FEDERAL IT SUMMIT SERIES

AUGUST 2019
FEDERAL MOBILE SUMMIT REPORT*

December 16, 2019

Jeff Stein, Cameron Boozajomehri, John Remmes, DJ Shyy,
Collin McRae, Cj Rieser, Justin F. Brunelle
The MITRE Corporation

Tom Suder
The Advanced Technology Academic Research Center

Contents

1 ABSTRACT

The most recent installment of the ATARC (Advanced Technology Academic Research Center) Federal Mobile Technology Summit was held on August 6, 2019, in Washington, D.C. During this summit, five MITRE-ATARC Collaboration sessions provided representatives from industry, academia, government, and MITRE the opportunity to discuss challenges the government faces in the adoption and use of mobile technology. This year's collaboration session participants explored a variety of topic areas consisting of Mobile Identity Management, the 21st Century Integrated Digital Experience Act (IDEA) [1], 5G, Mobile Security and FISMA Metrics, and Mobile Health. Within these discussions, participants worked to understand challenges in these specific areas as well as develop a set of recommendations moving forward.

The Mobile Identity Management session participants investigated how to leverage existing identity sources for mobile identity management and discussed some of the confusion regarding the current guidance on the topic. The 21st Century IDEA session focused on the implementations of the act, specifically with regard to cost and security requirements for implementation, cultural barriers to implementation, as well as better understanding how it would be enforced. The Mobile Security and FISMA Metrics discussion explored the difficulty in developing and adopting new mobile metrics as well as the challenges of mobile security in general with regards to FISMA. The 5G discussion focused on supply chain issues regarding 5G hardware, a lack of US-made equipment, and the expanded attack vectors of 5G as compared with older 4G technology. Lastly, the Mobile Health session explored how to improve engagement between providers and patients, requirements for mobile health services moving forward, and how to realize the patient benefits of mobile health.

The summit sessions provided valuable insight to the participants. The following summarized findings provide the main take aways from each session.

> The Mobile Identity Management session recommended taking stock of the current state of an agency's enterprise and current identification procedures and protocols, moving toward zero trust, and more collaboration between industry and government.
>
> The 21st Century IDEA session recommended that as assets are developed and upgraded, agencies should focus on adopting industry best practices as well as focusing on a unified development strategy where both mobile and non-mobile content are treated equally rather than having to maintain multiple development lines. Additionally, the group came up with a vision of what success would look like five years in the future.

The findings of the 5G session were focused primarily on increasing engagement between the United States government and industry with the goals of influencing and incentivizing 5G technology development, participating in 5G standards development, and funding a 5G testbed that can be used as a means of evaluating the effectiveness of 5G technologies to meet different government mission requirements.

The Mobile Security and FISMA metrics session recommended two new metrics as well as suggested FISMA officially adopt a definition of what constitutes a mobile device. Sessions cited that FedRAMP – while a good starting point for cloud security – must often be modified or supplemented to suit agency goals.

The Mobile Health session recommended that mobile health solutions need to increase their focus on enhancing the patient-provider relationship. The discussion then explored a variety of expected outcomes that would stem from this enhanced patient-provider engagement.

2 INTRODUCTION

The latest ATARC (Advanced Technology Academic Research Center) Federal Mobile Technology Summit was held on August 6, 2019 in Washington, D.C. During this summit, five MITRE-ATARC Collaboration sessions provided representatives of industry, academia, government, and MITRE the opportunity to discuss challenges the government faces using mobile. The goal of these sessions is to create an interactive forum for participants to exchange ideas on best practices, recommendations, success stories, barriers, and requirements to advance the adoption of mobile within the government. Participants ranged from Director, Chief Technology Officer (CTO), and other executive levels from government and industry to practitioners from government, industry, and MITRE. Each collaboration session had a MITRE, government, and industry lead to facilitate the participants' discussions about challenge areas in mobile and create recommendations to address these challenges.

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs)[1] [12]. 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 Technology Summit.

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. The sessions for this summit addressed the following topics:

- Mobile Identity Management
- 21st Century Integrated Digital Experience Act
- 5G

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

- Mobile Security and FISMA Metrics
- Mobile Health

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

3.1 Mobile Identity Management

The Office of Management and Budget (OMB) has released M-19-17 [14], providing guidance for the rapid delivery of new Authentication and Access Management Technologies. This memorandum introduces a path toward more flexible authentication tools that agencies hope will transform how they secure their enterprise. However, many participants were clear that though they understood the spirit of the memorandum, they were still uncertain how to turn these goals in to a tangible roadmap for their agencies. Much of the session discussion would center on defining these next steps, specifically how each agency should understand Identity in the context of their enterprise, and how to adopt concepts such as Zero Trust into their agency's architecture.

3.1.1 Goals

The goal of this session was to explore the implications of M-19-17, with a focus on the following topics:

- Exploring agency use cases in the in the context of User and Device Identity
- Expanding on the concept of Zero Trust [8]
- Identifying challenges around Device Context and Shared Devices
- Recommend guidance on identifying appropriate levels of assurance for each use

3.1.2 Challenges

Participants identified several challenges with adopting mobile identity tools and technologies.

