NEXT GENERATION FIRST RESPONDER
CASE STUDY
MOBILE DEVICE MANAGEMENT

What's Inside?

1.....Executive Summary

3.....Introduction

4.....OpEx Overview

15.....OpEx Results

16.....Implementation for Your Agency

18.....Summary

19.....References & Recommended Reading

Want More?

To learn more about the NGFR Apex program, associated projects, and how DHS supports first responders nationwide, visit our website and social media accounts and LIKE, CLICK and SHARE!

WEBSITE
www.dhs.gov/NGFR

FACEBOOK
@DHSSciTech

TWITTER
@DHSSciTech

EMAIL
NGFR@hq.dhs.gov

Homeland Security
Science and Technology

EXECUTIVE SUMMARY

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) launched the Next Generation First Responder (NGFR) Apex program to help tomorrow's first responder become better protected, connected and fully aware. DHS S&T has held a series of NGFR Integration Demonstrations to incrementally test and evaluate interoperable technologies currently in development. These demonstrations have evolved from tabletop integrations to field exercises with partner public safety agencies and have involved increasingly complex technology integration.

DHS S&T partnered with Harris County, Texas, and the City of Houston to host the first major urban NGFR Integration Demonstration in December 2018. The NGFR – Harris County Operational Experimentation (OpEx), involved testing a variety of integrated technologies in an operational environment with participating first responders from Harris County, City of Houston, U.S Coast Guard (USCG), SouthEast Texas Regional Advisory Council, Cy-Fair Volunteer Fire Department and the Atascocita Fire Department.

During the OpEx, Harris County and Houston-area responders and federal partners used integrated responder technologies to enhance their mission capabilities in a hazardous materials (HAZMAT) scenario that includes a simulated gas leak from a USCG Cutter (USCGC) vessel in the Port of Houston. Together, responders and DHS S&T evaluated how DHS-funded and commercial technologies integrated with existing public safety systems using open standards and how those integrated capabilities enhanced emergency communications, increase operational coordination, improve responder safety and augment situational awareness.

The NGFR – Harris County OpEx included 23 different DHS and industry-provided technologies, including six Internet of Things (IoT) sensors, five situational awareness applications and platforms, and live-stream video feeds. Additional OpEx technologies included body-worn cameras, deployable communications systems, and real-time data aggregation and access across multiple agencies.

This case study identifies and explains the mobile device management (MDM) solutions that provided an application-level cybersecurity assessment and remote device management during the OpEx and discusses how nationwide public safety agencies could implement MDM to enhance operational deployment of new devices and applications.

DHS S&T's technical team, DHS-funded and industry partners provided the sensors and integration work to support the OpEx, incorporating the feeds from multiple sensors to multiple situational awareness applications. The OpEx scenario provided sufficient realistic opportunities to assess the technologies and allowed participating responders to identify gaps and required enhancements to improve the participating technologies.

Figure 1. Participants Conduct Simulated Emergency Response Activities During the NGFR - Harris County OpEx

DHS S&T and partners brought new situational awareness capabilities to Houston-area responders, protected via MDM. By integrating data from multiple sensor types into unified situational awareness applications, the NGFR Apex program enhanced operational communications, increased operational coordination, improved responder safety and augmented situational awareness. The OpEx demonstrated that the first responders, incident commanders and emergency managers were able to maintain enhanced situational awareness during the scenario by interacting with the various situational awareness platforms provided for the OpEx, while ensuring necessary cybersecurity needs are met.

Administrative and Handling Instructions

The title of this document is the "Next Generation First Responder Case Study: Mobile Device Management." This document provides public safety agencies with an overview of how DHS S&T implemented MDM during the NGFR – Harris County OpEx and provides some areas that an agency may consider if they choose to implement the capability within their organization. All preparation and documentation for the NGFR – Harris County OpEx is unclassified.

Reference herein to any specific commercial products, processes or services by trade name, trademark, manufacturer or otherwise does not necessarily constitute or imply its endorsement, recommendation or favoring by the U.S. Government. The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. Government.

If you have any questions about this case study, or to request more information about the NGFR – Harris County OpEx, please contact NGFR@hq.dhs.gov. Public release of information is at the discretion of DHS S&T.

