FEDERAL MOBILE COMPUTING SUMMIT

OCTOBER 4, 2016 | MARRIOTT METRO CENTER | 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 October 4, 2016 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 Innovation
Government Lead: Jacob Parcell, GSA
Industry Lead: Nick Psaki, Pure Storage
Industry Lead: Uzi Eilon, Perfecto Mobile
MITRE Lead: Marie Collins

Challenge Area 2: Mobile Technology Roadmap: What's Next?
Government Lead: Vincent Sritapan DHS S&T
Industry Lead: Steve Taylor, Intel
MITRE Lead: Jeff Stein

Challenge Area 3: Identity and Access Management: Moving Towards Continuous Authentication
Government Lead: Phil Lam, NIST
Industry Lead: Ben Andreas, Intercede
MITRE Lead: Mark Russell

Challenge Area 4: Patterns of Success for Deploying Mobility
Government Lead: Rick Jones, GSA
MITRE Lead: Darshan Kadam
MITRE Lead: Mike Schoenfeld

Challenge Area 5: How Mobile Technology is Transforming Healthcare
Government Lead: Yvonne Cole, DoD-VA IPO
MITRE Lead: Duy Huynh

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

Challenge Area 1: Mobile Innovation

Mark Allen, GSA; Tarek Almiski, CBP; Kenneth Bennett, FBI; Robert Ellington, DOT; Kristia Hayes, DOT; Kelvin Jackson, DOJ; Frank Kidd, DOL; John Reece, CBP; Matthew Seitz, NGA; Dzuy Tran, Perfecto Mobile; Hung Trinh, DoD-VA IPO; David Wellington, DoD-VA IPO; Julie White, DoD-VA IPO

Challenge Area 2: Mobile Technology Roadmap: What's Next?

Barry Bazemore, JIDA; Jonni Burnham, DOT; Ronald Davis, NIH; Cesar Fausto, VA; Rush Filson, MITRE; Rajon Gilmore, DOS; Chelsea Gulaskey, DOS; Tom Harrell, NIH; Viet Le, DISA; Ken Luersen, FEMA; Jerome Madlock, OPM; Pradip Mazumder, DHS; Rebel McFetridge, CBP; Qing Mu, MITRE; Qais Nassiri, CBP; Thomas Ogden, DOS; Suro Sen, GSA; Fabiola St-fort, EPA; Jason Van Sice, Perfecto Mobile; Jimmy Word, DoD-VA IPO

Challenge Area 3: Identity and Access Management: Moving Towards Continuous Authentication

Ira Baron, DOJ; Michael Cull, TSA; Kevin Curran, Intercede; Jason Dudash, Red Hat; Corey Evans, GAO; Ambyr Fowler, BLM; Paul Harper, Intercede; Jamila Moore, DISA; Richard Parris, Intercede; Brett Pfrommer, CBP; Joe Portner, MITRE; Andy Pyles, MITRE; Christopher Quamina, BLM; Mike Ross, DoD-VA IPO; Meg Slesinger, Intercede; Stephanie Wolfram, DOS

Challenge Area 4: Patterns of Success for Deploying Mobility

Kelly Adams, GSA; William Berg, DHA; Ken Blount, DoD-VA IPO; Allison Burrey, DoD-VA IPO; Jordene Chabuk, GSA; Brian Farrell, DOS; Susan Gabriel-Smith, BLM; Andrea Glanville, USN; Paul Hill, TSP; Heath Marell, FBI; Charley Motter, Concur; Sean Rada, Rigil; Heather Scrudato, USCG; Kamran Shah, USCG, Marques Tibbs-Brewer, Concur

Challenge Area 5: How Mobile Technology is Transforming Healthcare

Mark Bellezza, VA; Tim Besecker, Perfecto Mobile; Yvonne Cole, DoD-VA IPO; John Cuddehe, Lookout; Anne Dalton, DHS; Debi Davis, MITRE; Miguel Gomez, HHS; Steven Kator, DoD-VA IPO; Mike McHugh, DOJ; Cathylynn Metcalf, DoD-VA IPO; John Morrison, Samsung; Christopher Muir, HHS; Noel Richards, NSA; Marc Schneider, MITRE; Gaurav Seth, DoD-VA IPO; Harold Smith, Monkton; Gilda Walker, DOS

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,

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

October 2016 Federal Mobile Computing Summit Report[*]

Patrick Benito, Marie Collins, Duy Huynh, Darshan Kadam, Mark Russell, Mike Schoenfeld, Jeff Stein
The MITRE Corporation[ϒ]

Tom Suder & Tim Harvey
The Advanced Technology Academic Research Center

[ϒ] The authors' 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 authors.