- Lack of clarity or guidance on leveraging existing credentials as agencies migrate to new methods for identity management.
- Lack of guidance on blending government approved tools and technologies with more readily available commercial solutions.

- NIST guidance for achieving different assurance levels for users and devices can often be in conflict with an agency's own mission [4].

3.1.3 Discussion Summary

The session began with introductions including participants' organizations and critical use cases. Many participants explained they were attending with the simple goal of understanding what exactly is "Mobile Identity Management" in hopes of learning how it might apply to their specific agency. Although some agencies have started down the path of mobile identity management, there was a clear disconnect between the success of the adopters and those looking to adopt due to a described lack of cross talk between agencies. Industry representatives were also in attendance, eager to learn each agency challenge to adopting Single Sign On (SSO)[3] and cloud-based approaches.

After introductions, session discussion shifted to an exploration of what exactly is "Zero Trust" and how it fit into the memorandum. Zero Trust describes a security paradigm in which no user, device, or system resource is trusted by default. Traditional IT security often took a "castle-and-moat" approach to security in that anyone or anything requesting access from outside the network was scrutinized, but those inside the network were trusted by default. This is problematic in the event a bad actor is able to circumvent security measures at the perimeter, or able to directly access the network from an internal resource. Zero Trust shifts this paradigm to say that no user or device should be automatically trusted, regardless of their location in the network and should be subject to ongoing verification. Furthermore, it puts an emphasis on strict access controls, the need for multifactor authentication, and the utilization of "context" [8] during verification.

This bled into conversation of how to treat Zero Trust in the context of other regulations and guidance such as NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations) [6], NIST SP 800-63-3 (Digital Identity Guidelines) [4], NIST SP 800-171 Rev. 1 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) [5], and FIDO 2 [3]. FIDO 2 proved particularly relevant to the conversation in that it centers on approaches and best practices used by agencies that had successfully adopted new SSO and Authentication mechanisms. This conversation helped identifying several important themes and concepts for session participants. Primarily, Zero Trust demands a re-evaluation of existing security architecture norms as users and devices begin to access agencies' resources from within the network, outside the network, and across multiple geographic and identity contexts. Network boundaries are no longer as well-defined as they

[3] techopedia.com/definition/4106/single-sign-on-sso

once were and – as a result – Zero Trust is becoming more important for protecting agency resources within network boundaries.

Overall, agency representatives who had successfully adopted Mobile Identity emphasized that – in most respects – the key to success came from leveraging security practices already in place. If an identity is already established, then leveraging derived credentials will be critical. The same is true for the devices themselves. Participants from government and industry expressed promise in merging commercial applications with users' personal devices, and Zero Trust to reduce the hardware management burden on agencies. A common theme throughout the discussion was that agencies are not solely interested in building solutions to make things easier for themselves but are dedicated to building tools that make life easier for citizens. Agencies want citizens to feel confident when interacting with the government, ideally providing a unified user experience across all government services.

3.1.4 Recommendations

The session produced several key findings as agencies move toward new modes and implementations of mobile identity management.

- **Zero Trust**: Agencies should move to adopt Zero Trust. Participants felt that Zero Trust was particularly well suited for the current mobile landscape where the distinctions between network boundaries have started to blur.
- **The Enterprise As-Is**: Agencies need to develop a clear understanding of the current state of their enterprise, including understanding existing methods of identify management, credentialing, and assurance. They should plan to utilize these existing resources where possible and adopt new identity management solutions where appropriate.
- **Continued Industry/Government Communication**: Industry and government want to collaborate for the good of the citizen but can have difficulty moving toward a single solution. Success can only be achieved when agency needs are clearly communicated, and industry or agencies' solutions are tailored to those needs.

In summary, this session involved an active exploration of mobile identity management and its value as agencies look to adopt new mobile solutions. Government participants were quick to engage and share agency use cases they felt most related to their enterprise. All shared in proactive conversation on how to leverage mobile technologies for identity management. By the end of the session it was clear to many participants that the promise the technology offers is worth the effort of its implementation.

3.2 21st Century Integrated Digital Experience Act

The 21st Century IDEA collaboration session explored the potential impact of the 21st Century Integrated Digital Experience Act [13]. The Act requires all government-produced digital products, including websites and applications, to be consistent, modern, mobile friendly, and to comply with the web standards developed by the Technology Transformation Service of the General Services Administration (GSA)[4]. Additionally, it calls for all in-person services, forms, and paper-based services, to the greatest extent practical, be available in a digital format.

3.2.1 Goals

This session focused on the impacts of the 21st Century IDEA. Passed by Congress in December of 2018, the 21st Century IDEA seeks to modernize and standardize the government's digital presence. This session set goals to discuss challenges and solutions around the following topical areas:

- Defining what the 21st Century IDEA is and what problems it seeks to solve
- Defining the scope and enforcement of the Act
- Gathering input from domain experts on development of standards and practices as well as definitions of success

3.2.2 Challenges

The session identified several challenges and questions, specifically related to implementation and enforcement of the 21st Century IDEA.

