atarc

FEDERAL MOBILE COMPUTING SUMMIT

APRIL 6, 2016 | GRAND HYATT | 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 April 6, 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 DevOps
Industry Lead: Josh Beard, AppDynamics
Industry Lead: Uzi Eilon, Perfecto Mobile
MITRE Lead: Mike Schoenfeld

Challenge Area 2: Continuous Mobile Integration
Government Lead: Brian Deyo, U.S. Peace Corps
Industry Lead: Joseph McKairnes, Silanis Technology
Industry Lead: Chris Taylor, Entrust
MITRE Lead: Jeff Stein

Challenge Area 3: Mobile App Vetting Strategy
Government Lead: Josh Franklin, NIST
Industry Lead: Tim LeMaster, Lookout
MITRE Lead: Carlton Northern
MITRE Lead: Mike Peck

Challenge Area 4: Secure Components of Mobility
Government Lead: Donovan Cozzens, U.S. Marine Corps
Government Lead: Chris Magaha, CSfC PMO
Industry Lead: Josh Dixon, Samsung
Industry Lead: Robert Nowak, Apriva
Industry Lead: Reinhard Schumak, Apperian
MITRE Lead: Michelle Casagni

Challenge Area 5: Mobilizing Legacy Government Applications
Industry Lead: Brian Love, Booz Allen Hamilton
MITRE Lead: Joe Portner

Challenge Area 6: Mobility Solutions to Enhance Citizen Engagement
Government Lead: Mike Pulsifer, U.S. Department of Labor

Academic Lead: Dr. Sukumar Ganapati, Florida International University
Industry Lead: Rohit Gupta, Artemis Consulting
Industry Lead: Eric Uhlir, Deloitte Digital
MITRE Lead: Matt Pollack

Challenge Area 7: How Mobile Technology is Transforming Healthcare
Government Lead: Nick Bogden, U.S. Department of Veterans Affairs
MITRE Lead: Marie Collins

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

Challenge Area 1: Mobile DevOps

Indhu Balasubramaniam, HHS FDA; Rolando Estrada, DHA; Michael Frascella, DOS; Evan Lee, U.S. Courts; Amanda Markovich, DOS; Hoa Pham, Artemis Consulting; Jeremy Ray, U.S. Courts; Chad Rossi, GSA; Neil Sethi, VA; David Stenger, GSA; Ben Yu, HHS FDA

Challenge Area 2: Continuous Mobile Integration

Brian Blankenship, Deloitte Digital; Jim Brown, VA; Joseph McKairnes, eSignLive; Dan Miller, Entrust; Punit Patel, VA; Jenna Reed, Deloitte; Ajay Singh, Deloitte

Challenge Area 3: Mobile App Vetting Strategy

Robert Aitken, DOS; Tony Andreoli, U.S. Navy; Cynthia Black, DISA; Kevin Do, DOS; Sean Frazier, MobileIron; Mike McHugh, DOJ; Barry Nash, MITRE; Kristina Kelly, DHS; Malachi Outen, DISA; Rob Palmer, DHS; Jon Peterson, DOS; Terri Phillips, MITRE; Dale Sesvold, DOJ; Nick Singer, NGA; Joseph Smith, U.S. Army; Vincent Sritapan, DHS; Salome Teweldes, DOS; Robert Zimmerman, DOS

Challenge Area 4: Secure Components of Mobility

Chris Barnes, DISA; Luis Coronado, Jr., DSS; Larry Crosland, GAO; John Cuddehe, Lookout; Bob Ellington, DOT; Timothy Havighurst, Apriva; Chris Hazelton, Apperian; Paul Hill, TSP; Xiaoyang Lee, DHS; Ervine Li, BLS; Kelly Miller, NRO; David Nolan, DHS; Jordan Packham, GSA; Noel Richards, NSA; Stephen Rossero, USAID; Amelia Rudisill, DISA; Nick Stablein, Samsung; Suro Sen, GSA; Douglas Thompson, U.S. Army; Jeff Williams, DLA

Challenge Area 5: Mobilizing Legacy Government Applications

Kyle Bradshaw, DOS; Roger Fritzel, DOD; Yancey Hall, Booz Allen Hamilton; Richard Jones, GSA; Eugene Kim, DISA; Andrew Moore, U.S. Coast Guard; Pattabhi Nunna, Booz Allen Hamilton; Risa Ohara, Artemis Consulting; Josh Welle, Crossdeck; John Veiga, GSA; Jianmei Wu, DISA

Challenge Area 6: Mobility Solutions to Enhance Citizen Engagement

Mike Lawlor, U.S. Peace Corps

Challenge Area 7: How Mobile Technology is Transforming Healthcare

Kelly Adams, GSA; J. Danielle Cunningham, DHA; Jaya Rao, PricewaterhouseCoopers; Gaurav Seth, DOD/VA IPO