Table of Contents

1 Executive Summary

The Federal Mobile Computing Summit includes 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 for key challenge areas were identified by session participants. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

Participants representing government, industry, and academia addressed five challenge areas in federal mobile computing: Mobile Innovation, Mobile Technology Roadmap: What's Next?, Identity and Access Management: Moving Towards Continuous Authentication, Patterns of Success for Deploying Mobility, How Mobile Technology is Transforming Healthcare.

This white paper summarizes the discussions in the Collaboration Sessions. Drawing from these discussions, MITRE and ATARC developed the following actionable recommendations for the government, academia, and industry:

Increase Government Participation in Open Source Community
Collaborative communities built around open source software and hardware projects has proven to be a valuable source of innovation. Innovation successes such as Google's Android Open Source Project, Appcelerator's Titanium, and Apache's Cordova benefited from collaboration and contributions from the open source community.

Government agencies should, where feasible, modify policies to mimic 18F's approach, where the default position to make new projects free and open source software (FOSS). Injecting projects into the open source community allows for non-traditional contributors (e.g., academia) to submit technology and ideas that help to spur innovation and advance government mobility. An added benefit of open source projects is that it will lay the foundation for government and industry to develop a common understanding of government's mobility requirements.

Continue Joint Commercial/Academia/Government Mobile Roadmap Brainstorming
Joint roadmap planning across commercial, academia, and government benefits all parties involved. Commercial agencies benefit by understanding the needs of the government, and can help align their product roadmaps to government needs. Academia benefits by gathering information to target new research. Government agencies benefit by gathering important information and ideas to better shape their roadmaps, and identify partnership opportunities with other government agencies and academic institutions.

Government agencies should identify forums to bring commercial companies and academic institutions together on a routine basis to develop and refine their mobility roadmaps. Data generated in the Federal Mobile Summit provides a good starting point for agencies to create (or refine) their mobile roadmaps.

Continue Evaluating New Industry-Backed Authentication Technologies

Mobility continues to be driven by the consumer and private sector. Evaluating new authentication technologies that have the backing of industry, such as the Fast Identity Online (FIDO) protocol, will help identify solutions that meet governments' requirements. Adopting authentication technologies that are backed by industry, will allow the government to take advantage of innovation in the market and implement new authenticators with less cost than government-specific standards and technologies.

Government should invest in a joint industry and academia initiative to: 1) Become more active in authentication standards efforts to help shape future standards, and 2) Establish an underwriter laboratory-like group to evaluate industry authentication products to gauge suitability for government use.

Define a Maturity Model for Government Mobility to Guide Agency Adoption

Feedback gathered during the Summit suggests there is no consensus for a definition of a government organization with a mature mobile enterprise. Furthermore, some participants indicated their mobility efforts are still in the early stages, and a framework to guide investments to mature mobility programs would be helpful.

Defining -- and measuring -- a government organization's mobile maturity remains a gap within the government. The government should initiate a light weight effort to define a maturity model, for agencies to use in the planning, execution and evaluation of a mobility program. An initial set of building blocks were developed during the Summit to feed such an effort.

2 Introduction

During the most recent Federal Mobile Computing Summit, held on October 4th 2016, five MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in mobile computing. Subject matter experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of mobile computing technologies and research in the government. Participants ranged from the CTO, CEO, and other executive levels from industry and government to practitioners from government, industry, and MITRE to researchers, students, and professors from academia.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs)[1]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology[2]. MITRE works in partnership with ATARC to host these collaborative sessions as part of the Federal Mobile Computing Summit. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in mobile computing, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a way to help guide research efforts, curricula development, and to help produce graduates ready to join the work force and advance the state of mobile computing research and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, industry, and academia while identifying cross-cutting issues among the challenge areas.