- **Cost and budgets are often mismatched**: How do agencies afford to implement the changes and how does it change budgets for non-digital services?
- **Security is not addressed in the 21st Century IDEA**: To what extent must an agency make digital services and experiences secure?
- **Government has a persistent cultural aversion to new standards**: How does government culture affect the digital current experience; how do we change it for the better?
- **Enforcement is not defined by the 21st Century IDEA, itself**: How should the 21st Century IDEA be enforced and who is responsible for enforcing?

[4] `https://www.gsa.gov/technology`

3.2.3 Discussion Summary

The session opened with introductions and a brief description of the Act from one of the moderators. They explained that the general focus of the Act is to improve the public-facing digital experience of government websites, apps, as well as the digitizing of existing paper forms. In order to accomplish this focus, several phases are outlined in the Act.

The first phase of the 21st Century IDEA focuses on data collection. According to guidance outlined in the Act, government organizations will collect data on all websites they operate as well as metrics on traffic. This data will then be used to create a prioritized modernization schedule. Additional data collection requirements, due at a later date, will have the organizations provide cost estimates for digitizing all their services, as well justifications for not digitizing specific services. This set of data will then be used to create a second timeline that focuses on the digitizing of non-digital services. Following phases will focus on implementing the modernization and digitization as well as continuing data collection and monitoring.

The Act specifies that new and redesigned websites are to be secure, accessible for those with disability, have a consistent appearance, search function, and be fully functional and usable on mobile devices. Some of these standards are not clearly defined. The 21st Century IDEA does not specify what it defines as secure. In the future those standards will be defined by GSA, input by subject matter experts, as well as some of the results from the data collected.

The later half of the session focused on confusion or concerns about 21st Century IDEA. One such concern was about enforcement. Questions were asked such as "who would enforce the 21st Century IDEA and how much strength is behind the enforcement?" Ultimately, Congress is responsible for enforcement of the 21st Century IDEA. Accessibility was another concern of the participants, and it was clarified that government resources will comply to Section 508 [11].

Implementation was also a large focus. Development tools were discussed as a means to standardize websites. GSA, for example, already provides tools (e.g., the Federalist[5]) that can be used to develop and maintain sites. Focus groups were discussed as a way to help develop better requirements and standards. Using crowdsourcing for developing apps for agencies was also mentioned as a possible way to modernize apps.

The session concluded with the participants defining what they believe success would look like five years later. The participants developed a variety answers that all focused on different aspects of the 21st Century IDEA. Many of the ideas of success were abstract and difficult to measure, while others offered up actual metrics. While these ideas were varied,

[5] `https://federalist.18f.gov`

the participants thought that success was attainable and had a positive outlook on the Act.

3.2.4 Recommendations

Through the discussion, recommendations were made about areas that need to be focused on as well as what success means five years in the future. Several recommended focus areas were proposed.

- **Culture and Big Picture**: The 21st Century IDEA is designed to provide a better digital experience to American citizens. As such, it is necessary for agencies to remember that modernizing is not about checking off requirements from a list, but making changes to websites, processes, and metrics that will go into making life for citizens better. It is also important to note that many of the tools and practices that could best improve user experience may not be standard government practice or tools. In order to bridge this gap, ideas were discussed such as providing the public with APIs to make and maintain their own apps, government hackathons[6], as well as other real-world examples.

- **Mobile Devices and Omni-channel Strategy**: The participants recommended that multiple options be considered and assessed regarding how the government supports mobile devices. Much of the discussion centered around app-based, web-based, and hybrid experience and the benefits of each. A participant brought up the omni-channel strategy as a solution/paradigm to help in assessing the benefits the 21st Century IDEA would bring . Instead of focusing on parallel development of apps and websites, government should develop these tools with a focus on resource sharing and integration. This well help integrate and develop new technology.

- **Definitions of Success**: The participants defined success in several different ways. Some definitions were more qualitative such as culture shifts and changing the approach toward digital experience and user experience (UX). Others defined success in more quantitative ways, such as using third-party surveys and ratings. Success for an organization would be defined as higher ratings and rankings. Overall, the participants defined success as decreasing the digital footprint of the government while increasing the digital experience.

[6] A hackathon is an event in which a large number of people meet to engage in collaborative computer programming with the goal of solving a problem or innovating.

3.3 5G

5G is the 5th generation mobile technology promising to provide broadband access, speed, and reduced latency. Concerns surrounding this new technology include interference problems, espionage, radiation, and financial burden.

The pace of evolution for wireless and cellular technologies is rapid, and the world is migrating from fourth generation to 5G wireless networks and technologies. Commercial 5G services have begun to be deployed around the globe in 2019.

The objective of this session was to provide an overview of 5G main usage scenarios and discuss the challenges government is facing, as well as recommendations.

3.3.1 Goals

As 5G technology emerges, government agencies will face a variety of obstacles such as supply chain risk management, points of engagement with users, vulnerabilities with legacy networks, and monitoring of network traffic. This collaboration session explored how agencies will navigate these issues.

