August 2014 Federal Mobile Computing Summit Collaboration Session Summary

Tom Suder
ATARC

Brian Brady, Darshan Kadam, Diane Hanf, Ronnie Daldos, Karen Caraway, Jared Ondricek, Patrick Benito, Marie Collins
The MITRE Corporation

Dr. Walt Scacchi
University of California - Irvine

Approved for Public Release; Distribution Unlimited. 14-1455

Executive Summary

The Federal Mobile Computing Summit took place on August 19th and 20th, 2014. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, discuss the main challenge areas in mobility, and discussed prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks.

The Collaboration Sessions covered four key mobility topics:

- Mobile App Legal & Acquisition Best Practices
- Impacts of the Emerging Internet of Things (IoT) on the Enterprise
- How to Embrace Contextually Aware & Wearable Computing
- Integrating Mobility Into the Enterprise – Moving Beyond Mobile Application Development (MAD)/Mobile Device Management (MDM)

Several key themes emerged as a result of the four Collaboration Sessions:

- A Federal-wide lessons learned and collaboration portal should be developed to share best practices in mobile acquisition.
- The concept of mobility is evolving as wearable computing and IoT becomes more mainstream.
- Reviewing policies and governance at the Federal level and identifying improvements in the policy creation and modification process for key areas like security and acquisition is crucial to the successful implementation and operation of mobility.
- The academic community is a ripe, largely untapped resource to use to help devote research to lower adoption risk by increasing the security and privacy of IoT and wearable computing.

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

Establish Federal Level Legal and License Templates for Mobile Apps

• The Federal CIO Council Information Security and Identity Management Committee's (ISIMC) Mobile Technology Tiger Team should work to create a common, tailorable, legal review process for Federal agencies to use in app acquisition

Develop an Agile, Federal Level Policy Development and Modification Process

• The Federal CIO Council ISIMC Mobile Technology Tiger Team should create a new, agile process for defining and refining Federal mobile policy.

Develop Common APIs and Security Model for Wearables

• Agencies like DISA and GSA should develop a common API and security model and work with commercial vendors to enhance wearable security

Invest in IoT Experimentation to Prepare for Secure Adoption of IoT

• The Federal CIO Council ISIMC Mobile Technology Tiger Team should appoint a single agency at the federal level to investigate and experiment with IoT

Table of Contents

1 Introduction

The Federal Mobile Computing Summit took place on August 19th and 20th, 2014. The Summit included a set of MITRE-Advanced Technology Academic Research Center (ATARC) led Collaboration Sessions that afforded industry, Government, academic, and federally funded research and development center (FFRDC) representatives an opportunity to collaborate, discuss the main challenge areas in mobility, and discussed prominent challenge areas in mobility. In some cases, potential solutions were identified for key challenge areas. The discussions were Government focused with the objective of refining gaps, and identifying features of potential solutions or frameworks. The discussions were Government focused and at a high-level, not addressing any specific solution and only identifying features of potential solutions or frameworks.

As part of the Collaboration Sessions, MITRE and ATARC invited academia to participate in each of the four challenge areas, and asked participating academics to identify courses of action to be taken to enable improved Government and industry collaboration with academic institutions. The academic participants focused on how they could build expertise in these technology areas, as well as address the specific challenge areas by changes in curricula, research, and outreach opportunities related to the challenges.

This white paper summarizes the results of the Collaboration Sessions and identifies suggestions and recommendations for Government and academia while identifying crosscutting issues that tie between the different challenge areas. It also proposes a community built around Government and industry collaboration with academia to leverage potentially previously untapped academic resources. The proposed community will be fostered by MITRE and ATARC to enable communications between the different participating communities. The outcomes of this community include:

- Academia produces higher quality, better-prepared, and "industry-ready" graduates for hire
- Government leverages graduate and undergraduate level research to help solve critical mobility challenges
- Government organizations have an integrated research and advisory capability made up of commercial companies, academic institutions, and federally funded research and development centers (FFRDC)