3 Collaboration Session Overview

Each of the five MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

1. Mobile Innovation
2. Mobile Technology Roadmap: What's Next?
3. Identity and Access Management: Moving Towards Continuous Authentication
4. Patterns of Success for Deploying Mobility
5. HealthTrac: How Mobile Technology is Transforming Healthcare

[1] https://www.mitre.org/about/corporate-overview

[2] http://www.atarc.org/about/

This section outlines the goals, themes, and findings of each of the collaboration sessions.

3.1 Mobile Innovation

Initiatives like DIUx, SOFWerx, ATARC Innovation Labs, and MASS Innovation Bridge are becoming popular to help accelerate innovation and connect the government with companies developing advanced technology. This session helped develop ideas and recommendations from the academic and commercial sectors for agencies to use when in creating future mobile innovation initiatives.

3.1.1 Session Goals

The goal of this session is to identify ideas and recommendations on how to bring mobile innovation to the government. Goals include:

- Develop recommendations on moving the government away from employing mobile technologies using traditional approaches used by desktops to a transformational one with that provides a true mobile experience
- Identify ideas on how to generate awareness within industry and academia on government challenge areas in mobility
- Define how the government can better engage industry to understand what they can offer

3.1.2 Session Summary

The session started with a discussion on approaches that different agencies have taken resulting in mobile innovation. Department of Labor (DOL) shared their competitions, providing data to the public and awarding prizes for the best solution. The benefit is low cost and broad reach. Customs and Border Patrol (CBP) talked about the valuable results from their hackathons. There was discussion on Defense Information Systems Agency (DISA) Rapid Innovation Fund, an innovative program funded out of the DOD Office of Small Business Programs (OSBP) to fund innovative technologies in support of the American warfighter. National Geospatial-Intelligence Agency (NGA) shared their Innovative geoInt app provIder program (Igapp). This program connects agencies to a qualified pool of registered application ("app") developers. The developers create apps that are then tested, evaluated and measured against customers' needs and posted on the app store. There was discussion on the desire for more government innovation labs and grand challenges for experimentation where the user community is engaged early on to get feedback and refine needs.

The discussion then shifted to identifying approaches for industry to understand government needs/challenges so they can share what solutions are available. DARPA was identified by industry as defining a good, actionable set of requirements in their broad area announcements (BAA), and that the financial institutions also provide a good model to follow where well defined requirements are included in requests for proposals (RFP). This contrasts with some agencies and industries that provide an exhaustive set of

requirements, which is difficult for industry to work with.

There was also discussion on how to move the Government from employing mobile technologies using traditional approaches used by desktops to a transformational one that provides a true mobile experience. There was a suggestion to capture "mobile moments", i.e. do an analysis of what users do and where mobile can enhance this. Assign a Mobile Innovation Group to identify these needs and using mobile developers who will make use of mobile features will transform them to mobile solutions.

3.1.3 Recommendations

The Mobile Innovation collaboration session participants identified the following recommendations:

- Government agencies should attend industry (e.g., financial, healthcare) shows/conferences that include mobility. Designing innovation requires routine engagement to see what others in the industry are doing. Government needs, in many cases, are not much different than other sectors and they will value from these industry conferences
- Government needs to increase participation in the open source community. The open source community embraces, and helps drive innovation.
- Invest in innovative approaches for mobile solutions such as coding competitions, hackathons[3], innovation events/labs
- Encourage government engineers to participate in local, regional, and national hackathon events to gain exposure to new, and non-traditional ideas
- Engage non-profit groups, such as Code for America[4], that foster innovation and work in the public interest
- Model requirements documentation after how DARPA BAA and the financial sector RFP approaches – industry indicated these are easier formats to work with and lead to more favorable outcomes because of this

3.2 Mobile Technology Roadmap: What's Next?

CIOs and CTOs need to stay on top of emerging technology that has the potential to disrupt government and commercial mobility so they can adequately plan for its adoption. This session collected thoughts on the next set of disruptive mobile technologies from commercial, government, and academia and created a series of technology roadmap inputs that Federal CIOs and CTOs can use in their mobility roadmap planning.