3.3.2 Challenges

There are several common challenges of deploying and adopting 5G within the government.

- **Lack of US-made equipment**: The United States leads the world in mmWave antenna array development but lacks leadership, or even a presence, in other 5G areas. Some other major players are Ericsson (Sweden), Nokia (Finland), Samsung (South Korea), and Huawei (China). What are strategies to incentivize US manufactures to build 5G equipment, and in the case that is not possible, what can be done to mitigate the risk of using foreign components?

- **Expanded Threat**s: 5G provides a flexible and scalable design and, as a result, the use cases supported by 5G are virtually endless. Where 4G is mainly to interconnect phones, 5G allows for the interconnection of virtually any device including mobile handsets, Vehicle-to-Everything (V2X) enabled vehicles, robots used in automation, Internet of Things (IoT) sensors for home appliances, delivery industries, smart farming, smart cities, and smart bases. This, in turn, means there is a significantly expanded threat surface as compared with 4G.

- **Software Virtualization**: Whereas 4G is primarily a hardware-based infrastructure, 5G relies heavily on software and virtualization. This can introduce additional security concerns. What will the security guidance be to solve these issues?
- **Network Slicing**: Network slicing is unique to 5G cellular technology. Network slices have the potential to meet various government missions by providing end-to-end security and guaranteed Quality of Service (QoS) [9]. Network slices will need to be independent, isolated, and separate; however, current methods lack the ability to be tested due to the relative immaturity of the tools.

3.3.3 Discussion Summary

This session discussed the use cases, features, and adoption strategies of 5G.

3.3.3.1 High-level Use Cases The International Telecommunications Union-Radiocommunications Sector (ITU-R) defines the requirements/capabilities for 3G, 4G, and 5G, as well as their specifications for global standards. The 3rd Generation Partnership Project (3GPP) is developing the standards for 5G, most of which will be contained in releases 15 and 16. The ITU International Mobile Telecommunications-2020 (IMT-2020) [10] defines the following three main usage scenarios for 5G:

- Enhanced mobile broadband (EMBB)
- Critical communications with ultra-reliable and/or low latency
- Massive machine type communications in support of IoT / Machine to Machine (IoT/M2M)

The applications and capabilities for supporting each of the three usage scenarios are summarized in Figure 1. EMBB's primary focus is higher data rates. The improvement of peak data rates from 4G to 5G is from 1 Gbits/s to 20 Gbits/s. The typical applications include 4K/8K ultra-high-definition (UHD) video, fiber replacement, augmented reality, and virtual reality.

Mission-critical communication requires enhanced capabilities for high reliability (up to 99.999% for packet success rate), low latency (down to 1 ms), and high mobility (up to 500 km per hour). The mission-critical service usage scenario is designed for health, government, or financial applications with stronger security and a need for a more trusted architecture.

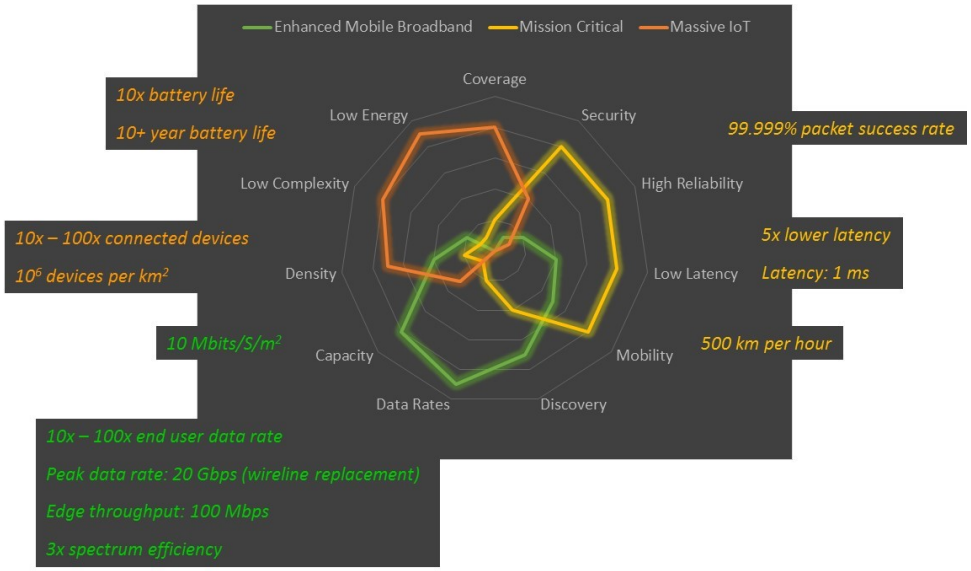

Figure 1: Usage scenarios and their capabilities for 5G. The stated capability improvements are found in ITU-R M.2410-0 [10]. The qualitative comparison of the relative strengths of the three use cases is MITRE's assessment.

Some of the applications include V2X communications, remote surgery, industry automation, and disaster recovery using drones.