Accessibility

DHS S&T is committed to providing access to our webpages for individuals with disabilities, both members of the public and federal employees. If the format of any elements or content within this document interferes with your ability to access the information, as defined in the Rehabilitation Act, please contact the Next Generation First Responder Apex program for assistance by emailing NGFR@hq.dhs.gov or calling 202-254-6060. A member of our team will contact you within two business days. To enable us to respond in a manner most helpful to you, please indicate the nature of your accessibility problem, the preferred format in which to receive the material, the web address (URL) or name of the document of the material with which you are having difficulty, and your contact information.

INTRODUCTION

Next Generation First Responder Apex Program

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) works with America's first responders to ensure they are more effective and safer—regardless of the hazards they face. DHS S&T develops and adapts innovative technologies that help first responders make communities more secure and resilient, because homeland security truly starts with hometown security.

The Next Generation First Responder (NGFR) Apex program is a five-year program that began in January 2015 and is part of a longer-term DHS S&T commitment to envision and assist the responder of the future. The NGFR Apex program works to make responders better protected, connected and fully aware by developing, adopting and integrating cutting-edge first responder technologies using open standards. This complex, multi-disciplinary program consists of a diverse but related portfolio of projects that span from basic research to advanced technology development, and an initiative to define a common set of open standards for technology integration. These open standards enable industry partners to develop standards-based solutions that easily plug-and-play into an interoperable responder ecosystem, including legacy systems. This approach opens doors to industry while lowering costs and increasing choices for public safety organizations, helping them rapidly adapt to changing environments and evolving threats as they secure communities nationwide.

NGFR Integration Demonstrations

Since 2016, DHS S&T has held a series of NGFR Integration Demonstrations to incrementally test and evaluate interoperable technologies currently in development. These demonstrations have evolved from tabletop integrations to field exercises with partner public safety agencies, including the rural 2017 Grant County—DHS S&T NGFR Apex Program Technology Experiment. This case study highlights the efforts, lessons-learned and guidance from the NGFR – Harris County Operational Experimentation (OpEx) that was held in December 2018 in Houston, Texas, to demonstrate the interoperability of DHS S&T and industry-developed responder technology and increase community resilience.

DHS S&T has incorporated the results and responder feedback from the NGFR Integration Demonstrations into the NGFR Integration Handbook, which outlines a standards-based environment that enables commercially-developed technologies to integrate with existing first responder infrastructure. Using the lessons learned and responder feedback from these integration demonstrations, DHS S&T has also produced materials to help public safety agencies implement new technologies that address their operational priorities, such as the NGFR Case Study series, which this document is part of.

NGFR Operational Experimentation in Harris County, Texas

DHS S&T collaborated with public safety agencies from Harris County and the Houston area to host the NGFR – Harris County OpEx from December 4-5, 2018, at the Port of Houston. Participating agencies included Harris County (Fire Marshal's Office, Sheriff's Office Marine Unit, Office of Homeland Security and Emergency Management, Central Technology Services, and Community Emergency Response Team), the City of Houston (Fire Department, Police Department Marine Unit, and Information Technology Services), Port of Houston Authority (Emergency Management, Fire Department, Police Department), SouthEast Texas Regional Advisory Council, Cy-Fair Volunteer Fire Department,

Atascocita Fire Department, U.S. Coast Guard Sector Houston-Galveston, DHS Federal Emergency Management Agency's Integrated Public Alert and Warning System Office, and DHS Cybersecurity and Infrastructure Security Agency's Emergency Communications Division.

The goal of this OpEx was to integrate and demonstrate a variety of cutting-edge responder technologies, assist Houston-area response organizations in incorporating them into their daily operations, gather responder feedback to help improve both individual DHS-funded and industry technologies, and demonstrate the value of the NGFR Apex program. During the OpEx, Houston-area responders and federal partners used integrated responder technologies to enhance their mission capabilities in a HAZMAT and mass casualty incident response scenario in the Houston Ship Channel. Together, responders and DHS S&T evaluated how selected S&T-developed and commercial technologies integrated with existing public safety systems using open standards and how those integrated capabilities enhanced emergency communications, increased operational coordination, improved responder safety and augmented situational awareness.

