# FEDERAL MOBILE COMPUTING SUMMIT

AUGUST 12, 2015 | RONALD REAGAN BUILDING | WASHINGTON, DC

On behalf of the Advanced Technology Academic Research Center, I am proud to announce the release of a White Paper documenting the MITRE-ATARC Mobile Collaboration Symposium held on August 12, 2015 in Washington, D.C. in conjunction with the ATARC Federal Mobile Computing Summit.

I would like to take this opportunity to recognize the following session leads for their contributions:

**MITRE Chair:** Pat Benito

**Challenge Area 1: Mobile App Vetting Tools & Trends**
**Government Lead:** Vincent Sritapan, DHS S&T
**Industry Lead:** Adam Salerno, Veris Group
**MITRE Lead:** Drew Buttner

**Challenge Area 2: Mobile Pilot Challenges and Lessons Learned**
**Government Lead:** Jacob Parcell, GSA
**Industry Lead:** Nicolas Tempestini, Accenture
**MITRE Lead:** Marie Collins

**Challenge Area 3: Access Control Patterns for the Mobile Device World**
**Government Lead:** Paul Grassi, NIST
**Industry Lead:** Ben Andreas, Intercede
**MITRE Lead:** Mark Russell

**Challenge Area 4: Internet of Things**
**Government Lead:** Eric Simmon, NIST
**Industry Lead:** Craig Ano, Samsung
**MITRE Lead:** Dave Keppler

**Challenge Area 5: Mobilizing Legacy Government Applications**
**Government Lead:** Peter Chin, U.S. Courts
**Industry Lead:** Stu Hammer, HP Enterprise Services
**Industry Lead:** David Park, HP Enterprise Services

**Challenge Area 6: Mobile Capabilities for Field Data Collection**
**Government Lead:** Rob Farley, USDA APHIS
**Government Lead:** Pam Hird, USDA NASS
**Industry Lead:** Kelly Bennett, Adobe

Below is a list of government, academic and industry members who participated in these dialogue sessions:

### Challenge Area 1: Mobile App Vetting Tools & Trends

Nathaniel Becker, U.S. Army; Jon Johnson, GSA; Darryl Morris, MITRE; Sarah Mahgoub, DOE; Barry Nash, MITRE; Jon Peterson, DOS; Terri Phillips, MITRE; Nicole Seamands, Census; Shoaib Sherwani, U.S. Army; Angelos Stavrou, Kryptowire; Yasir Syeed, Red Hat

### Challenge Area 2: Mobile Pilot Challenges and Lessons Learned

Josh Bentley, Red Hat; Pam Bodart, CFTC; Tony Ellis, NCTC; David Fern, SSA; Nick Fisher, Lookout; Jermaine Hawkins, OPM; Tracy Minter, DHS CBP; Carlton Northern, MITRE; Charlie Yang, NOAA

### Challenge Area 3: Access Control Patterns for the Mobile Device World

Cori Asaka, DHS CBP; Cameron Hernandez, NIH; Hyong Ngo, USDA APHIS; Cathy Graziose, NRC; James Kim, USN SPAWAR; Alec Squaire, DOJ; Neil Sethi, VA; Mike Lawlor, Peace Corps; Nick Stablein, Samsung

### Challenge Area 4: Internet of Things

Larry Coleman, DHS; Frederic de Vaulx, NIST; Brian Deyo, Peace Corps; Josh Dixon, Samsung; Carey Erickson, GSA; Ryan Fetterman, DoD; Chris Folk, MITRE; Brett Fox, DOJ; Yolanda Gayol, Fielding Graduate University; Tim Howard, NSF; Jacques Malebranche, GSA; Mike Maurer, Accenture; David McClure, NOAA; Moses Namara, University of Maryland, College Park; David Peters, GSA; Brett Pfrommer, DHS CBP; Tiffany Sargent, Intel; Charles Sun, EXIM; German Vazquez, DOJ; Paul Worsham, DHS TSA;