Massive IoT requires the design of low complexity and low power consumption devices, which translates to longer battery life. In addition, this requires the ability of the base station to serve thousands of devices in a small geographical area. Figure 1 summarizes the capabilities required for each of the usage scenarios.

3GPP R-16 introduces the support of non-terrestrial networks (NTN) as the 4th usage scenario. The focus of this usage scenario is for global coverage. The NTN includes satellite communications (geosynchronous equatorial orbit (GEO), medium Earth orbit (MEO), and low Earth orbit (LEO)) and unmanned aerial vehicles. Applications for this scenario include the following:

- IoT (e.g., for agriculture, critical Infrastructures metering, asset tracking)
- Public safety and associated emergency networks

3.3.3.2 Technology Capability The ITU definition of 5G services, which requires significant capability improvements over 4G, are shown in Table 1.

To achieve the aforementioned capability improvements, 5G is equipped with a variety of technology enablers. One such feature is the flexibility in the time and frequency domains

Key Capability	4G	5G
Peak data rate (Gbits/s)	1	20
User experienced data rate (Mbits/s)	10	100
Relative spectrum efficiency	1x	3x
Mobility (km/h)	350	500
Latency (ms)	10	4 (EMBB); 1 (Mission Critical)
Connection density (devices/km2)*	105	106
Relative network energy** efficiency	1x	10x
Area traffic capacity*** (Mbit/s/m2)	0.1	10

Table 1: Capability Improvements from 4G to 5G
** Connection density: The number of connected devices in a given area*
** Relative network energy efficiency: A ratio of how much network energy is required vs. how much energy is used for network traffic*
*** Area traffic capacity: A measure of the maximum amount of data that can be sent per second in a given area*

of the new air interface known as "new radio" (NR). Another technology enabler is called network slicing.

The prerequisite for network slicing is the resources of various aspects of the network are virtualized in the form of virtual functions (VFs). Slices, created by integrating multiple VFs, can deliver differentiated levels of quality of service and security to different sets of users with various performance requirements.

The 3GPP standards for 5G will be finalized in two phases. 5G Phase 1 was completed in July 2018 and codified in the 3GPP Release-15[7]. The capabilities included in 5G Phase 1 are mainly tailored to the EMBB usage scenario. 5G Phase 2 will be completed in 3GPP Release-16[8] with an expected timeline of 2Q 2020. The focus of Phase 2 will be enhancing 5G capabilities to serve massive IoT and mission critical services.

Both standalone (SA) and non-standalone (NSA) deployment options are included in the 5G Phase 1 specification. An NSA deployment means that the 5G radio access network (RAN) is deployed for faster data speeds while using an existing 4G RAN and core network as its anchor. 5G devices will be connected to 4G and 5G RANs at the same time, using 4G for signaling and both 4G/5G networks for data. This provides a gradual transition from Long-Term Evolution (LTE) to 5G, such that LTE carrier's investments can continually be used. An SA deployment implies that the 5G core and RAN are fully operational and independent of any other radio access technology. Currently, all U.S. 5G providers offer 5G Phase 1 services

[7] `https://www.3gpp.org/release-15`
[8] `https://www.3gpp.org/release-16`

with NSA option in selected cities. SA deployments will not occur until late 2020.

3.3.3.3 Spectrum and Deployment Strategy The initial 5G deployment model focuses on using fixed wireless as a replacement for fiber or cable, particularly for network backhaul and interconnection applications. 5G mobility services follow the fixed deployment. The expected deployment scheme for mobility services for at least the next five years is to have high capacity 5G cells that coexist with larger coverage LTE cells to balance capacity and coverage requirements. These deployments can be categorized into the following three technology groups, with the focus on millimeter wave (mmWave) spectrum, where the mmWave spectrum is defined to be between 30 GHz and 300 GHz:

- 5G NR mmWave (short range)
- 5G NR sub-6 GHz (medium range)
- LTE below 2 GHz (long range)

Another way of looking at 5G deployment is to differentiate various usage scenarios by their most appropriate spectrum bands, as described below. These classifications are not rigid, but rather provide a general guideline for expected deployment; these general categories are listed below:

- mmWave: Broadband
- Mid Bands: Mission Critical
- Below 1GHz: Longer Range (IoT)

3.3.4 Recommendations

5G technology continues to evolve. Government should continue to track newly developed 5G technologies, analyze 5G capabilities, and investigate their potential impacts on government missions. There are several recommended methods of achieving these goals.

- Form partnerships between government and industry to collaborate in 5G research.
- Engage commercial vendors to inject government requirements into 5G products during the earlier stages.

- Influence the development of 3GPP 5G standards and ATIS[9] supply chain standard by adding government requirements in the standards.
- Fund the development of a 5G testbed which is tailored to reduce risk to demonstrate the solutions to meet government requirements.
- Participate in a 5G Secure Profile meeting with participation from government, industry, and academia to jointly develop 5G security guide.

3.4 Mobile Security and FISMA Metrics

The Mobile Security and FISMA metrics session focused on assessing agencies' progress toward achieving outcomes that strengthen federal cybersecurity. In particular, the FISMA metrics are used to do the following tasks:

- Ensure that agencies implement the governments priorities and best practices
- Provide the OMB with the performance data to monitor agencies' progress toward implementing the Administration's priorities

3.4.1 Goals

This session set goals to discuss challenges and solutions around several topical areas.