Purpose of this Case Study

This case study describes how DHS S&T employed mobile device management (MDM) for the smartphones that were provided to support Long Term Evolution (LTE) data communications during the NGFR – Harris County OpEx. It provides an overview of the systems used, the challenges encountered and the solution implemented for the OpEx, as well as considerations that any public safety agency should think through if they intend to implement MDM solutions for their organization.

OpEx OVERVIEW

OpEx Objectives

DHS S&T hosted the OpEx to validate and advance the Next Generation First Responder Apex program, as well as benefit Houston-area public safety and technology provider partners. The OpEx integrated NGFR technologies to support an operationally-relevant, mission-based scenario centered on HAZMAT and mass casualty response operations. The goal of this OpEx was to demonstrate the capabilities of new technologies and provide a proof of concept to participating responders to illustrate how the technologies could be incorporated into daily operations and existing systems. By gathering feedback from first responders on the technologies and how they did or did not augment public safety emergency response capabilities, the NGFR Apex program seeks to better ensure new technologies fully meet responder needs.

Figure 2. Atascocita and Cy-Fair Paramedics connect physiological sensors to an OpEx "patient" prior to transport

OpEx Requirements

Initial discussions with Harris County resulted in the identification of the following technology requirements for the OpEx:

- Geo-location of first responder personnel in three dimensions on map displays provided to the Incident Commander, the command staff and on smartphones carried by responders.
- Capability to monitor patients' physiological condition and send the data wirelessly to the Incident Commander and command staff for viewing using a visual "dashboard" on a monitor and/or smartphone.

- Remote monitoring of HAZMAT using body-worn gas sensors transmitting alerts to the Incident Commander and command staff.
- Integration of all sensor feeds into one data feed provided to multiple situational awareness applications, especially the two existing applications in place or planned for use by Harris County and the Port of Houston (Intrepid Response and AVERT C2, respectively).

DHS Core Capabilities Alignment

The NGFR – Harris County OpEx was shaped around critical requirements identified by operational partners from Harris County, the City of Houston, Port of Houston Authority, U.S. Coast Guard, SouthEast Texas Regional Advisory Council, Cy-Fair Volunteer Fire Department and Atascocita Fire Department. These requirements included helping fill gaps identified during the response to Hurricane Harvey in 2017, particularly gaps around information sharing and multi-jurisdictional coordination. The planning process included joint identification of OpEx objectives and targeted DHS Core Capabilities, which included:

- Operational Communications;
- Operational Coordination;
- Environmental Response/Health and Safety;
- Intelligence and Information Sharing;
- Access Control and Identity Verification;
- Mass Search and Rescue Operations;
- On Scene Security, Protection and Law Enforcement;
- First Responder Safety; and
- Situational Awareness.

OpEx technologies were selected to meet these Core Capabilities and the scenario was developed to test the technologies and the associated operational capabilities.

Figure 3. A DHS Data Collector Observes the Harris County HAZMAT Team During the OpEx

OpEx Scenario

The OpEx scenario provided sufficient realistic opportunities to assess the various technologies' utility and integration with existing systems (technical and human). The scenario also provided opportunities for participating first responders to identify gaps and required enhancements to improve the participating technologies. The evaluation team was able to verify that the NGFR system architecture implemented and configured at the Port of Houston was easy to install, easy to use and provided capabilities that were valued by the first responders.

The NGFR – Harris County OpEx consisted of an operational scenario divided into three vignettes:

- **Vignette A**: A HAZMAT spill occurs on USCGC Hatchet and the resulting gas cloud also affects the civilian vessel, the M/V Sam Houston, following in its wake. The vessels moor across Buffalo Bayou and HAZMAT teams are activated from the Port of Houston, Harris County and the City of Houston, as well as EMS units from the City of Houston, Atascocita Fire Department and the Cy-Fair Volunteer Fire Department. Harris County and the City of Houston marine units respond, as well as the Port of Houston Fireboat 1 and a USCG Response Boat Small (RB-S). All HAZMAT and marine units arrive on scene at the Sam Houston Pavilion and the Battalion Chief from the Port of Houston establishes Incident Command to evaluate the situation.
- **Vignette B**: The Harris County HAZMAT crew sets up a decontamination station at the Sam Houston pavilion, boards the M/V Sam Houston, and starts evaluating the passengers and crew.