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

2016 Federal Mobile Computing Summit Report

Patrick Benito, Michelle Casagni, Marie Collins, Carlton Northern, Mike Peck, Matt Pollack, Mike Schoenfeld, Jeff Stein
The MITRE Corporation[1]

Tom Suder & Tim Harvey
The Advanced Technology Academic Research Center

[1] 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 seven challenge areas in federal mobile computing: Mobile DevOps, Continuous Mobile Integration, Mobile App Vetting Strategy, Secure Components of Mobility, Mobilizing Legacy Government Applications, Mobility Solutions to Enhance Citizen Engagement, and How Mobile Technology is Transforming Healthcare.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government, academia, and industry while identifying intersecting points among challenge areas. The sessions identified actionable recommendations for the government, academia, and industry which are summarized below:

Create Government Wide Repository of Success Patterns, and Tools to Help Agencies Operate More Agilely in Mobility
Organizational and technology agility is key to success. More enterprise data needs to be exposed for mobile consumption, and more business processes should involve mobile devices. Rapid development tools and techniques need to be pervasive in the government community, along with associated process and a culture that fosters agile development to respond to changing user needs and technology.

Creating a repository with lessons learned and enterprise licenses for modern continuous integration and DevOps tools can be useful to help entice federal agencies to adopt and maintain modern mobile software development practices.

Create Partnerships with Universities to Identify Novel Approaches to Existing Mobility Problems
Academia can provide strong technical resources and insights into the challenge areas discussed. To alleviate the burden on the government, academics should be included in the mobile research and innovation efforts to provide high quality technical input from a different vantage point. Qualified mobile engineers (software & hardware) are in high demand, and universities can help provide access to researchers and work with government to identify high value concepts that are beneficial to both parties.

Increasing partnerships with academic institutions that specialize in engineering and healthcare can help to find novel approaches to healthcare related mobility challenges.

Creating a federal wide list of key healthcare related mobility challenges and sharing it with the appropriate academic institutions may be useful to start the discussion of where and how partnerships can be created.

Increase the Innovation Activities, Like Hackathons, That Produce Tangible Outputs and Bridge Commercial and Government Together

Federal Summits and specialized working groups that help broker the conversation within government and between government, academia, and industry will continue to provide high value impacts for government mobility efforts. Furthermore, increasing the frequency of collaborative events that produce tangible artifacts (e.g., hackathons) are highly recommended. These events can lower risk in key technology areas, and help government and industry develop a common understanding of government's mobility requirements.

Targeting some collaborative events around NSA's Commercial Solution for Classified (CSfC) program will help industry gain a better understanding of the government's requirements for use cases like tactical mobility, as well as give the government a better understanding for how commercial products work in an integrated environment with multiple vendor products.

2 Introduction

During the most recent Federal Mobile Computing Summit, seven 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)[2]. ATARC is a non-profit organization that leverages academia to bridge between government and corporate participation in technology[3]. 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:

- Mobile DevOps
- Continuous Mobile Integration
- Mobile App Vetting Strategy
- Secure Components of Mobility
- Mobilizing Legacy Government Applications
- Mobility Solutions to Enhance Citizen Engagement
- How Mobile Technology is Transforming Healthcare

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

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

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

3.1 Mobile DevOps

The *Mobile DevOps* session focused on policy and technology challenges; and solutions for rapid mobile development and a striving for continuous delivery[4] of application code.

3.1.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Identify the challenges of an organization to implement a rapid mobile development environment that consistently delivers quality Apps
- Identify, for a Federal government agency, the planning, development, testing, and IT operation – DevOps mechanisms that will have the most impact on improving agility and quality of a mobile application project and its deliverables

3.1.2 Session Summary

The *Mobile DevOps* session focused on discussing challenges and potential solutions of making rapid mobile development and deployment a reality at the respective federal agencies of the professionals sitting in on the session. There were eleven Federal government agencies agencies represented at this session.

The session discussion was dominated by organizational, agile project management, quality assurance, and production based feedback loop challenges. Some challenges were common to all development and some were distinctive and unique to mobile application development.

Organizational discussion indicated that some agencies were far from ready for an effective DevOps approach. Cultural changes from leadership on down would have to be made for development to work seamlessly with operations and maintenance (O&M) teams. There were experiences of development teams that delivered a tested application to O&M and O&M turnaround time could be as long as two months before infrastructure was in place for deployment to a production environment.

Agile discussions included testimony from some agencies still attempting to climb to an Agile competency level. Many agencies are still stuck in between gears using Waterfall project management (PM) Methodologies. There are projects claiming Agile, but are just giving it “lip service”. Leadership and staff have to be trained in Agile. There are a number of agencies that possess very little development staff and outsource most of their development work to contractors. Contractors need to be verified, in order to ensure they operate with good Agile and DevOps practices. A significant cultural change is needed

[4] http://martinfowler.com/bliki/ContinuousDelivery.html

and this can only be influenced by leadership; standardizing Agile PM as the designated approach of the agency.