- Identify the classifications of mobile device that fall under FISMA.
- Discuss ways to create a standardized set of FISMA mobility metrics for use across all agencies.

3.4.2 Challenges

During the course of the Mobile Security and FISMA session, several key challenges were noted from both industry and government participants. Two challenges in particular were identified as the most impactful to the implementation of FISMA metrics.

- It is difficult to create new metrics that encompass mobility across all agencies.
- Mobile security is not a primary consideration of FISMA.

[9] https://www.atis.org/01_strat_init/5G/

3.4.3 Discussion Summary

The session began with a discussion of how FISMA metrics are formed, specifically around mobility. It quickly became apparent that there is not a standard definition of a mobile device. While a NIST specification exists for mobile devices (NIST 800-53 [6]), most agencies use it as a baseline for creating compliance standards and further tailor it to suit their individual needs. This leads to a lack of homogenous compliance standards for use by industry, leading to difficulty in supporting more than one contract.

The session participants frequently cited the lack of a definition of "mobile" throughout the session and to frame most discussions. This absence of a common definition persists in the private sector, as well. Industry members indicated that mobility can be considered anything that is provided to an end user and touches cellular. Ultimately, the participants defined a device as being mobile if it runs the Android or iOS operating systems. Security for desktop operating systems is often much better than the security on mobile operating systems. Classifying a mobile device as any device running Android or iOS can lead to misclassification of some IoT devices, but the contributors generally agreed it would be a very useful definition in the context of FISMA.

Following the discussion of mobile device classification, the group discussed potential new metrics. First, the group touched on how user identity is managed on devices. Industry contributors agreed that the level of information on the device (e.g., PII, FOUO) should be linked to how users authenticate. This led to the suggestion of a minimum standard of authentication to access sensitive information both on the device and remotely. Another new metric discussed included a ratio of devices managed by Mobile Device Management (MDM) systems versus the number of total devices owned. This metric would primarily function to assist industry in understanding how many devices are registered through the proper channels, as opposed to BYOD devices being improperly used. Finally, the last metric introduced would define anything as "mobile" if it was able to remotely access a corporate network. This definition would also make the distinction between a mobile device and mobile endpoint based upon the operating system in use. The session concluded with a review of the new metrics proposed, and potential avenues for improving the roll out process of future metrics.

3.4.4 Recommendations

The following new metrics should be introduced to FISMA:

- Minimum standard of authentication required to access sensitive information on the

device and remotely

- Ratio of devices managed by MDMs versus the total number of devices owned

Additionally, the group would like FISMA to make the following official definition of a mobile device:

> A mobile device is anything that can access data remote from a corporate network. Devices themselves should categorized based upon their operating systems, with endpoints being classified as mobile devices not running Android or iOS.

3.5 Mobile Health

The Mobile Health session focused on the use of mobile devices to enhance and provide healthcare services. Specifically, the session focused on the use of mobile devices to assist with the generation of mobile health (mHealth) records, the current regulatory issues, enablement of tele-medicine, the potential benefits of real-time biometric data alerts, and potential mobile healthcare payment solutions.

3.5.1 Goals

This session had several goals.

- Discuss the implications of mHealth records and delivering healthcare with the assistance of mHealth.
- Discuss the regulatory challenges of using mobile devices to assist healthcare providers.
- Consider the challenges and benefits of mHealth for the practitioner and patient.

3.5.2 Challenges

The Mobile Health session participants identified the following key focus areas for mHealth adoption:

- Improving patient-provider engagement
- Realizing patient benefits
- Requirements for future mHealth services

The participants noted that these focus areas will need to be resolved to facilitate mHealth adoption. The participants also highlighted the need for – and challenge of – cross domain collaboration (e.g., between practitioners, technologists, and patients) to enable innovation in the mHealth space. The benefits of mHealth are likely predicated upon the advancement of Electronic Health Record (EHR) services and solutions.

3.5.3 Discussion Summary

This session began by discussing the clinical need for mHealth solutions. The participants mentioned that mHealth solutions would ideally be able to help identify population-based needs based on given criteria or standards. Additionally, mHealth solutions could be utilized to conduct analysis on organizations or persons as well as what medical conditions exist. This analysis could be leveraged to identify alternative mobile health solutions.

After discussing the need for mobile health solutions, the discussion moved to the need for patient data as well as the challenges associated with managing the data. Data integration is important to enable data-driven knowledge and decisions. The more data in a system, the smarter the system is able to become. The utilization of sensors is one way to increase the amount of data in a system. IoT leveraged for clinical purposes is a low-cost avenue for accumulating a large amount of data. Augmented intelligence (AI) is a way to leverage patient data because it is good at matching information. While discussing the benefits of AI, software developers mentioned the need for healthcare experts and professionals to provide input on how to match the information to create a useful and smart system. In mHealth, any discussion of patient data must be coupled with the need for privacy. Gathering data through sensors and IoT presents a unique privacy concern because there are always-on devices. Global data and analytic privacy laws such as the General Data Protection Regulation (GDPR)[10] are dramatically reshaping the mobile app ecosystem and insights on how data is used.