2 Collaboration Session Overview

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

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

The challenge areas are as follows:

- Mobile App Legal & Acquisition Best Practices
- Impacts of the Emerging Internet of Things on the Government Enterprise
- How to Embrace Contextually Aware & Wearable Computing
- Integrating Mobility Into the Enterprise – Moving Beyond Mobile Application Development (MAD)/Mobile Device Management (MDM)

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

3 March 2014 Federal Mobile Computing Summit Collaboration Sessions

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

3.1 Mobile App Legal & Acquisition Session

This session focused on determining the top priority acquisition and legal implications associated with creating mobile applications and reusing them across Government agencies through app stores. It also developed recommendations on how to address these issues, taking into account viewpoints from Government, commercial, and academia.

3.1.1 Session Goals

- Identify the key legal and acquisition issues associated mobile apps type during a typical lifecycle
- Determine legal and acquisition issues associated with sharing and reusing apps across Government agencies
- Rank identified issues by relative importance
- Identify the natural order in which issues should be addressed along with recommendations on how to address them

3.1.2 Session Summary

The Mobile App Legal & Acquisition Collaboration Session started with the introduction of the audience to the concept of Legal Reciprocity. Equivalent to Cybersecurity Reciprocity, Legal Reciprocity seeks to standardize legal review results performed by any Federal legal team, and making it readily available to other Federal Legal professionals. This is seen as a way to shorten mobile app acquisition timelines so that Federal Enterprise-level App Stores can be more rapidly populated. The group identified one implication of the approach—unique Department/Agency laws and rules may need to be applied. The group recommended that the Federal CIO establish a Federal Legal Reciprocity baseline for Mobile Application Terms and Conditions that is applicable across all agencies. Each agency would then only have to conduct a review for their additional unique legal requirements resulting in acquisition process efficiencies.

The session participants then listened to a short presentation and demonstration on the National Geo-Intelligence Agency's (NGA) App Store and future plans. The App Store contains iOS and Android mobile applications, web applications and other software components that are accessed by the Federal workers in performing intelligence, combat (DoD) and humanitarian (e.g., DHS, FEMA) missions. NGA App Store's future plans include a novel business model in which an Application Operations Service Provider (acquisition broker) published NGA Broad Area Needs and procures candidate mobile applications from academia and large and small commercial providers and then populates the App Store. Providers are reimbursed based on application usage. There are five key best practices that are emerging from this approach:

1. Establish a common end user license to simplify user acceptance and streamline mobile application creation and acquisition
2. Establish a streamlined legal checklist (Legal Shared Agreement) that all providers sign showing that they will produce components that adhere to Enterprise legal requirements
3. Ensure brokers used in this type business model are Organizational Conflict of Interest cleared
4. Use a clearly stated Governance process that identifies up front the criteria against which applications are vetted (NGA uses 7 criteria)

The NGA App Store discussion led to the group identifying the need for a Lessons Learned document for use by Federal agencies that captures mobile application acquisition and sustainment issues when deployed in a market-based environment. Having viewed the scope of establishing an Enterprise-level App Store such as the NGA's, the group determined that a Federal Enterprise App Store that is shared among smaller agencies would be a Best Practice that could lead to cost savings.

Finally, the group listened to an eye-opening presentation from Drs. Walt Scacchi and Thomas Alspaugh of the University of California at Irvine in which they identified the complexity associated with licensing mobile applications. The key issue is: quickly understanding the Government's rights and obligations when a mobile application is initially purchased and then updated. As narrow in scope as a mobile app is, it can be composed of many licenses, which should be analyzed to ensure that they meet organizational legal requirements. The complexity of the Intellectual Property licensing structure, as demonstrated by Drs. Scacchi and Alspaugh's review of one popular mobile device management application (it had 12 subsuming licenses) will dramatically increase the legal team workload. The cost of legal analysis can far exceed the cost of the component, suggesting that a more cost effective best practice would be to provide the acquisition force an automated license management tool to realize process efficiencies.