Quality Assurance discussion included the daunting task of testing a mobile app that is targeted for bring your own device (BYOD) end-users or the public. There over 19,000 unique Android devices and dozens of iOS device and operating system permutations. There are also Windows devices to think about especially for agencies that are Windows shops. A session member mentioned that a newly developed app may need to be tested on up to 32 devices for providing the necessary coverage of a BYOD or public end-user use case. There is also the necessary layered testing; unit, integration, system, Ux, security, and performance. Device emulators are used to help with testing at some agencies, but this cannot completely replace testing on real devices. Especially for Hybrid and HTML5 apps that are built on cross platform development tools. These apps rely on a level of support for HTML5 functionality from platform to platform.

Users in the Wild discussion included end-users that a project team may not know and understand, because the app is targeted for BYOD users or the public. A session member mentioned his agency developed a public app that is distributed from the Public App Store; their only user feedback comes through the public store reviews. The frequency and timeliness of this feedback is too slow to be effective.

508 Compliance discussion included questions on how apps are developed to be 508 compliant. Most development tools claim that their platform allows you to build 508 compliant UIs. Unfortunately, developers can also build non 508 compliant UI's with the same tools. One agency has employed certified 508 compliance testers from a contractor for their projects.

3.1.3 Recommendations

The Mobile DevOps collaboration session participants identified the following recommendations:

- A Mobility Governance Board that owns the agency-wide mobility initiative and a Mobility Center of Excellence that evangelizes, consults, and provides oversight to all mobility activities can help drive home Agile and DevOps culture change. Also, advertising Agile and DevOps success stories, certifying staff, and recognizing good Agile and DevOps practices will go a long way to that paradigm change

- Testing mobile apps is one of the biggest challenges to DevOps and continuous delivery development. Much of the testing can be automated with scripting and test recording tools. Mobile device test clouds exist for an agency to access the mobile devices that a project requires for their specific QA effort

- The employment of user engagement functionality and app monitoring can provide good feedback loops for improving future versions of an app. App monitoring can include recording app activity, performance, and auditing for both the mobile app client and backend

- Employing certified 508 compliance testers during the development phase of a mobile development project can ensure the UI is designed for 508 compliance from the app planning stages

3.2 Continuous Mobile Integration

Commercial mobile technology evolves at a very rapid pace, often faster than government acquisition cycles. This leads to organizations sustaining obsolete mobile technology. Government mobility programs need to be able to evolve with the commercial sectors to ensure the best technology is provided to employees to improve their productivity, happiness, and security against emerging cyber threats. Continuous integration is a software practice through which each incremental change to an asset is automatically tested, providing feedback about any issues that result. This session's goal was to identify programmatic and technical approaches to continuously integrate **and deploy** new mobile technology, **including hardware and software**, into the enterprise, and capture best practices and lessons learned on continuous mobile integration.

3.2.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Develop an understanding of the infrastructural components and their interactions of a prototypical continuous integration pipeline for software development, as well as understand the concepts of continuous delivery and deployment

- Investigate if and how continuous integration principals can be applied to mobile hardware assets

- Discuss cultural and organizational issues that may arise in the adoption of a continuous integration strategy

- Identify, at a high level, the testing requirements for mobile technologies, both hardware and software

3.2.2 Session Summary

This session opened with a definition of what continuous integration is and how it is used in software design. Continuous integration was defined as a software design practice in which every incremental change is tested to determine whether it can be integrated with the existing software code base. Starting from this point the definition was expanded to a practice in which continually changing inputs are continually tested in order to identify issues as soon as they arise.

Next, the group decided to focus on what was termed *the mobile ecosystem* in which mobility solutions exist. This ecosystem consists of a variety of components both under and outside the control of the federal government such as the operating system of a mobile device, the physical device hardware, the networking environment, and mobile device management (MDM) profiles loaded on a mobile device, specific versions of apps and software running on the device as well as other factors. In evaluating this problem space the group agreed that mobile solutions cause unique issues for the federal government. In the past, for example, the federal government was able to affect and plan for change. In this new ecosystem model, however, the government is often forced to react to change.

The discussion next shifted to an exploration of some of the main problems federal agencies face when a change in the mobile ecosystem does not integrate correctly. The first issue identified was business continuity; simply put, whatever features existed and worked before an update need to continue functioning after that update. A secondary issue was potential security flaws or fixes that could be introduced by an app update. Both of these issues are confounded by a third problem which is version control of mobile assets. Mobility solutions do not make it very easy to downgrade to previous versions of software. Although you can often delay an upgrade, it is difficult if not impossible to downgrade in many case. This, in turn, leads into a discussion of when and how to apply updates. On one hand, one could wait until a new update was tested before applying it. However, in some cases updates are security related and there is a level of risk in waiting until the update has been fully tested. The group did not come to a decision on this specific thread of discussion.