The discussion then moved to the gaps in collaboration that limit effective implementation of innovation. New innovations are only useful if they address a healthcare need. Software developers need healthcare professionals to tell them what they need. By working with the need in mind, software developers will be able to produce a product that is beneficial to healthcare professionals. This kind of community-driven collaboration will allow the healthcare industry to take advantage of new technologies. In helping patients manage their condition(s), a challenge for app developers will be to develop holistic mHealth apps rather than focusing on a single condition. Some tools and vendors' individual EHR and electronic

[10] https://gdpr-info.eu/

medical record (EMR) systems advertise a promise to integrate and consolidate data from multiple health apps.

The session participants also discussed the current opportunities in the adoption of mHealth. Integration is underway of mobile health patient generated health data into large scalable environments and ecosystems like the Department of Veteran Affairs (VA) Open Application Programming Interface (API) [7] with EHRs and EMRs, smartphones, and other medical devices that empower consumer-provider communications.

Patients who use mHealth services are more likely to be actively engaged in their health-care management and diagnostics[11]. One provoking question is whether some consumers are opting out of shared decision making with their providers in their pursuit of their own health improvement due to physicians' reluctance to embrace mHealth.

mHealth apps incorporated into a patient's daily living have the potential to enhance patient-provider engagement and data-sharing. Physicians can access mobile apps to inform evidence-based decision making. The key limiting factor slowing adoption of mHealth among providers (along with privacy concerns) is the barrier of direct payment for mHealth. The barrier of direct payment for mHealth is lowering for providers as they take on more value-based forms of reimbursement, including pay-for-performance, bundled payments, and assuming the role of the medical home.

When adopting mHealth tools, clinicians highly rank extending patients preventive support, continuity of care, and telehealth as areas where mHealth can positively impact care. For providers who use an EHR, there may be a need to integrate the information coming from a patient's mHealth app into the EHR - if this does not integrate seamlessly into the EHR workflows, it may be a barrier to provider adoption of these tools. Along with cost, privacy is a key barrier that physicians cite in their adoption of mHealth technologies. As wearable health device adoption grows among consumers, regulators are focusing in on health data security. It is important to plan a strategy for measuring success well in advance of the launch. Some emerging standards like IEEE P2795 [2] focus on creating communities of care via sharing personalized privacy preserving medical analytics to the edge without necessarily centralized third-party data accumulation, instead allowing metadata analytic exchange networks.

There are many potential long-term metrics of success for an mHealth initiative. It may be successful based on clinical outcomes, sustained use, costs saved, or loyalty to the institution. Whatever the goals for the application, it is critical to create programs to track and measure indicators of success from the beginning.

[11] https://www.himss.org/mhealth-app-essentials-patient-engagement-considerations-and-implementation

3.5.4 Recommendations

Patient-Provider Engagement: mHealth solutions need to focus on improvements to patient-provider engagement. This is a challenge that - once resolved - has the following features:

- Taking a patient's needs, wants, and goals into consideration when designing treatment plans
- Facilitating shared patient-provider decision making on a patient's goals and treatment plans
- Increasing a patient's willingness to follow through on jointly developed treatment plans
- Supporting patient empowerment such that patients become proactive in the management of their overall health

In support of this larger goal, mHealth services are likely to exist in apps that provide daily features such as the following:

- Supports patients in pursuit of their daily goals
- Enables patients to have follow-up discussions based upon a history of mHealth app information shared with their healthcare provider

With these recommended service features, along with tracking daily health, an mHealth solutions should allow a patient and provider to increase the frequency and flexibility of communication in the following ways:

- Providing disease-specific information
- Facilitating communication with their provider outside the office setting
- Addressing questions as patients evaluate their decision to make a change
- Enabling patients to obtain an answer quickly from their provider

4 SUMMIT RECOMMENDATIONS & CONCLUSIONS

The August 6 2019, Federal Mobile Technology Summit highlighted several challenges facing the federal government's adoption and integration of mobile technologies and presented recommendations to address those challenges.

This year's collaboration session participants explored a variety of topic areas consisting of Mobile Identity Management, the 21st Century IDEA, 5G, Mobile Security and FISMA Metrics, and Mobile Health. Within these discussions, participants worked to understand challenges in these specific areas as well as develop a set of recommendations moving forward.

The Mobile Identity Management session investigated how to leverage existing identity sources for mobile identity management and discussed some of the confusion regarding the current guidance on the topic. The group recommended that agencies need a complete understanding of the unique characteristics of their organization before adopting new mobile technologies and as they move toward a Zero Trust model of identify management. When adopting Zero Trust, they should leverage existing identity management use cases and derived credentials. Lastly, organizations may need to tailor existing legislation and guidance to their specific needs in order to be successful.