### Challenge Area 5: Mobilizing Legacy Government Applications

Joshua Lashbrook, DLA; Jeff Williams, DLA

### Challenge Area 6: Mobile Capabilities for Field Data Collection

Pam Carpenter, Adobe; David Crabtree, MITRE; Patricia Meyertholen; ED; Luis Nataniel, ED; Hyong Ngo, USDA APHIS; Jared Ondricek, MITRE; David Rogers, Mobilegov; Julio Rodriguez, ED; Mikhael Schlossman, DHS FEMA; Matt Schrader, Adobe; Jordan Thomas, Census;

Thank you to everyone who contributed to the MITRE-ATARC Mobile Collaboration Symposium. Without your knowledge and insight, this White Paper would not be possible.

Sincerely,

George Thomas Suder

Tom Suder
President, Advanced Technology Academic Research Center (ATARC)
Host organization of the ATARC Federal Mobile Computing Summit

# August 2015 Federal Mobile Computing Summit Collaboration Session Summary

*Tom Suder, Tim Harvey*
*ATARC*

*Mike Peck, Gaurav Seth, Mark Russell, Patrick Benito, Marie Collins*
*The MITRE Corporation*

**Approved for Public Release; Distribution Unlimited. Case Number 15-3849**

**The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author**

## Executive Summary

The Federal Mobile Computing Summit took place in August of 2015. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, and discuss prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

The Collaboration Sessions covered three key mobility topics:

- Access Control Patterns for the Mobile World
- Mobile Pilot Challenges and Lessons Learned
- Mobilizing Legacy Government Applications

This white paper summarizes the results of the Collaboration Sessions and provides detailed actionable recommendations for Government and academia, which are summarized in the table below.

Continue to evaluate access control solutions that have proven effective in private sectors such as finance, and the potential to adopt out-of-the-box solutions that provide adequate security.

- Generate feedback that can be shared with the private sectors to help build common public/private requirements that can be shared with vendors so they can work towards better standardization of cryptographic interfaces in commercial mobile devices

Create an informal Government group to share lessons learned and best practices that come out of these pilots to reduce redundant costs and improve the overall effectiveness of government mobility.

- Agencies from across the federal government should routinely come together to share, and document, past, current and future efforts to identify partnerships and efficiency opportunities.

Development a Government wide modernization lessons learned and best practice guide will help agencies learn from each other as they modernize their legacy IT to support mobility.

- This should include feedback on technical approaches, and products to allow agencies to pick from proven technologies and practices.

Create a community built around Government, industry, and academic collaboration to leverage potentially previously untapped academic resources to help advance Government mobility.

- Leverage graduate and undergraduate level research to help solve critical mobility challenges, while attracting students to public service and preparing them for a future career.

## Table of Contents

**1 Introduction ........ 4**

**2 Collaboration Session Overview ........ 4**

**3 Federal Mobile Computing Summit Collaboration Sessions ........ 5**

**3.1 Session 1: Access Control Patterns for the Mobile World ........ 5**

3.1.1 Discussion Summary ........ 5

3.1.2 Recommendations ........ 8

**3.2 Session 2: Mobile Pilot Challenges and Lessons Learned ........ 8**

**3.3 Session 3: Modernizing Legacy Apps ........ 8**

3.3.1 Discussion Summary ........ 9

3.3.2 Recommendations ........ 9

**4 Summary & Recommendations ........ 10**

# 1 Introduction

The Federal Mobile Computing Summit took place in August of 2015 in Washington, D.C. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, discuss the main challenge areas in mobility, and discussed prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks. The discussions were Government focused and at a high-level, not addressing any specific solution and only identifying features of potential solutions or frameworks.

As part of the Collaboration Sessions, MITRE and ATARC invited academia to participate in each of the four challenge areas, and asked participating academics to identify courses of action to be taken to enable improved Government and industry collaboration with academic institutions.

This white paper summarizes the results of the Collaboration Sessions and identifies suggestions and recommendations for Government and academia while identifying crosscutting issues that tie between the different challenge areas.