---

[3] https://en.wikipedia.org/wiki/Hackathon

[4] https://www.codeforamerica.org/

3.2.1 Session Goals

The goal of this collaboration session was to bring together government, industry, and academia to build a technology roadmap of disruptive emerging technologies in the mobile space for agencies to use in their mobile roadmap efforts.

3.2.2 Summary

The session began with a discussion of the mobile ecosystem as defined by the National Institute of Standards and Technology (NIST)[5]. Expanding the NIST definition to include the Internet of Things (IoT) the group chose to focus on six key technology areas: Device, Networks, Apps, Device + OS Infrastructure, Enterprise, and IoT.

After laying out the ecosystem the session examined an existing technology roadmap that The MITRE Corporation had prepared for DISA as a starting point. The moderators affixed a large five-foot poster divided into three sections to the wall. Using stickie notes participants would callout, discuss an affix suggested technologies to either the Current, Near term, Far term columns.

Current was defined as technologies that current exist in the private sector but are not widely used in the government. Near term was defined as technologies that have a clear path to market but are not yet readily available, and Far term encompassed both theoretical technology and technology still in the infancy of research.

Once the roadmap was populated a second poster was brought where each time-period was subdivided into the six sectors representing each sector of the mobile ecosystem. Moderators and participants worked together to sort the technologies into the appropriate sector.

3.2.3 Recommendations

At the end of this session the group generated the below Mobile Technology Roadmap. The Mobile Technology Roadmap collaboration session participants recommend that agencies who are in the process of developing, or updating, their technology roadmaps leverage the inputs below.

Device Technologies		
Current	*Near Term*	*Far Term*

[5] http://csrc.nist.gov/publications/drafts/nistir-8144/nistir8144_draft.pdf

• Device as Credentials • Fingerprint Authentication • HCM LOA-4 (Host Credential Mapper – Level of Assurance[6]) • CAC-PIV Derived Credentials LOA-3 • Mobile Sensors (IR, Sound, Video)	• Improved Battery Technology • Perceptual Computing • Strong Authentication • Device to device sharing of mobile threat intelligence	• Voice ID for Universal Device • Modular Phone • Device Generated Intelligence • Continuous Authentication

Network Technologies		
Current	*Near Term*	*Far Term*
• 4G/LTE • Bring your own device (BYOD) • LMR (Land mobile radio) / Push-To-Talk • Multi-waveform radios • VOIP VXX-600	• Li-Fi • FirstNET Implementation • High Bandwidth, High resiliency backhaul at tactile edge	• 5G • Encrypted Bluetooth (wearables) • Phone as cloud processors • Ad-Hoc mobile cloud networking

[6] For more details on Level of Assurance see: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

App Technologies		
Current	*Near Term*	*Far Term*
• Mobile Test Farm • Cloud Storage (e.g. Box.net, Dropbox) • Emergency Warning Apps • NIAP App Development Platform • Instant Apps • Context Awareness • Tele-medicine / Tele-government • Mobile App API for FedRAMP (L4, L5, L6 Content)	• Uber style app for summoning Drones or Robots (MULE) • Emergency Management (IPAWS) • Identity management of the public for Government Services (connect.gov)	• Continuous App Vetting • Simultaneous Location and Mapping (SLAM)

Device + OS Infrastructure		
Current	*Near Term*	*Far Term*
• Encrypted SMS • Mobile Virtual Device Infrastructure (VDI)	• Mobile Type 1 Hypervisor	• Multi-Level Security (MLS) Devices

Enterprise Technologies		
Current	*Near Term*	*Far Term*
• Enterprise Mobility Management (EMM) • Mobile backend as a service (MBaaS) • DevOps Tools • On Demand Dev & Test Environment • Hypervisor based virtual app deployment • Mobile DevOps • Mobile/Remote Helpdesks	• GeoFencing for EMM • Mobile for CDM	• None

Internet of Things Technologies		
Current	*Near Term*	*Far Term*

• IoT Mobile Security • Mobile Health Sensing • Wearables (watch) • Swarming technology for Drones • Conductive Textiles	• IoT Enabled Security • IoT Protection Profiles • IoT failing safely • Mobile Med PAC pack vehicle	• IOT Security • Smart Contact Lens • UAS + Mobile / Drones

3.3 Identity and Access Management: Moving Towards Continuous Authenticatio

This session featured a discussion of emerging trends in Identity and Access Management (IdAM), agencies' goals and challenges for authentication and authorization of mobile device users, and recommendations on how to move the government forward to stronger credentials and access control.