HAZMAT crews from the Port of Houston and City of Houston board Fireboat 1 and are transported across the bayou to USCGC Hatchet. They board the vessel to evaluate the crew and identify the source and nature of the HAZMAT spill. They also note that one of the crewmembers is unaccounted and is assumed to have fallen overboard prior to mooring.

- **Vignette C**: Victims from civilian vessel M/V Sam Houston undergo technical decontamination, triage and treatment, and are prepared for transport. Victims from USCGC Hatchet undergo gross decontamination and are then transported by Fireboat 1 over to the pavilion, where they undergo technical decontamination, triage and treatment. The USCG crew and a helicopter search for and find the missing crewman in the bayou, the RB-S crew retrieves him and returns him to the pavilion for decontamination, triage and treatment.

OpEx Technologies

DHS S&T worked with federal, industry and on-contract performers to provide 23 technologies, many of which were integrated to increase information sharing and situational awareness during the OpEx. DHS S&T and partners used data and alert standards to facilitate technology integration, including the Sensor Things server running their Open Geospatial Consortium (OGC) standard Application Program Interface (API), and Message Queuing Telemetry Transport (MQTT). Full descriptions of all OpEx technologies are available in the NGFR – Harris County OpEx Playbook and After Action Report listed in the References and Recommended Reading section. Note that the following descriptions were current as of the NGFR – Harris County OpEx in December 2018, and that throughout this document, technologies are frequently referred to by the name of the company rather than the name of the technology. OpEx technologies relevant to this case study include:

ARES Security Corp.

AVERT C2

AVERT C2 is an intelligent command and control platform that provides collaborative situational awareness by allowing each user to view and share the information sources and layers they need to understand and manage events as they unfold. AVERT C2 ingests and visualizes data from virtually any sensor—including chemical sensors, biometric sensors, cameras, radar, access control and alarm systems—to manage all security and response information through a single user interface.

Haystax, a Fishtech Group Company

Haystax Constellation

Haystax Constellation for safety and security helps first responders prepare and respond with confidence, using a cloud-based platform for early threat detection, situational awareness and information sharing. Haystax Constellation gives first responders advanced analytics to automatically score the highest-priority threat signals and rapidly deliver them to the right people at the right time and provides a tightly-integrated ecosystem of web and mobile apps that enables users to manage their critical assets and respond effectively to incidents and natural hazards.

Intrepid Networks, LLC

Intrepid Response

Intrepid Response is a mobile application that enables enhanced situational awareness by providing live responder locations and static locations of interest with a simple user interface. The mobile application extends situational awareness to the end users, effectively closing the communication loop between first responders, and supervisors and commanders. Open API architecture provides integration capability for higher level command and control tools or other platforms.

Intrepid Connect (Moxtra)

Moxtra, powered by Intrepid Networks, provides robust team collaboration with rich multimedia sharing, whiteboarding, task management and secure text communication. Intrepid Connect supports multiple concurrent operations with role-based channel support, and dramatically reduces reliance on voice communication alone, thereby saving LMR voice traffic for emergency communications.

Metronome Software, LLC

SENSEI – Sensor Secure Enterprise Infrastructure

Currently partnered with MobileIron and Kryptowire, SENSEI integrates Enterprise Mobility Management and Mobile App Vetting technology to provide a comprehensive system of mobile security for Internet of Things and mobile endpoints. SENSEI ensures that mobile apps are risk analyzed prior to deployment and provides users confidence that their mobile devices are not compromised. Metronome Software is currently funded by DHS S&T for this technology.

MobileIron Inc.

Unified Endpoint Management

Provides visibility and IT controls needed to secure, manage and monitor any corporate or employee owned mobile device or desktop that accesses business critical data. Secures all endpoint devices and their information, providing the assurance that lifesaving operational decisions can be made reliably. MobileIron Inc. is currently funded by DHS S&T for this technology.