# 2 Collaboration Session Overview

MITRE and ATARC created an outreach and collaboration process to crowd-source the development of recommendations to key Government challenges. This process focuses on soliciting input from a diverse group of participants and exploits their diverse backgrounds, points of view, and skillsets to create new, novel, and innovative recommendations to key problems.

Each MITRE-ATARC Collaboration Session was a focused and moderated discussion between Government, industry, and academic representatives centered on key mobile challenge areas that were solicited from the Government prior to the event.

The challenge areas are as follows:

- Access Control Patterns for the Mobile World
- Mobile Pilot Challenges and Lessons Learned
- Mobilizing Legacy Government Applications

Participants discussed current problems, gaps in current and planned work programs, potential solutions, and ways forward for each of the challenge areas. Section 3 outlines the goals, outcomes and summary of each of the three collaboration sessions.

# 3 Federal Mobile Computing Summit Collaboration Sessions

The outcomes of the four Collaboration Sessions are included in this section. This section elaborates on the Session goals, a summary of the discussions, and identification of relevant outcomes.

## 3.1 Session 1: Access Control Patterns for the Mobile World

This session featured a discussion of the problems, challenges, and emerging solutions for securely providing access to Government enterprise resources to mobile device users. The goals of the session were to:

- Identify current challenges in authentication and authorization of mobile users
- Discuss recent technology and policy changes and how they could help agencies
- Discuss lessons learned and successes from agency mobile pilots
- Identify areas where Government needs are not being met by current solutions

### 3.1.1 Discussion Summary

The session began with a discussion of the evolution of enterprise access control from the client/server environment to the current state of mobile and cloud integration. Traditional desktop authentication and single sign-on (SSO) protocols can provide a seamless user experience across multiple enterprise applications and systems. However, they depend on tight coupling and established trust between clients and enterprise authentication systems, and were typically not designed for the risk environment of public networks. As the demand to support access to enterprise applications and data from commercial smart phones, tablets, and other devices has exploded, IT departments have been challenged to connect new device types to enterprise systems. Most of these devices do not support the access control mechanisms that traditionally worked in the desktop realm, and many government systems have not evolved to support new models. While they are maturing, commercial mobile devices still lack open Cryptographic Service Provider (CSP) interfaces. The mandate to use Personal Identity Verification (PIV) credentials for authentication posed further challenges, since smart cards are not easily integrated with mobile devices. Providing access to enterprise data and applications on mobile devices while maintaining data security, requiring strong authentication and authorization, complying with Federal IT policy, and delivering a good user experience has proven to be an immense challenge for many agencies.

Much of the discussion focused on user authentication challenges. The represented agencies are mainly using PINs and/or passwords for device screen or “secure container” unlock, with one agency reportedly using Apple’s TouchID fingerprint sensor to unlock devices. Some participants cited a lack of clarity in federal authentication policy as an issue; in particular, the definition of “multi-factor authentication" and specific requirements for implementing it have been the subject of significant debate.

A repeated theme of this discussion was the need to balance usability and security concerns, especially with authentication mechanisms. While a user might log onto a desktop and then go to get coffee before expecting to be productive, mobile devices are expected to provide immediate availability when needed. They also may be used frequently for very short periods (e.g., to quickly check weather, message feeds, or status information) and need to be unlocked repeatedly. Onerous requirements like complex passwords, especially difficult with cramped on-screen keyboards, severely hamper the usability of devices, as does the need to fumble with hardware components such as smart card readers or one-time password tokens. Users also have a tendency to work around these difficulties. One participant related a story where a user had left his one-time password token at home with a publicly-accessible web cam pointed at it, so that he could obtain the current code from anywhere without having to carry the token.