3.2 Impacts of the Emerging Internet of Things on the Government Enterprise Session

This session focused on identifying aspects an organization should consider when implementing technologies and concepts that are encompassed by the IoT. The session went beyond the hype of IoT and identified the practical implications associated with adopting this emerging concept.

3.2.1 Session Goals

- Define a practical working definition of Internet of Things as it pertains to the Government
- Identify impacts the IoT will have on mission and data centers
- Determine security shortfalls and provide recommendations on what needs to be done to secure IoT
- Define challenges and recommendations to current technology on-boarding processes

3.2.2 Session Summary

The Collaboration Session discussion initially focused on the Government's definition of IoT. However, the definition resulted more in an itemized list of characteristics or components rather than a definition. As a result of the discussion, a participant created a definition based upon the identified characteristics: "A set of physical, interconnected endpoints that interact with each other and with the internet to enable the environment-aware, real time data, related applications and processes in a Government ecosystem." The discussion shifted towards potential use cases, which are identified in Table 1:

Narcotics Information Reporting	Traffic flow control
Human rights reporting to Congress	Agriculture use of sensors to analysis growing conditions with ability to send UAV to fertilize, water, etc.
Autonomous Vehicles and Trucking Data to improve roads and efficiencies based on activity	Industrial control and environmental concerns using microcontrollers
Weather data for assist in disaster recovery such as evacuation of people	Legislatively driven reporting such as pollution indices
Disaster recovery logistics	Public safety alerts and reporting
Smart Cities	Social Services to consumers via digital licenses
Smart Parking (e.g. availability of parking)	

Table 1: IoT Use Cases

The discussion transitioned to IoT impacts on information security and privacy & data protection. The Government needs to rethink how they conduct business in order to minimize the impact to IoT systems for potential attacks. Tampering of data can potentially occur by the injection of fake data that could be used to mask physical attacks, modify the results of the aggregated data or disrupt service to the control processes; or by

compromising the control processing by sending incorrect commands that could be used to trigger events causing damage.

The group identified that the Government needs to put in place additional safeguards to identify anomalies based upon mission to determine when systems or aggregated data has been comprised. IoT requires security and awareness at all layers, not only at the network layer.

Subsequently, the group identified a five-step process for the Federal Government on securing IoT, shown in Figure 1.

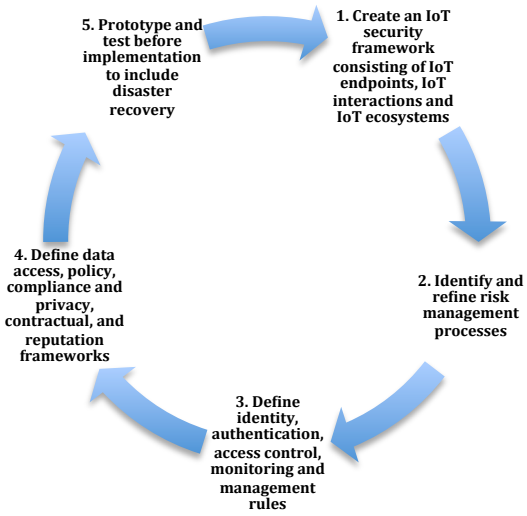

Figure 1: Process for Securing IoT

3.3 How to Embrace Contextually Aware & Wearable Computing Session

This session focused on looking at the new world of contextually aware applications and wearable computing. While business applications of the past have largely delivered static content, mobile computing has rapidly enhanced user experience such that users are coming to expect personalized interactions with their data. This can have an impact to organization's security and legal matters. It also has direct impact on in house development and testing procedures. Finally, it forces us to view how this computing model impacts us as individual organizations and as a whole.