N5 Sensors, Inc.

Compact Multi-Gas and Particulate Matter Detector

A compact, low-cost gas and particulate detector leveraging N5's patented chip-scale nanoengineered gas sensor technology. It provides real-time detection of multiple of toxic and fire gases along with particulate matter counts in a wide range of environmental conditions. N5 Sensors, Inc. was funded by DHS S&T under the Small Business Innovation Research program for this technology.

National Aeronautics and Space Administration (NASA) Jet Propulsion Laboratory

WAMS – Wearable Alert and Monitoring Systems

WAMS provides front-end processing for the Assistant for Understanding Data through Reasoning, Extraction and Synthesis (AUDREY), enabling AUDREY agents to efficiently receive personalized sensor data, alerts and events and supporting voice-to-text conversion. NASA Jet Propulsion Laboratory was funded by DHS S&T for this technology.

SensorUp, Inc.

SensorThings

SensorUp provides the Internet of Things platform for customers who rely on geospatial in their IoT Implementations. SensorUp helps make sense of data, combining all different sensors into one easily-managed visualizer and get the bigger picture. SensorThings technology rapidly aggregates and coordinates disparate sensors and IoT systems transforming them into actionable insights. SensorThings provides the primary sensor integration platform for the OpEx by connecting and aggregating various sensors and providing that actionable information to situational awareness tools. SensorUp, Inc. was funded by DHS S&T through a subcontract for this technology.

Sonim Technologies, Inc.

Sonim XP8 Smartphones

The Sonim XP8 is an ultra-rugged smartphone built to provide those who serve with the smart communication they need when and where they need it most. The Sonim XP8 offers dedicated OneTouch Push-To-Talk for quick emergency communication, plus the ability to power remote speaker microphones without additional batteries.

TRX Systems, Inc.

NEON® Personnel Tracker and NEON® Command

NEON Personnel Tracker delivers ubiquitous location indoors and out, improving operational efficiency, command effectiveness and safety for security, public safety and industrial applications. NEON Personnel Tracker is an Android application tightly integrated with the NEON Location Service where a suite of patented algorithms fuse inertial sensor data. NEON Command is a PC based visualizer used to view location data remotely in real-time. TRX Systems, Inc. was previously funded by DHS S&T for indoor tracking solutions under the Firefighter Accountability and Proximity Systems project.

OpEx Constraints and Limitations

DHS S&T identified the following constraints and limitations for the OpEx:

- Most of the technology providers were identified through a Request for Information process and worked under Cooperative Research and Development Agreements (CRADAs) with DHS S&T, which did not include funding. This constrained the scope of their participation.
- DHS S&T could not interface with existing Computer Aided Dispatch (CAD) systems for the City of Houston, Port of Houston or Harris County, so the sensor feeds had to be aggregated, normalized and sent to situational awareness applications entirely outside of the local CAD systems.
- The primary situational awareness solutions used—AVERT C2, Intrepid Response and Haystax Constellation—were selected because they were already in use (or planned for use) by Harris County and the Port of Houston.
- A complete integration of the SENSEI solution that would have allowed secure data transfers was not possible due to the performers having only enough time and resources committed to their primary development and integration efforts.

OpEx Communications Architecture

Based upon site visits, a baseline technology assessment of all participating agencies and ongoing collaboration with Harris County and other participants, DHS S&T developed a notional architecture. This established the foundation for the OpEx architecture, as well as ensured consistency with the expectations and needs of participating public safety organizations, as shown in Figure 4.