There was significant interest in Derived PIV Credentials, a relatively new government standard for provisioning Public Key Infrastructure (PKI) credentials onto mobile devices using hardware or software cryptographic modules. Derived PIV Credentials provide an alternative to the PIV card that is designed for mobile use while still meeting the Homeland Security Presidential Directive 12 (HSPD-12) PIV mandate. Some agencies have begun pilots and proof-of-concept deployments of Derived PIV Credentials, but integration challenges remain. The lack of common CSP interfaces on mobile devices requires the integration of proprietary vendor Software Development Kits (SDKs) with each mobile app that will use the credential. Operating System (OS) provided cryptographic keystores are another option, but many do not meet policy requirements including FIPS certification and security measures required by policy. Integration with enterprise services, many of which are not PKI-enabled and rely on desktop SSO for authentication, also can be problematic. At the same time, Enterprise Mobility Management (EMM) vendors are beginning to advertise Derived PIV Credentials solutions, but some do not understand the numerous policy requirements of PIV and related standards, warranting caution in evaluating vendor claims of compliance. Agencies are working through these issues, and Derived PIV Credentials remain a promising technology for enterprise mobile authentication.

PIV authentication over Near-field Communications (NFC) is another alternative supported by recent policy updates. In this approach, the PIV card communicates directly with the device over the near-field radio connection, with the advantage that no additional hardware is needed and no new credentials need to be issued and managed. Typically, agencies will need to re-issue PIV cards with models that support the new Virtual Contact interface in order to use NFC. The unavailability of the NFC radio on iPhones for third-party application use somewhat limits the applicability of the solution, but NFC radios are common on Android and Windows

Phone devices. However, compatible software able to communicate with the card over the wireless interface is still required on these platforms.

Multiple participants also expressed a need to provide access to different classes of non-organizational user populations including other government agencies, state and local government partners including law enforcement, and in some cases the public at large. While Derived PIV Credentials can only be issued to current PIV holders, a similar mobile credentialing scheme could be used to provision trusted credentials to these users. In these cases, agencies need to weigh the benefits of provisioning credentials to these users against the potential to accept federated authentication, if the partner organization has the capability. Another question is what certificate policy would be used to issue these credentials. The new policy identifiers added to the Federal Common Policy for Derived PIV enable the issuance of credentials that can be accepted across government without further identity proofing, but its use is limited to PIV cardholders. No analogous policy exists for non-PIV users.

Some agencies are currently using biometric authentication, in the form of Apple's TouchID fingerprint authentication system. Many users prefer fingerprint authentication to PIN or password entry, and these systems can typically also support remote network authentication (e.g., to authenticate mobile payments). All commercial device fingerprint scanners are prone to attacks through "lifting" an authorized user's fingerprints. However, the security of these systems should be evaluated in relation to alternatives; they likely compare favorably to the use of a short PIN, for example. More importantly, not all implementations are equal, and some have serious weaknesses enabling theft of fingerprint images through software compromise of the device. Agencies should carefully research these solutions before adopting them. These solutions face some policy challenges, such as the stipulation that a Derived PIV Credential must be unlocked with a PIN (not a biometric), and their use for network authentication is not supported by policy. There is no standard means, for example, to convey the assurance of the biometric or how it was registered and measured to a remote host.

A wide range of emerging technologies for mobile access control were discussed. An industry group called the Fast IDentity Online (FIDO) Alliance is developing standards for strong authentication from mobile devices that support the use of biometrics and other authenticators, and eliminate reliance on simple password-based authentication. The FIDO work provides standard interfaces for client and server applications, providing an end-to-end standard with industry backing. Though the FIDO standards are currently incompatible with federal authentication policy, the potential to create a FIDO profile that would comply with federal PKI policies is being explored.

The group discussed access control models including Attribute-based Access Control (ABAC), Risk-adaptive Access Control (RAdAC), delegated authorization with OAuth and UMA, and federated authentication with OpenID Connect. ABAC is extensively used in certain environments, but government use of these other models remains relatively minor. Perhaps one reason is that many agency mobile initiatives remain focused on providing basic messaging and office automation functionality. There is general agreement that mobile devices will eventually deliver a range of mission-focused applications, but in many cases this has not yet occurred. Perhaps the coming years will see a transition from the current "remote access" paradigm to one of Application Program Interfaces (APIs), where more advanced access control models will be a requirement.