The group identified two additional areas to discuss which are training and triage techniques. In the current mobile ecosystem when a breaking change happens and it is not picked up during testing, the support desk will often be the first group to detect an issue. A potential problem for helpdesk staff occurs when they do not have the same capabilities as a user. For example, if the helpdesk staff does not have access to Wi-Fi they will be unable to assist in diagnosing a new issue that arose with Wi-Fi connectivity after a recent update. Additionally, when an issue arises it needs to go through an entire triage process before it can be addressed and/or fixed. The flow of information could go from service desk to service desk manager to engineering back to service desk as well as to the app vendor who will eventually fix the bug. This information flow needs to be well documented and communicated so that new issues can be easily triaged in the future.

Finally, as the discussion wrapped up the group came to the consensus that there is much more to explore in this discussion area. The group identified the key areas in which further research is warranted including suggestions to investigate some of these areas with pilot programs.

3.2.3 Recommendations

The Continuous Mobile Integration collaboration session participants identified the following recommendations:

- Recognize that mobility solutions exist as a small part of an entire mobile ecosystem of which many parts are out the federal government's control

- Consider creating pilot programs to apply continuous integration principles of to the following areas:
  - Business Continuity
  - Security
  - Version Control
  - Training
  - Triage Techniques

- Provide helpdesk staff with the equipment and capabilities they need in order to correctly diagnose user problems, as well as appropriate techniques and procedures to triage problems that arise

- Identify an organization or group within an agency to own and lead continuous integration efforts

3.3 Mobile App Vetting Strategy

Creating and sustaining a mobile application vetting capability within an organization can be an expensive and time consuming prospect. This session focused on identifying existing strategies and best practices within the government and private sector to be documented and shared. This session also discussed current government mobile application vetting standards and criteria and potential areas of improvement. Finally, this session discussed current capabilities of application vetting tools and their abilities to enable implementation of application vetting standards.

3.3.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Identify strategies and best practices in use within the government and private sector that could be documented and shared with others

- Discuss the current government mobile app vetting standards and criteria (such as NIST's Special Publication 800-163 and NIAP's Protection Profile for Application Software) as well as any applicable private sector standards to identify pain-points, gaps, and potential improvements

- Discuss current capabilities of app vetting tools, their abilities to enable implementation of application vetting standards, and potential areas of improvement

3.3.2 Session Summary

The session was well attended with participants from a variety of government agencies as well as commercial industry. Discussion began on the issue of how to handle vetting of app updates, as many mobile apps are updated on deployment cycles of days or weeks as opposed to the traditional cycles of months or years seen in desktop apps. This rapid pace of updates makes any manual evaluation of apps infeasible as the workload required to vet and re-vet updates on a weekly basis would be unwieldy. The group discussed several potential solutions to this issue, including:

- For the initial scan of an application, use an automated vetting tool combined with manual analysis. For updates, rely solely on automation, only bringing in manual analysis if a specific area of concern is identified by the automated tool

- Explore the use of tools that can identify only the changed portion of the app, and then analyze just that portion

- Explore the use of solutions that divide the mobile device into unmanaged and enterprise managed areas, where only the managed area can access enterprise resources. Provide users the flexibility to run apps in the unmanaged area without enterprise vetting, while enforcing whitelisting on the enterprise managed area and focusing vetting efforts on those apps

Next, the group discussed the current state of app vetting tools. The group discussed the need to engage with vendors to encourage adoption of the security requirements in NIAP's Protection Profile for Application Software as app vetting criteria, as well as the need for tools to provide evidence that can be used by security analysts to clarify or confirm the reported results in order to make an appropriate risk decision. The group noted that there is currently a wide variation in types of analysis performed by app vetting tools, and also noted that automating the NIAP requirements is likely not a trivial undertaking. The group also noted that Apple and Google perform app vetting themselves as part of the Apple App Store and Google Play Store, and it could be worth exploring whether it is possible to leverage their efforts.

The group discussed the potential for a US Government wide repository of app vetting results that could be used for reciprocity purposes. When one organization evaluates a specific version of an app, they post their results including underlying evidence data to the repository. Other organizations could then use those results, applying their own risk algorithms to determine whether or not the risk level is acceptable or if further evaluation needs to be performed. The group noted that there are many small government agencies that may not be able to individually afford app vetting tools and may only have a small number of apps that require vetting.

Conversation then shifted towards gaps with current policies. The group noted that the definition of mobile device in NIST Special Publication 800-163 is out-of-date given the advanced capabilities of today's smartphones and tablets. The Risk Management Framework was noted as not being clear. The NIAP Protection Profile for Application Software was discussed as providing clear criteria for evaluators of apps, but not for app developers. A companion document that helps developers appropriately implement security into their applications would be valuable. Both Google and Apple provide useful guidance to developers, but this guidance could be complemented by something that specifically addresses the Protection Profile requirements.