The 21st Century IDEA session primarily focused on the implementations of the Act, specifically with regard to cost and security requirements for implementation, cultural barriers to implementation, and a better understanding of how it would be enforced. The group mapped out what success would look like in five years and discussed what would be needed to get there. Organizations should adopt the spirit of the 21st Century IDEA, which is to improve digital experiences for all Americans, rather than try to meet the specific requirements at the loss of the bigger picture. The current landscape between apps and websites is somewhat fragmented; the group recommended that agencies to move toward a unified development landscape where a single code base can support both the web and apps. Lastly, a variety of success metrics were discussed, ranging from both objective and subjective measures.

The 5G discussion focused on supply chain issues regarding 5G hardware. Specifically, there is a lack of US-made equipment and the expanded security concerns of 5G as compared with older 4G technology. The group recommended the government needs to stay abreast of 5G developments and should do a better job of partnering with industry and academia to both research 5G as well as inject specific government requirements into 5G products during early stages of development. Additionally, the participants suggested building a 5G testbed to mitigate and reduce risks as well as working across industry and academia to generate a 5G Security profile.

The Mobile Security and FISMA Metrics discussion explored the difficulty in developing and adopting new mobile metrics as well as the challenges of mobile security with regard to FISMA guidance. The group recommended the need for a broader definition of what constitutes a mobile device, specifically anything that can access data remotely. They suggested a metric for minimum standard of authentication required to access data remotely as well as a ratio of devices managed by MDM vs. non-managed and personally owned devices.

The Mobile Health session explored how to improve engagement between providers and patients, requirements for mobile health services moving forward, and how to realize the patient benefits of mobile health. The primary recommendation that came out of this discussion was that mobile health solutions need to focus on improving the patient to provider engagement. Once established, this enhanced patient-to-provider relationship should have many benefits to the healthcare industry, including increasing the ease at which providers and patients can communicate, ultimately improving patient outcomes.

Participants were excited about the future of mobile technology within the US government. They see a bright future for both employees and the American citizen. Across the sessions, however, two themes arose specifically regarding areas for improvement:

- Security concerns with regard to new technology
- Lack of clarity or guidance on policy, recommendations, and regulations

Participants highlighted that as the government starts to use and adopt new technology, it's likely that existing security procedures will become outdated or no longer applicable. Participants highlighted the importance of making sure that security is a first-class concern when adopting new technology. Additionally, they desired more guidance and clarity on the "right way" to implement security within their organizations moving forward, as well as the best way to account for security metrics.

In conjunction with this concern, participants felt both confused and overwhelmed with the number of technological options available – either lacking clear government guidance about the technology, or not understanding existing guidance. In the cases where regulations existed participants were unclear on the implementation and enforcement details - and in the cases where there were no regulations, participants sought to have some sort of official guidance.

5 ACKNOWLEDGMENTS

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 who helped make the collaborations and discussions possible. A full participant list is maintained and published by ATARC on the ATARC Mobile Summit website[12].

REFERENCES

[1] 115th Congress. H.R.5759 - 21st Century Integrated Digital Experience Act. https://www.congress.gov/bill/115th-congress/house-bill/5759/text, 2018.

[2] EMB/Stds Com - Standards Committee. P2795 - Standard for Shared Analytics Across Secure and Unsecured Networks. https://standards.ieee.org/project/2795.html, 2018.

[3] FIDO Alliance. FIDO2: WebAuthn & CTAP. https://www.congress.gov/bill/115th-congress/house-bill/5759/text, 2019.

[4] NIST. Digital Identity Guidelines. Technical Report Special Publication 800-63-3, National Institute of Standards and Technology, 2017.

[5] NIST. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Technical Report Special Publication 800-171, National Institute of Standards and Technology, 2018.

[6] NIST. Security and Privacy Controls for Federal Information Systems and Organizations. Technical Report Special Publication 800-53, National Institute of Standards and Technology, 2018.

[12] https://atarc.org/event/mobile-summit-2019-08/

[7] Office of Public and Intergovernmental Affairs. VA announces new Veterans Health Application Programming Interface. https://www.va.gov/opa/pressrel/pressrelease.cfm?id=5158, 2018.

[8] PaloAlto Networks. What is a Zero Trust Architecture? https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture, 2019.

[9] Radiocommunication Sector of ITU. IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. Technical Report M.2083-0, International Telecommunications Union, 2015.

[10] Radiocommunication Sector of ITU. Minimum requirements related to technical performance for IMT-2020 radio interface(s). Technical Report M.2410-0, International Telecommunications Union, 2017.

[11] Section508.gov: GSA Government-wide IT Accessibility Program. IT Accessibility Laws and Policies. https://www.section508.gov/manage/laws-and-policies, 2019.

[12] The MITRE Corporation. FFRDCs – A Primer. http://www.mitre.org/sites/default/files/publications/ffrdc-primer-april-2015.pdf, 2015.

[13] The Office of Energy Efficiency & Renewable Energy. The 21st Century Integrated Digital Experience Act. https://www.energy.gov/eere/communicationstandards/21st-century-integrated-digital-experience-act, 2019.

[14] R. T. Vought. M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management. https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf, 2019.