### 3.1.2 Recommendations

- OMB should provide agencies with clearer guidance on access control requirements, particularly in the area of "multi-factor" authentication
- Government should continue to evaluate access control solutions that have proven effective in other sectors such as finance, and the potential to adopt out-of-the-box solutions that provide adequate security
- Vendors should work towards better standardization of cryptographic interfaces in commercial mobile devices is needed to enable better interoperability of solutions and eliminate the need for explicit one-off vendor integration efforts
- Academic institutions should combine usability and human factors elements into security related engineering courses to help train young engineers the art and science of designing user friendly security features

## 3.2 Session 2: Mobile Pilot Challenges and Lessons Learned

This session discussed mobility pilots across the government and identified key lessons learned and challenges that need to be overcome to run a successful mobility pilot. This session focused on capturing lessons learned and recommendations that span people, process and technology. This information was codified into a companion document, Mobile Pilot Best Practice Guide.

## 3.3 Session 3: Modernizing Legacy Apps

As the Federal government moves toward a mobile workforce, legacy government applications and supporting backend infrastructure, such as case management systems, need to be mobilized to meet the needs of workers in the field. This session examined the strides made by agencies in mobilizing legacy applications and discuss the challenges faced during these projects. The goals of the session were to:

- Understand the challenges with modernizing legacy applications for mobile use
- Capture best practices and lessons learned from agencies going through this process

### 3.3.1 Discussion Summary

The session began with a discussion on some of the key challenges associated with modernizing legacy applications. The top challenges include modernizing the legacy backend, ensuring a good user experience as applications are ported for mobile devices from laptop/desktops, creating a cost effective testing program, and making sure internal engineering processes are able to be flexible enough to evolve with the fast evolution of mobile technology.

For each of the key challenge areas, the participants shared lessons learned around each of the key challenges:

- Lessons learned for modernizing legacy backend
    - Not all legacy backend IT (e.g., web services, app servers, security software) needs to be modernized. Analyzing your agency's backend IT can help to identify which portions must be migrated, could be migrated, or don't need to be migrated
    - Upgrading legacy backend IT at once, or in very large upgrade cycles, can be very disruptive, expensive, and can lead to major issues due to cost, and complexity. Small, continuous upgrades have proven to be more effective and allows an agency to learn and improve in smaller, less disruptive, cycles
- Lessons learned on ensuring a good user experience
    - Focus on functionality to drive modernization. Not every app or feature works on mobile, nor should every app or feature be ported to a mobile application
    - Build in user feedback mechanisms within mobile apps to drive features, and prioritize user feedback
    - Don't fall into "electronic tiller" mindset, new IT will drive new innovation. A good modernization program will allow users and engineering teams to innovate to
    - Support for offline especially for apps used in the field and factor in designing apps to define typical data transfer
    - Leverage built-in device capabilities, and innovate around different input methods – handwriting, voice recognition, etc.
- Lessons learned on making sure internal engineering processes are able to be flexible enough to evolve with the fast evolution of mobile technology
    - If an agency is conducive to Agile, move to Agile methodology and have frequent releases
    - Embrace commercial techniques such as DevOps, continuous integration (CI) and continuous deployment (CD) to facilitate smaller updates, and allow your agency to be more agile in how it responds to needs and changes

### 3.3.2 Recommendations

- Conduct assessments to determine what needs to be modernized, and what does not need to be modernized

- Develop strategy and implementation plan for mobile & legacy jointly between business/mission owners and IT owners that includes:
    - Prioritized list of needs
        - Includes return on investment assessment
    - Resource estimates to mobilize legacy IT
    - As-is and to-be technical views, with gap assessments
    - User engagement plan to ensure users influence future direction of modernization
    - IT development and maintenance plans that include modern practices such as Agile, DevOps, and CI/CD
    - Workforce training and management plan to transition legacy developers to new style of IT development

# 4 Summary & Recommendations

Several key recommendations emerged as a result of the three Collaboration Sessions. Firstly, Government should continue to evaluate access control solutions that have proven effective in private sectors such as finance, and the potential to adopt out-of-the-box solutions that provide adequate security. These evaluations can help generate feedback that can be shared with the private sectors to help build common public/private requirements that can be shared with vendors so they can work towards better standardization of cryptographic interfaces in commercial mobile devices, leading to better interoperability of solutions and eliminate the need for explicit one-off vendor integration efforts.

