent need for agencies to evaluate their pilots before making larger investments.
- Establish a cross-functional team to evaluate the technical, legal, privacy and other factors associated with the use of non-GFE. Waiting for legal precedence on these topics is resulting in agencies accepting increased risk.
- Continue development of a mobile computing decision framework which adds a methodical approach to determining mobile solution implementation and collaborate with Federal entities and standards organizations on the development of mobility standards and a Federal mobile reference architecture.
- Develop either Federal-wide or agency policy and guidance to support more flexible use of commercial mobile devices, and develop an acquisition strategy for procurement of mobile technologies that comply with Government-wide policy, emerging standards and requirements.
- Continue development of requirements and recommendations to enable the use of strong authentication and encryption to accelerate the use of mobile devices in a secure manner.

As agencies begin to evaluate mobile solutions to satisfy user demand and address mission needs, Federal CIOs and other senior executives will determine additional actions necessary to facilitate the cost-effective and secure use of mobile devices, and provide guidance regarding standards for device selection, refresh periods, plan selection, validation, and security. It is essential that agencies continue to develop an understanding of the missions, use cases, and impacts beyond the initial innovation of mobility.

In the next phase of Digital Government Strategy implementation, several deliverables will help address some of the recommendations presented in this document. For example, the mobile security reference architecture encompassed in Milestone Action 9.1 will include use cases that will help the Federal Government adapt policy, accept technology, and provide risk management requirements that better match the use of mobile innovation. The reference architecture will help agencies maintain data security, protect the Federal enterprise, and allow for acceptable risk based on mission requirements. The government-wide MDM platform (Milestone Action 5.5), models for the delivery of commercial mobile applications into the Federal environment (Milestone Action 5.4), and shared mobile app development program (Milestone Action 3.6) will also help agencies adopt secure, cost-effective mobile solutions.