3.3.3 Recommendations

The Mobile App Vetting Strategy collaboration session participants identified the following recommendations:

- Handling app updates is an unsolved problem. A complete evaluation involving both automated tools and manual analysis is infeasible when 3rd party apps are regularly updated on daily/weekly frequencies. However, security-critical changes to these apps could have occurred. Vetting of these apps needs to continue, but automation is key.

- Need guidance for app developers for how to securely develop apps. The NIAP Protection Profile for Application Software provides useful guidance to security analysts performing app vetting, but it can be difficult to understand by app developers without security expertise. What guidance can be provided specifically oriented to app developers?

- Each organization has its own acceptable level of risk, driven by its own unique environment and use cases. In order to enable organizations to make their own risk determinations, app vetting tools must provide detailed results with evidence, not just simple yes or no results. Additionally, any centralized repository of app vetting results must provide this evidence information as well.

- The group did not reach clear consensus on whether all apps on a device need the same degree of enterprise vetting, or whether it is possible to just analyze enterprise apps and not personal apps. Personal apps certainly have risk concerns as well, but most mobile devices provide capabilities to separate the two types of apps from each other to limit the impact of vulnerabilities or harmful behavior.

- One benefit provided by the mobile environment (and traditionally not seen in desktops) is that apps are generally installed from commercial app stores. This property makes it feasible to analyze the commercial app stores to obtain information such as a count of the number of all applications, hashes of all applications, and the application binaries themselves.

- The continued need exists to engage with app vetting vendors to encourage their adoption of government standards to drive availability of automated vetting solutions that will meet government needs.

3.4 Secure Components of Mobility

This session focused on what is necessary to build a partnership between commercial mobile vendors and the government to assist with adoption of government driven mobile security requirements in commercial products. The ultimate goal is to create a new market that is lucrative for commercial vendors to participate in while making government and critical private sectors more secure.

3.4.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Review the existing processes that drive requirements for secure mobile solutions
- Identify the gaps in requirements and components
- Educate commercial sector to provide an even playing ground

3.4.2 Session Summary

The session began with an overview of the challenges faced by government agencies that want to use commercially available products to field classified mobile solutions. It is challenging to attract commercial vendors to build to government requirements since the classified space represents a significantly smaller sales volume than Department of Defense (DoD) unclassified space. There is a high cost of entry for vendors to meet DoD security requirements and the profit margins are greater in private sectors. The security requirements are driven by the Commercial Solutions for Classified (CSfC) program, as well as other standards and policies such as National Information Assurance Partnership (NIAP) Protection Profiles (PP), National Institute of Standards and Technology (NIST), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Risk Management Framework (RMF), and the Federal Information Security Management Act (FISMA). Added to these are internal security processes from procurement to distribution which often differ across government organizations, services, and agencies; differ based on operational needs and missions; and differ at enterprise, theatre, and tactical levels.

A table listing security requirement categories, guiding processes and relevant documents was presented to the group to drive discussion around trying to identify the gaps. Windows 10 requirements and Committee on National Security Systems Policies

(CNSSP) were mentioned before the discussion moved towards the need for reciprocity, convergence and transparency. Currently, when a product or solution is approved to operate on a classified network, that approval is not valid across all government installations. Each organization, service or agency will run their own security processes against the product or solution prior to allowing it to operate on their networks. This is mostly due to ownership of who assumes the risk for contamination or breach of security. It was mentioned that there is a need for reciprocity across government organizations.

The discussion moved into how there are several lists of government approved products and that these lists differ. A product may be on one list, but not the other. These lists also have separate validation strategies for a vendor to get their product on the list. Product and application validation processes are expensive and often times a vendor will only go after one certification. It was agreed by the session attendees that there is a need for convergence on validated/approved product lists and how to achieve those validations.

Part of the challenges for commercial vendors is there is not enough transparency into the government mobility requirements and security policies. Often times the government requirements are released after a capability comes out and it is much harder to build into a product afterwards. It was suggested that the government monitor maturity trends and provide requirements to commercial vendors early. It is also recommended that government policy makers keep industry informed of policy changes and provide insight into what is on the horizon.

Other points made during the discussion included the need for better guidance and policy engineering to address tactical use cases, factoring in more about the environment, external factors and intelligence life. The need for guidance on use of secure mobile devices inside and outside of secure spaces and ways to remove the security decisions (e.g., automation) away from the user. Guidance on how to handle mixed solutions such as Type 1 plus CSfC and military radio plus Bluetooth for peripheral devices. It was also expressed that there is a need for architecture as mobile solutions break down at integration points. An understanding of what’s trending will facilitate integration, which also goes back to transparency.

3.4.3 Recommendations

The Secure Components of Mobility collaboration session participants identified the following recommendations:

- The government and industry should collaborate more often to provide transparency into capabilities, maturity trends, requirements and security policies
- The government should work towards converging the approve product lists including the validation strategy for getting products certified
- Generate tactical use cases for both government and industry to guide policies and capability requirements

3.5 Mobilizing Legacy Government Applications

The Mobilizing Legacy Government Applications session discussed the challenges and constraints that the government faces when attempting to migrate to a mobile ecosystem.