3.3.1 Session Goals

- Explore security impact of wearable computing, both from employees and outsiders perspectives
- Explore legal impact of wearable computing devices both inside and outside of controlled spaces
- Discover where contextually aware computing has already impacted the federal Government and capture pros/cons

- Discuss development and testing environments and how they differ from other environments
- Discuss internal training and awareness impact
- Discuss available tool sets that exist in this arena

3.3.2 Session Summary

The Collaboration Session began by discussing the definition of what was meant by wearable computing. While many wearable devices that are produced today are Internet connected, connectivity is not a hard prerequisite to being considered wearable computing technology. Examples include a soldier's helmet that includes a heads-up display of information about his surroundings and uses accelerometers to monitor for impact. Additionally, there are devices such as pinhole cameras or police officer cameras that could be considered wearable technology but do not do a lot of computing. In addition, we discussed the topic of active vs. passive technologies with radio frequency identification (RFID) being the passive technology example. It was undecided whether passive tech like an RFID chip would fall in the same category as other wearable devices if only identification and not computing or data transmission occurs. Ultimately, the session participants did not come to a definitive answer to what constitutes wearable computing in the Government space. This is a reasonable outcome since the commercial wearable field is rapidly changing.

The next topic discussed was use cases for wearable tech in the Government. As previously mentioned, the soldier's helmet with real time information displayed as needed was a prime example of a useful wearable device. Another example is the emergency first responder who could have a Google Glass-like device with specialized applications to assist them in identifying or responding to areas with the greatest needs. These examples serve to illustrate the fact that there are multiple factors that influence use cases of wearables' implementation and need.

This leads to interesting questions, such as who owns the data that is generated by the wearable devices? If personally identifiable information (PII) data is collected during the normal usage of the wearable device, does the owner or the wearer of the device own the data? One solution posed was to have policy that states what data is collected and what parts of the data are used and what parts are discarded in the event that it is not possible to avoid data collection.

One theme that was present during the session was that the Federal Government does not want to perpetually play catch-up when it comes to technology. While it is understood that proper vetting and security testing needs to precede the adoption of technology, Government employees want to be able to do their jobs in the most efficient manner. Younger employees that are entering the field have a preconceived expectation of being able to utilize wearable technology such as smart watches, smart glasses, etc. If these technologies are barred from the workplace, many potential employees may opt to enter a different working environment.

MDM software was the next topic discussed in the session. Since MDMs already have a presence in many Government and commercial mobile deployments it makes the most sense to use that existing infrastructure to manage wearable computing devices. It does not matter as much if they are represented as being individual units or sub-units of existing devices (for example, wearable sub-units tethered to a smartphone). However, certain capabilities such as remote wipe should be available through the MDM administrator interface.

Of course, security is a huge concern when discussing any mobile technology and wearable computing is no exception. Due to the nature of the limited computing power, battery life, etc. on smaller devices combined with the need to have data encryption at rest as well as data in transit, this led to a discussion of what data should even be allowed to be stored on wearable devices. No one wants to wear something that will only last a short period of time before it needs to be recharged in order to be useful. In an operational environment it warrants a survey of what data will actually be used on the device to see what security measures are required to certify that a device can be on the network, if at all. Along these lines, it could be warranted that either a security technical implementation guide (STIG) or security requirements guide (SRG) should be created for wearables separate from other mobile devices.

Authentication was another topic that was discussed in this session. The question that generated the most conversation was whether a mobile device warranted the same level of scrutiny in the authentication process as other mobile devices such as phones and tablets. In conjunction with the prior discussion on determining what data exactly is stored on the device, it makes sense that if nothing or hardly anything is stored locally then a lower level of authentication might be fine in the context of getting access to the notifications that the wearable device might convey.

On a final note, legal concerns were discussed for these devices both in the case that they are worn inside and outside of controlled Government spaces. There are the obvious privacy concerns, both of the wearer and potentially those nearby (for example, if the wearable has a camera attached to it, the device may raise a privacy concern). Yet there was also discussion of what certifications and accreditations would be required in order for a device to be able to connect to Government owned networks. Internal training would have to be considered to fully incorporate wearable devices into any work environment, as well.