3.3.1 Session Goals

The goals of the session were to:

- Discuss challenges agencies are facing with authentication as well as innovation in the product space, and identify opportunities and gaps
- Discuss upcoming changes to the government's digital authentication guidelines
- Come up with recommendations and strategies for agencies to adopt and manage stronger authentication methods

3.3.2 Session Summary

The session began with a discussion of major revisions being made to NIST special publication 800-63, a key set of guidelines for how agencies should perform digital authentication. An early draft of the latest 800-63-3 revision has been posted to GitHub for public collaboration, and includes significant changes. Notably, the Levels of Assurance (LOA) scheme for analyzing the strength of an authentication transaction has been redesigned, splitting it into the components of identity proofing, credential strength, authentication protocols, and federated authentication. Previously, these different factors were combined in a single LOA rating. Other changes include considerations of remote identity proofing and strict new password requirements along with a strong recommendation to avoid password authentication altogether. Citizen-to-government interactions where personal information is changed will also require multi-factor authentication.

The group then discussed different methods for continuous authentication of mobile device users. Traditionally, users authenticated to systems to establish a session lasting until the user logs out or exceeds an inactivity timeout. Authenticated sessions are at risk of unauthorized access due to session hijacking or physical access (e.g., device theft).

Continuous authentication addresses this risk by authenticating users throughout their interactions with the system. Factors used to authenticate the user, frequently used in combination, can include:

- Comparing the user's usage of the device (e.g., commonly used apps and services) to an established profile
- Tracking the device's location and movements and comparing them to an established profile
- Biometric measurements including gait, iris, voice, or device interactions such as the angle at which the device is held, pressure used to tap and drag, etc.
- Proximity tokens (e.g., Bluetooth), which in some cases also measure a biometric such as heart rate

Some of these factors depend on a training period, in which a profile of the user's typical behavior is built as a baseline to which future actions can be compared. The group recognized the potential of these techniques to address the risks associated with lost or stolen mobile devices. However, no one in the group had real-world deployment experience with these technologies, and agencies seem to be struggling with more basic issues. Some early adopters have begun to deploy Derived PIV Credentials, but integration with enterprise systems has proven difficult and many agencies still rely on PINs or passwords and authentication of the device by a Mobile Device Manager (MDM). Some agencies are making use of biometric sensors integrated with mobile devices, such as Apple's Touch ID, but these implementations are not well integrated with enterprise IdAM systems. Some concerns over the adoption of continuous authentication included:

- Questions as to the maturity and practicality of current-generation products, along with cost, staffing, and training considerations
- Concern over the irrevocability of biometric authenticators that have been compromised
- Privacy concerns over behavioral profile-based models, particularly with persistent location and movement tracking
- The rapid introduction of new modalities such as gait and touch-screen interaction profiles without extensive testing of error rates

Some other prevailing IdAM challenges include difficulties in using credentials across government agencies, as well as sharing identity proofing and vetting information, which leads to duplicate provisioning and repeated proofing of the same individuals at different agencies, and in some cases between departments in the same agencies. Many agencies also have not categorized their data and systems according to risk levels, which severely limits their ability to implement fine-grained or risk-based authorization policies.

Given the current state of IdAM and challenges facing agencies, the consensus view was that while continuous authentication shows promise, agencies are still dealing with more basic issues in mobile IdAM in the near term.

3.3.3 Recommendations

The group identified the following recommendations to continue to evolve the government's IdAM capabilities:

- Implement a cross-government identity proofing and clearance capability, or at least improve capabilities for sharing of information across agencies, to reduce the duplication of effort across agencies
- Though agencies have made some progress in accepting authentication credentials from other agencies, continue to develop these capabilities using standard federation protocols
- Develop a government strategy for identity proofing and authentication of members of the public for authentication to government services
- Continue to evaluate new authentication technologies that have the backing of industry, such as the FIDO protocol, to enable the government to take advantage of innovation in the market and implement new authenticators with less cost than government-specific standards and technologies

3.4 Patterns of Success for Deploying Mobility

This session focused on the best practices of deploying mobility within an organization and its challenges due to the increasing complexity of mobile enterprise solutions, and the fast evolution of mobile technology.