3.5.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Determine differences between legacy application and mobile application development, where processes can be adapted and where they are fundamentally incompatible

- Identification of the biggest challenges encountered in mobilizing legacy applications, and identify possible solutions to these challenges

3.5.2 Discussion Summary

The discussion started by identifying numerous challenges being faced today, which can be categorized into three main groups.

Technology Challenges

- **Infrastructure pre-requisites:** If an organization does not already have a mobile infrastructure in place, there are often many pre-requisites that must be accounted for: mobile device management (MDM) and/or enterprise mobility management (EMM) solutions, app distribution technology, and much more. Creating a secure mobile access solution is a non-trivial and costly task.
- **Data access:** Legacy enterprise data sources can be incompatible with mobile applications. Additionally, services which could once be secured by the network perimeter must be somehow opened up to the Internet so mobile devices can access them. Database abstraction layers must be created/obtained, network architecture must be modified, and security mechanisms applied to ensure that data can be safely accessed by mobile devices.
- **User interface:** Mobile devices are vastly different from legacy computers. With smaller screens, touch interfaces, and a bevy of sensors, mobile apps must leverage newer interface components to provide a user-friendly experience. Translating a legacy interface to a mobile-friendly interface, while providing the same functionality and data, is no easy task.
- **Connectivity:** Some organizations, especially those in the DoD, must also be concerned with supporting use cases in disconnected, intermittent, and limited (DIL) connectivity environments. Many mobile development paradigms are

explicitly designed with the assumption that devices will be network-connected. Changes to development may be necessary to support DIL environments.

Process and Policy Challenges

- **Overall strategy:** Especially for larger organizations, it is imperative that mobile application development is approached in a consistent way across the organization. Like infrastructure pre-requisites for technology, an overall strategy should be crafted firsthand so policies will be in place to support and guide development efforts—this should cover scope, principles, goals/objectives, and a phased roadmap. It can be difficult to make sure the overall strategy is crafted to take the needs of all stakeholders into account.
- **Platform selection**: A variety of mobile devices are commercially available, but because of the rapid pace of mobile evolution, it can be very costly and difficult to support multiple platforms. A single platform (whether that be native, or a cross-platform solution) should be carefully chosen to provide consistency across the organization and ensure that all apps can be supported long-term.
- **Data ownership:** Some legacy applications that are developed and supported by contractors may pose problems in the mobile migration process. If the contractor retains ownership of the data, transfer of that ownership to the government organization may be needed to support development and fielding of the mobile app.
- **Procurement lifecycle:** Government procurement lifecycles are measured in years, but mobile device evolution is still moving at a rapid pace. Changes must be made to these procurement lifecycles to support mobile technology and ensure that mobilized apps don't become obsolete before they are even released.
- **Realistic cost:** Oftentimes, because of the various supporting pieces required and the learning curve compared to legacy application development, developing a mobile app can balloon in cost and scope. Organization leadership needs to ask themselves "What can we afford?", justify the return-on-investment (ROI), and determine how to measure that ROI before deciding what they should be developing.

People Challenges

- **Resistance to change:** Users are often resistant to change, and frequently want mobile apps to provide an identical interface to its legacy counterpart. However, making a user-friendly interface for mobile apps will simply necessitate some changes.
- **Learning curve:** Especially when presented with new devices, users will face a learning curve to interacting with mobile applications. Help and support must be readily available to ensure that users have a smooth transition, stay happy, and stay productive.
- **Fear of failure:** Government organizations often have a culture that fosters a fear of failure. Mobile app development is an iterative and rapid process, and not every idea works well when created as a mobile app. Fear of failure causes

stagnation, whereas taking reasonable risks has the potential to result in great impact. Organizations must start embracing failure as a realistic outcome, and something to be learned from, if they are to be successful in new development paradigms.

- **Pilot to production:** Organizations sometimes develop apps as a pilot, and wind up moving those pilots to production without assessing them with proper rigor. The pilot-to-production process should be well thought out, and steps should be taken to ensure that apps are robust and secure.
- **Access to real users:** Mobile app development is highly iterative, and without access to real users, may result in a poorly-designed and under-utilized app.

Participants started by discussing the main challenges and barriers to entry concerning mobilizing legacy government applications. Much of these challenges stem from mobile application development itself, and are not unique to the legacy-to-mobile problem. It was proposed that these challenges are grouped into three categories: technology, process/policy, and people. Some of these challenges may be lessened (or may not apply at all) for organizations depending on their size, demographics, and prior development experience. Generally speaking, many of these challenges are foundational; if they are addressed properly up front, it will make future mobile app development in the organization much quicker, smoother, and more cost-effective.

Afterwards, discussion shifted towards how to help organizations navigate through the aforementioned challenges. A framework or “playbook” to guide migration, with a checklist of activities, would greatly benefit organizations that are new to such a process. This playbook should be based off of existing frameworks and guidance, should help identify if it makes sense to mobilize an application, and should guide the build-or-buy decision. With an emphasis on small and iterative migration, it would help organizations make a roadmap to developing its mobile apps.