In the end there was more to discuss than there was time to discuss it. Since this field is still changing at a rapid pace, it is difficult to see where it will end up in the future but the participants feel that there is a place for it in the federal workforce, even if it is used in a controlled manner.

3.4 Integrating Mobility Into the Enterprise – Moving Beyond MAD/MDM Session

This session focused on the impacts mobile technologies have on the Enterprise. It went beyond the technical aspects, and looked at how the Government must re-think the Enterprise, and how people work in a mobility enabled organization. This session documented the considerations organizations should address after basic mobility technologies and processes are established, in order to realize the efficiencies mobility offers.

3.4.1 Session Goals

- Define the scope of mobile technology on the Enterprise: SmartPhone, Tablets, Internet of Things
- Compare the Enterprise's mobility enabled operational model vs. the traditional operational model
- Detail how people work and collaborate in a mobile enabled Enterprise
- Describe the ideal Enterprise required to support this new mobile paradigm (Includes people, processes, and technology)

3.4.2 Session Summary

Knowing in advance that the Collaboration Session was going to be well attended, the session moderators sent a survey to the registered attendees to help share the session and focus on key challenges. As shown in the Figure 2, there was no clear "priority", but rather numerous mobility challenges across the Enterprise.

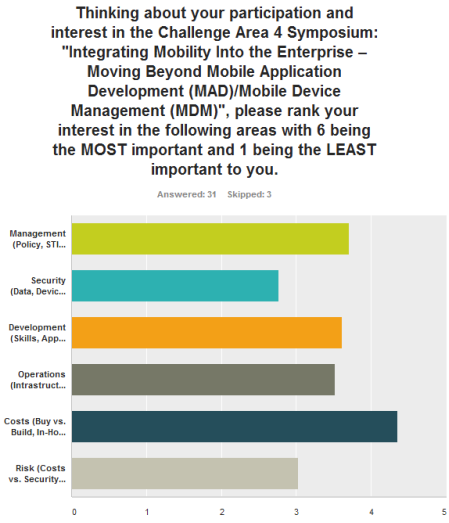

Figure 2: Survey Results

Based on survey inputs, the moderators focused on three key areas for the session, breaking out into the following Enterprise challenge areas:

- Technology

- People and Organization
- Policy and Governance

The Technology working group focused on the integration of technology into the Enterprise and the challenges that result. The discussions initially focused on how Government agencies must embrace innovative mobile technologies to support, retain, and attach staff. Some agencies cited examples where they have been unable to recruit good talent because of policies (e.g., security) and slow acquisition timeframes preventing employees from working one modern technology. Most agencies taking part of the discussion indicated they are looking at mobility as one of the areas to attract new recruits into Government service.

The general feeling among the participants is that implementing policy is one of the toughest challenges within agencies. Examples of existing policies (such as security) are causing delays in technology adoption, in certain instances technology is replaced by the time policy is updated. Also, the way "data" that is accessed via mobile devices is perceived has become a generational issue – the younger and more mobile savvy audience looks at data that needs to be shared and opened for public access whereas the older and experienced audience looks at securing and restricting access to the data that has historically never been available over mobile. The group recommends that Government agencies make user demands and data access the two cornerstones of any mobility strategy. The group also recommended that Government agencies do not cite all policy as inhibitors. The Government should identify the key policies that are hindering adoption, and work at the Federal CIO level, through the Mobile Technology Tiger Team, to reform Security and Acquisition policies.

The group shifted discussion towards the impact of Enterprise mobility upon people and organization. Since mobile IT is different from traditional IT, the group discussed how Enterprises must establish an adoption strategy for the adoption of mobile technology in the Enterprise. The key elements of an adoption strategy the group recommends agencies include are:

- Define business problem
- Identify business champion
- Develop strategy within PMO
- Streamline procurement, standards on technology, devices across agencies
- Sounds engineering processes
- Training users on mobile technology; policy compliance and usage risks

There is no "one size fits all" mobility adoption strategy, but the group recommended that there be a repository at the Federal level to share lessons learned and best practices for all Federal agencies to access and use. OMB MAX was cited as a potential repository.