3.4.1 Session Goals

- Identify the challenges for driving a federal agency to a mobile digital workplace
- Describe the building blocks of a mature federal agency mobile digital workplace

3.4.2 Session Summary

Attendance for this collaborative session included representatives from eight government agencies. Several contributors conveyed their insight and perspective on their organization's mobility initiatives, however, the number of attendees that did not see their respective organizations moving forward with mobility was surprising. These people were looking for information on how mobility could help their organizations and how to initiate mobility programs from a leadership or as an individual contributor.

The challenges identified for deploying mobility varied; however, there was an overriding theme that a mobility champion, within leadership, must be found that understands the significant benefits of a mobile workplace and is willing to make the investments required for success. The procuring of the appropriate technical expertise within an organization was a significant roadblock to the challenges of mobile device management, internal development, app store management, security, privacy, and 508 considerations. These technical challenges can be overwhelming to attempt and tackle them all at once.

The discussion shifted and focused on how difficult it is to balance the short-term (tactical) needs for mobility with the long-term (strategic) planning. This can be a challenge for any initiative. However, the nature of mobility: disconnected devices;

multiple device manufacturers, platforms and OS versions; and the endless form factors enforce the need to standardize the management of devices, app development, app vetting, and security practices. A strategic plan that is disseminated and evangelized top-down is essential or an organization will chase the ever-accelerating mobile technology unsuccessfully.

Other challenges brought up over the course of the afternoon included: meeting the high expectations of (internally developed) business app end-users that are sophisticated users of personal mobile apps. Additional challenges mentioned: standardizing the app deployment process; finding secure and reliable authentication practices (e.g. derived credentials); finding cost effective methods to mobilize legacy applications; and orchestrating all organization stakeholders to move the agency's mobility initiative forward effectively and efficiently.

Many of the attendees indicated their agency's mobility initiatives were immature when compared to the private sector. There were also some questions surrounding the characteristics of an agency with a mature mobilized workforce. Defining and measuring an agency's mobile maturity, remains a gap within the government.

3.4.3 Recommendations

The session recommends the government define a maturity model, to help guide agency adoption of mobility, and help measure how mature mobility is within an organization. The group developed the initial set of building blocks, shown below, to feed into a future mobile maturity model analysis and development effort. There was not enough time during the collaboration session to develop an exhaustive set of building blocks or associated building block metrics to provide further insight into an organization's maturity. The group recommends refining these building blocks, and identify relevant metrics (focused around effectiveness and efficiency) to further define an organization's mobile maturity.

Governance Building Blocks
• Enterprise mobility mission problem definition and vision
• Enterprise mobility tactical and strategic plan
• Enterprise mobility policy and defined, repeatable, processes
• Centralized mobile project tracking
• Operational mobile governance board and mobile center of excellence
Technical Building Blocks
• Enterprise mobility reference architecture
• App vetting, deployment tools and platforms
• App lifecycle management, 508 and security compliance processes
• Enterprise mobile device management
• Enterprise mobile development platform
• Enterprise business API bus
• Enterprise mobility shared services

3.5 HealthTrac: How Mobile Technology is Transforming Healthcare

The HealthTrac session is an enduring session at the Federal Mobile Summit, hosted by the DoD/VA Interagency Program Office (IPO). This particular session deviated from the routine collaboration session format, to take advantage of an opportunity to have a detailed review of an emerging standard being developed by the NIST National Cybersecurity Center of Excellence (NCCoE). NIST NCCOE presented their Special Publication (SP) 1800-1: DRAFT Securing Electronic Health Records (EHRs) on Mobile Devices. This SP is broken into the following sections:

- SP 1800-1a: Executive Summary
- SP 1800-1b: Approach, Architecture, and Security Characteristics
- SP 1800-1c: How-To Guide
- SP 1800-1d: Standards and Controls Mapping
- SP 1800-1e: Risk Assessment and Outcomes

The intent of this session was to educate the audience on the draft standard, answer questions, and collect any feedback. The details of the SP are out of scope for this report, as the report can be found at the URL outlined above. There were some key discussion points worth highlighting:

- A common concern is that some clinicians work in multiple clinical settings, and they are forced to carry and manage multiple devices, which is not desirable. One approach to simplify provide EHRs access is via Bring Your Own Device (BYOD) scenario. BYOD is out of scope for this SP series. However, concepts could be borrowed for a BYOD effort. Specifically, access to the EHRs could be provided via mobile browser using the web based Transport Layer Security (TLS) encryption. Prior to providing access to EHRs, the device/user could be authenticated using 802.1X EAP TLS to provide additional layer of TLS encryption. This approach also mirrors dual encryption methodology recommended within NSA's commercial solutions for classified (CSfC) recommended approach
- There are no set implementation requirements that address how the PHI data should be secured on mobile devices *and* ensure interoperability across government agencies (e.g., DoD & VA). Interoperability guidance and associated standards are still needed within the government healthcare community
- There is a need for an independent group, like NIAP, to assess and approve commercial products for use with EHR

4 Conclusion & Summit Recommendations

As with past Federal Mobile Summits, the collaboration sessions discussions had a common set of themes. While the cultural barriers to adoption, rapid advancement of mobile technology and accompanying user demand for bleeding edge technology, and security remain, success stories are emerging from government adoption efforts. With

continued collaboration and sharing, establishing success stories and best practices is becoming more common-place and mobile adoption is becoming easier for government agencies.

Drawing from the discussion and content generated during the Collaboration Sessions, MITRE and ATARC developed several key overarching recommendations:

Increase Government Participation in Open Source Community
Collaborative communities built around open source software and hardware projects has proven to be a valuable source of innovation. Innovation successes such as Google's Android Open Source Project, Appcelerator's Titanium, and Apache's Cordova benefited from collaboration and contributions from the open source community.

Government agencies should, where feasible, modify policies to mimic 18F's approach, where the default position to make new projects free and open source (FOSS). Injecting projects into the open source community allows for non-traditional contributors (e.g., academia) to submit technology and ideas that help to spur innovation and advance government mobility. An added benefit to open source projects, is that it will lay the foundation for government and industry to develop a common understanding of government's mobility requirements.

Continue Joint Commercial/Academia/Government Mobile Roadmap Brainstorming
Joint roadmap planning across commercial, academia, and government benefits all parties involved. Commercial agencies benefit by understanding the needs of the government, and can help align their product roadmaps to government needs. Academia benefits by gathering information to target new research. Government agencies benefit by gathering important information and ideas to better shape their roadmaps, and identify partnership opportunities with other government agencies and academic institutions.

Government agencies should identify forums to bring commercial companies and academic institutions together on a routine basis to develop and refine their mobility roadmaps. Data generated in the Federal Mobile Summit provides a good starting point for agencies to create (or refine) their mobile roadmaps.

Continue Evaluating New Industry-Backed Authentication Technologies
Mobility continues to be driven by the consumer and private sector. Evaluating new authentication technologies that have the backing of industry, such as the FIDO protocol, will help identify solutions that meet governments' requirements. Adopting authentication technologies that are backed by industry, will allow the government to take advantage of innovation in the market and implement new authenticators with less cost than government-specific standards and technologies.

Government should invest in a joint industry and academia initiative to: 1) Become more active in authentication standards efforts to help shape future standards, and 2) Establish an underwriter laboratory-like group to evaluate industry authentication products to gauge suitability for government use

Define a Maturity Model for Government Mobility to Guide Agency Adoption
Feedback gathered during the Summit suggests there is no consensus for a definition of a government organization with a mature mobile enterprise. Furthermore, some participants indicated their mobility efforts are still in the early stages, and a framework to guide investments to mature mobility programs would be helpful.

Defining, and measuring, a government organization's mobile maturity, remains a gap within the government. The government should initiate a light weight effort to define a maturity model, for agencies to use in the planning, execution and evaluation of a mobility program. An initial set of building blocks were developed during the Summit to feed such an effort.

5 Acknowledgements

The authors of this paper would like to thank The Advanced Technology Academic Research Center and The MITRE Corporation for their support and organization of the summit. The authors would also like to thank the session leads and participants that helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the FedSummits web site.