Such a playbook should also discuss “app rationalization”, which will help organizations inventory and prioritize existing systems and best practices to guide investments. Finally, the playbook should provide established criteria to help determine expected ROI. Such criteria should measure both quantitative and qualitative aspects (e.g. safety, satisfaction). The criteria should define productivity and how to measure it, and should spell out legal implications that must be considered. Also, the criteria should help manage expectations for mobile app development and deployment.

After discussing the idea of a playbook, conversation shifted towards the groups of people that such guidance would apply to. Participants centered around three groups of people involved in the app development process: leadership, management, and developers. These three groups should communicate about what development should entail and how it should be executed:

1. **Leadership:** determine business needs, what should be mobile-enabled, and manage expectations; determine what the organization can afford; and develop

governance and intra-agency policies through brainstorming, education, and focused discussion.

2. **Managers:** evangelize new technology to the organization, communicate technology needs to leaders, and carefully choose the platforms/technologies that will allow them to solve problems most effectively.

3. **Developers:** conduct DevOps, Continuous Integration (CI) and Continuous Deployment (CD); conduct security assessments and comply with policies; help define standards (languages, etc.) and the "emerging technology bucket" to be used in the development process

3.5.3 Recommendations

The Mobilizing Legacy Government Applications collaboration session participants identified the following recommendations:

- Develop strategies to address top challenges early and effectively
- Consider what is realistic and affordable; it may be necessary to pare down desired features and content to make a successful mobile app
- Ensure that leadership, managers, and developers are aware of the challenges they should address, and are communicating with each other

3.6 Mobility Solutions to Enhance Citizen Engagement

This session focused on policies and strategies that public agencies might use to increase and enhance citizen engagement with government.

3.6.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Identify recommendations on employable methods and technologies that can be leveraged to better enable access to data and services by U.S. citizens.
- Provide recommendations on lowering barriers to access.

3.6.2 Session Summary

This session began with a discussion of APIs that support mobile apps and later focused on the apps themselves. The session initially touched on the ability of government agencies to provide APIs in a consistent manner. The speakers discussed the need for not solely relying on postings through data.gov or agency websites, but instead promoting them through their social media and other marketing channels. The speakers discussed that with APIs that provide data, it is important to provide the raw data to the consumers of the API, and if there is derived data that is presented, it is important to mark it as such.

In most cases, it would be better for an agency to provide both the raw and derived data if it exists.

The session then considered the circumstances for building a responsive website and identified when using a mobile app is appropriate and necessary. There are criteria that can be used to make that decision including functionality, reach, ability to support offline access, and cost, to name a few.

The speakers also addressed the kind of apps being built for citizen engagement at the local or county level and how they differ from the ones being created for the state and federal arena. In addition, they briefly compared mobile apps built by other governments to ones in the U.S. They discussed how some of the international apps issued by governments would not scale in the U.S. due to the larger population size, and how some of the international apps issued by governments would be considered threatening commercial markets in the U.S. and overstepping the bounds of what government should do.

The speakers and participants also discussed the need for simplicity of visual design in an app. Many logo and branding images will confuse the end-user. The end-user wants to use the app to get information or perform a transaction and is not necessarily interested in how an agency is organized. The details of what Federal groups or agencies collaborated to build an app is best left in an "about" section of the app.

The total cost of ownership was also a topic discussed during the session. Everyone agreed that looking at the full cost of owning a mobile app over many years is important, agreeing that an app requires a multi-year commitment from an agency. Reasons for this include planning for maintenance as OS upgrades are published and new features are needed. Simply publishing an app on the app store can be considered the beginning of the process of citizenship engagement.

3.6.3 Recommendations

The Mobility Solutions to Enhance Citizen Engagement collaboration session participants identified the following recommendations:

- Ensure that the design of mobile apps is centered on the user experience
- Critical to increased engagement is a clear understanding of the needs and wants of the targeted user community
- Simply and standardize access to, and understanding of data. This requires the owner of the data to collaborate with those who wish to provide access to the data
- Increase attention to marketing. If the user community is not aware of app availability, they will not use it
- Plan for long term maintenance. Abandoned and poorly operating apps turn off users and reduce engagement
- Embedded branding of apps is unnecessary and may lead to user confusion

3.7 How Mobile Technology is Transforming Healthcare

Many federal agencies are leveraging mobility to improve healthcare delivery. There are many common mobility challenges in healthcare with opportunities to share solutions. There is an ongoing effort by the DoD/VA Interagency Program Office (IPO) to ensure mobile healthcare efforts are synchronized across the two departments. This session examined key mobility use cases common to DoD and VA healthcare, as well as identified new use cases that can improve government healthcare. Also discussed during this session are key efforts across government, industry, and academia that both departments should consider leveraging to mitigate these use cases and solve key challenges.