The same "one size fits all" limitation applies to mobility policy. The group discussed how Enterprise (Government and agency levels) policies are not keeping pace with the evolution of mobile technology. The group recommended that the Mobile Technology Tiger team focus on refining the policy process so it is more proactive rather than

reactive, and refreshed continually with set timeframes. Furthermore, the group recommended that tiers of policy get developed, that are tailorable at the Federal, Agency, and Local levels. In addition, mobility SMEs should be included in all aspects of the policy development process to help educate and inform policy authors.

4 Summary

Several key themes emerged as a result of the four Collaboration Sessions. Firstly, the Government mobile space is still fragmented. There are a wide variety of independent efforts scattered across the Government that are trying to solve similar problems independently. There are some examples of cross agency sharing (e.g., MTTT App Vetting), but these engagements are still largely ad hoc without a central knowledge repository at the Federal level.

Secondly, the concept of mobility is evolving as wearable computing and IoT becomes more mainstream. These concepts and technologies are going to introduce even more disruption in the commercial and sectors. It is highly recommended that the Federal Government begin to understand how these concepts can be adopted, and prepare early for adoption to help ensure a smooth integration of emerging mobility into existing traditional and mobile IT.

Thirdly, policy and Governance continue to be seen as roadblocks to successful adoption of mobility. While some policy and governance are indeed impediments to adopting mobility, not all policy and governance is a hindrance. Reviewing policies and governance at the Federal level, and identifying improvements in the policy creation and modification process for key areas like security and acquisition is crucial to the successful implementation and operation of mobility.

Fourthly and lastly, the academic community is a ripe, largely untapped resource to use to help devote research into some key challenges, and Government and industry can work with academia to not only shape research, but to help shape curricula to produce engineers prepared to work in the mobile application security space.

5 Recommendations

Establish Federal Level Legal and License Templates for Mobile Apps

The Mobile Technology Tiger team should work to create a common, tailorable, legal review process for Federal agencies to use in app acquisition. This will provide a common process across each agency, and agency would then only have to tailor the process for any unique legal requirements. Part of this effort should include a standard, tailorable, mobile app terms and conditions template for all agencies to use during app acquisition efforts. The NGA Application Operations Service Provider is a good baseline for this effort, and should be used as the basis for any work in this area.

Develop an Agile, Federal Level Policy Development and Modification Process

While policy was cited as being a barrier to agile delivery of mobility, all policy should not be treated as inhibitors. The Mobile Technology Tiger Team should create a new, agile, process for developing and refining mobile policy. This process, and resulting policies, should be tailored and used by Federal agencies. This will allow the Federal CIO to keep good policies in tact, identify policies that need updating, and reform the policies that inhibit innovation and progress.

Develop Common APIs and Security Model for Wearables

Wearables introduce new capabilities, as well as security risks to the Government. Since a large amount of data will be collected by wearables, the Mobile Technology Tiger Team should define policy surrounding data ownership and protection. Furthermore, agencies like DISA and GSA should conduct experiments and pilots that result in the development of a common API and security model and work with commercial vendors to enhance wearable security. These issues exist, and have not been addressed, in the commercial world, and the Government is in a good position to help shape future commercial efforts. This experimentation should use academic research to the fullest extent possible to help accelerate the effort.

Invest in IoT Experimentation to Prepare for Secure Adoption of IoT

The Mobile Technology Tiger Team should appoint a single agency at the federal level to investigate and experiment with IoT, to help mature commercial security models in this space. The experimentation should produce a security model, risks, mitigations, and development frameworks for IoT adoption in the Federal Government. The agency appointed to lead this effort, should partner with one or more academic institutions to help accelerate the effort.