Secondly, as more agencies look to adopt mobility and conduct pilots, it will become even more important to share lessons learned and best practices that come out of these pilots to reduce redundant costs and improve the overall effectiveness of government mobility. Agencies from across the federal government should routinely come together to share, and document, past, current and future efforts to identify partnerships and efficiency opportunities.

Thirdly, development of a Government wide modernization lessons learned and best practice guide will help agencies learn from each other as they modernize their legacy IT to support mobility. This should include feedback on technical approaches, and products to allow agencies to pick from proven technologies and practices.

Fourthly and lastly, create a community built around Government and industry collaboration with academia to leverage potentially previously untapped academic resources. The proposed community will enable communications between the different participating communities. The outcomes of this community include:

- Academia produces higher quality, better-prepared, and "industry-ready" graduates for hire

- Government leverages graduate and undergraduate level research to help solve critical mobility challenges
- Government organizations have an integrated research and advisory capability made up of commercial companies, academic institutions, and federally funded research and development centers (FFRDC)

# Mobile Pilot Best Practice Guide

*Tom Suder, ATARC*
*tsuder@atarc.org*

*Tim Harvey, ATARC*
*tharvey@atarc.org*

*Patrick Benito, The MITRE Corporation*
*rbenito@mitre.org*

*Marie Collins, The MITRE Corporation*
*mcollins@mitre.org*

**Approved for Public Release; Distribution Unlimited. Case Number 15-3849**

**The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author**

This page intentionally left blank.

# Background

The Federal Mobile Computing Summit took place in August, 2015 in Washington, D.C. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, discuss the main challenge areas in mobility, and discussed prominent challenge areas in mobility.

As part of the Collaboration Sessions, MITRE and ATARC invited academia to participate in each of the four challenge areas, and asked participating academics to identify courses of action to be taken to enable improved Government and industry collaboration with academic institutions.

This white paper summarizes the results of the Mobile Pilot Challenges and Lessons Learned Collaboration Session and provides suggestions and recommendations for Government agencies as they plan and execute mobility pilots.

# Lessons Learned

The following list identifies some of the key lessons learned from pilot efforts:

- Devices
  - The more homogenous the devices, the easier operations and management will be in the longer term. For the pilot, test multiple device types using a diverse user group to drive towards identifying the one, or two, that best meets most needs. It should be noted that there is no single device that will satisfy all needs.
  - Backend infrastructure product (e.g., mobile device management, mobile app store) integration is more important than the device – pick product first and then choose device. Most do this the other way around and it's much harder to fit a product to a device and infrastructure, whereas devices change very frequently.
- Users
  - Make sure people in the pilot are motivated to participate and continuously use the device – user engagement and feedback is key to a successful pilot. It is a good idea to get users to sign agreements outlining roles and responsibilities, and also provide them with information to let them know their feedback matters, and is driving future development. It is also helpful if rewards can be given to those who actively participate.
  - Have actual users participate in the pilot and are able to respond to surveys (e.g., very hard to get feedback from senior level executives).
  - Users, including system administrators and help desk support staff, may not be familiar with new products and devices. Train users and consider giving them a sandbox and time to learn about the new mobile capabilities so they can effectively support the pilot.