3.7.1 Session Goals

The goal of the joint session, with participants from the government, industry and academia, was to:

- Develop an understanding of the common mobility challenges in healthcare delivery
- Develop an understanding of the infrastructure components that a mobile medical ecosystem depends on
- Discuss what ongoing activities are addressing these challenges where solutions can be shared across the mobile medical community

3.7.2 Session Summary

The session started with by discussing the VA's Technology Strategies for Enterprise Design Patterns being developed as part of their Enterprise Technical Architecture. This project will support Veterans' expectations for instant access to information and self-service options via the Internet, and increasingly through mobile devices like tablets and smartphones (and the next generation "smart" devices that are yet to be deployed). The design patterns are incorporated into the One VA Enterprise Technical Architecture (ETA)[5]. They provide a standardized framework of capabilities and constraining principles to aid all integrated project teams (IPT) in the development, acquisition, and/or implementation of IT systems and services.

The discussion shifted to a focus on the mobility use cases developed by the DoD VA IPO Joint Exploratory Team (JET). These use cases support their goal to identify common research challenges with needs associated with mobile use in healthcare to identify alignment opportunities and build a shared roadmap. The use cases and

[5] http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp

associated technical views were presented to the group. These views highlight the key challenges related to interoperability with mobile devices and personal/electronic health records. The use cases presented were:

1. Patient management of Personal Health Record (PHR) from a Personally Owned Device
2. Healthcare Provider Management of Electronic Health Record (EHR) from an approved non-GFE device
3. Healthcare Provider Management of EHR from a GFE mobile device
4. Common Risk Assessment approach for Mobile App use in Both DoD and VA IT Environments
5. Interact with Mobile Health Monitoring Sensor from a Mobile Device
6. Administer Medicine via a Wireless Medical Device
7. Common software development kit for Mobile Medical Apps to support use of a mobile device as a medical device
8. Cross agency access to medical systems with approved mobile devices

Some of the key challenges are security-focused, specifically the use of non-managed devices by clinicians (3rd party) and patients which includes securing the data locally stored on the device and during transit, and identity management and methods for strong authentication. Participants also discussed the creation of Interagency App Development Design Team to establish standard application development framework where the security and interoperability are baked in the development cycle. There is also a need to build mobile application reciprocity amongst agencies.

3.7.3 Recommendations

The How Mobile Technology is Transforming Healthcare collaboration session participants identified the following recommendations:

- Conduct a pilot following the Mobile Technology Tiger Team's (MTTT) CONOPS across DoD/VA

- Establish standard application development framework where the security and interoperability is baked in earlier in the development cycle

- Develop a common approach to support identity management to include strong authentication to support 3rd party medical providers using Non-GFE mobile devices/technologies needs to be defined. Identify an organization (DoD, VA) to pilot solutions

- Conduct analysis on how health kit platforms integrate securely into the mobile ecosystem

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.

Several key overarching recommendations emerged as a result of the seven Collaboration Sessions.

Create Government Wide Repository of Success Patterns, and Tools to Help Agencies Operate More Agilely in Mobility

Organizational and technology agility is key to success. More enterprise data needs to be exposed for mobile consumption, and more business processes are involving mobile devices. Rapid development tools and techniques need to be pervasive in the government community, along with associated process and a culture that fosters agile development to respond to changing user needs and technology.

Creating a repository with lessons learned and enterprise licenses for modern continuous integration and DevOps tools can be useful to help entice federal agencies to adopt and maintain modern mobile software development practices.

Create Partnerships with Universities to Identify Novel Approaches to Existing Mobility Problems

Academia can provide strong technical resources and insights into the challenge areas discussed. To alleviate the burden on the government, academics should be included in the mobile research and innovation efforts to provide high quality technical input from a different vantage point. Qualified mobile engineers (software & hardware) are in high-demand, and universities can help provide access to researchers and work with government to identify high value concepts that are beneficial to both parties.

Increasing partnerships with academic institutions that specialize in engineering and healthcare can help to find novel approaches to healthcare related mobility challenges. Creating a federal wide list of key healthcare related mobility challenges and sharing it with the appropriate academic institutions may be useful to start the discussion of where and how partnerships can be created.

Increase the Innovation Activities, Like Hackathons, That Produce Tangible Outputs and Bridge Commercial and Government Together

Federal Summits and specialized working groups that help broker the conversation within government and between government, academia, and industry will continue to provide high value impacts for government mobility efforts. Furthermore, increasing the frequency of collaborative events that produce tangible artifacts (e.g., hackathons[6]) are highly recommended. These events can lower risk in key technology areas, and help government and industry develop a common understanding of government's mobility requirements.

Targeting some collaborative events around CSfC will help industry gain a better understanding of the government's requirements for use cases like tactical mobility, as well as give the government a better understanding for how commercial products work in an integrated environment with multiple vendor products.

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[7].

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

[7] http://fedsummits.com/mobile/