    - It is a good practice to have one or two human factors engineers involved in the pilot to measure the user experience of the devices and software. Providing a poor user experience is a key factor that can lead to a mobile project's failure.
- Scaling
    - One agency ran a small pilot and discovered it did not scale well to full rate production. Performance issues encountered when hit over 10,000 devices. When designing a pilot, make sure that you use a representative environment, and are able to run tests to identify potential scalability issues.
- Security
    - Security is critical. The pilot should consider both technical, policy, and legal ramifications of deploying mobility, and make sure the high risk areas are included in the pilot.
    - It is a good practice to have security technical profiles in place before piloting and refine these during the pilot. This includes data protection, user authentication, data at rest (DAR), and data in transit (DIT) profiles.
    - Have security engineer/administrator involved early and during the pilot. The security controls may not be the same for the pilot and operational infrastructure.
    - Think about how to authentic to devices and use the pilot to figure out the optimal solution. Identity and access management (IdAM) can be technically challenging, and if the user experience is hindered by poor IdAM technology, users will either not use the device, or bypass certain security protections.
    - DoD logistics (e.g., IA approval and architecture design) tend to be the biggest hurdles.
- Infrastructure
    - Will everything be on premise or use cloud services? Run the pilot as you would for production because there are differences between cloud and on premise deployments.
    - Leverage existing infrastructure as much as possible, for example one agency just used device as handset to existing VoIP architecture
    - Always-on VPN doesn't work well because it kills the battery quickly.
    - A mobile device management (MDM) capability is critical for the pilot. Without one, you will be blind and can't ensure users aren't changing the security settings.

Look at all the things that need to be procured and start the procurement and IA processes in parallel to planning the pilot. Don't commit to pilot start date until devices in hand and infrastructure ready.

## Recommendations

Mobile capabilities span technology, people and organizations, policy and governance. It is important to understand the complete mobile vision and frame the pilot to answer the key questions and mitigate key risks involved in achieving the vision. The following is a sampling of recommended activities to consider for developing a mobile vision, strategy and pilot.

1. Develop Mobility Strategy:
    - What are you looking to do on mobile devices? Are there any “unique” needs of the organization?
    - What is the sensitivity /required handling of the data on the device?
    - Are you integrating mobility into the enterprise?
    - What is your device strategy: company/government owned or BYOD or Hybrid approach?
    - Do you plan to build mobile applications? For internal use, external use, or both? Use a mobile application store (MAS)?
    - What are the current IA related requirements? Any other security policies?
2. Collect Mobile Requirements:
    - Any current information system requirements which are valid on mobile devices?
    - Any new requirements based on your mission needs plus mobile operating system/device type?
    - Develop infrastructure, MAS and MDM requirements
    - Consider app development strategy and requirements
    - Leverage requirements from known published requirements (NIAP, DISA, NIST, etc.)
3. Develop Mobile Governance Model:
    - Define security approach
    - Define mobile business model
    - Develop device polices
    - Define organization roles and responsibilities
4. Define the Mobile Pilot Architecture
    - How will the pilot architecture integrate into the enterprise, or will it be isolated
    - Consider scalability as you define the pilot architecture with particular focus on existing gateways/perimeter security .
5. Develop and Assess Pilot Capabilities and Candidates:
    - Create detailed pilot plan with the objectives, test plan and metrics.
    - What are the mobility architecture alternatives to assess?
    - Test, Integrate, and Evaluate COTS products
        - Many vendors offer free trials which could be leveraged in a pilot
    - Infrastructure Integration: Based on current core components (AD, IIS, Exchange, DNS etc.), should the solution be on premise or on the cloud?
6. Execute Pilot and Capture Feedback:
    - Pull together a panel of staff to define and execute pilot (e.g., 1 security, 1 Engineer, 2-3 Infrastructure/backend administrators)

    - Define scenarios/tests to perform, calling out specific applications and functionality to use, with expected results and have users execute tests, record results with ratings
    - Structure the feedback mechanism, such as a survey, to collect feedback from users – need a balance of technical/user/security related feedback

7. Pilot Metrics:
    - Metrics can be hard to collect, especially if the system doesn't have support for doing it automatically (e.g. logging)
    - Performance is hard to evaluate in a small pilot
    - Good idea to run a penetration test with the device – can someone break in? What are the vulnerabilities?
    - Examples of metrics
        - User satisfaction
        - Usability of devices
        - How many users
        - How often device, apps, features used
        - What features, apps specifically using
        - Amount of time takes to fix data spillage, recover lost device, or identify if a device is in violation of security policy or jail-broken