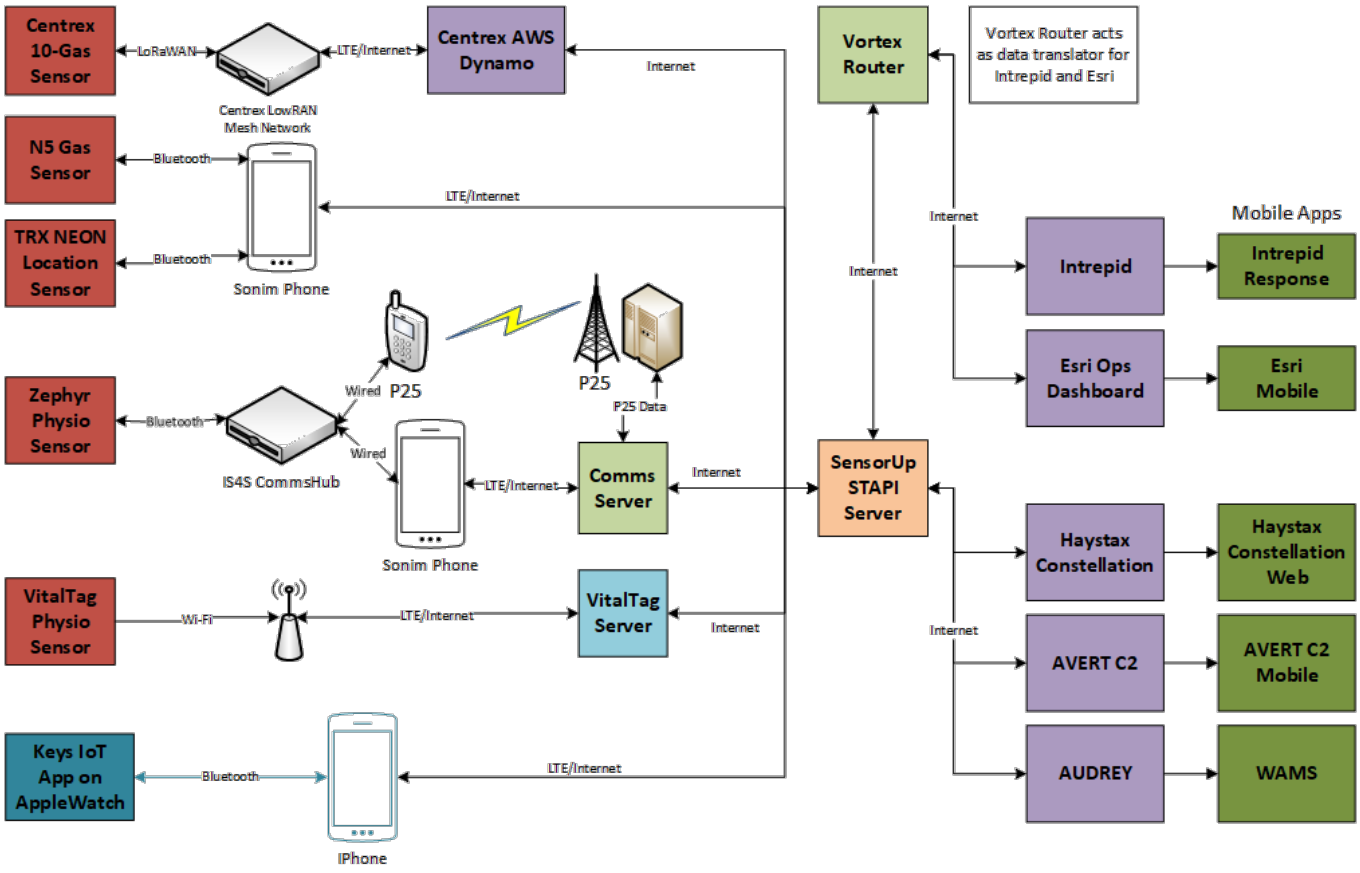

Figure 4. OpEx Communications Architecture with Central SensorUp Data Integration Point

Implementing Mobile Device Management Solutions

It is crucial for public safety agencies to ensure that first responders' mobile devices and their applications (including any data) are managed, monitored and secured so that the responders can perform their jobs effectively, efficiently and safely. Having the ability, for example, to instantaneously and simultaneously push updated apps to all mobile devices or even deactivate a mobile device due to a threat provides first responder agencies greater control and productivity.

Figure 5. The DHS S&T OpEx Team Monitors the AVERT C2 Dashboard During the OpEx

Although MDM in its simplest definition is an industry term that refers to the control of one or more mobile devices through various types of access control and monitoring technologies, its scope is continuously evolving and expanding. The MDM solution used for the NGFR – Harris County OpEx included additional capabilities such as mobile device attestation, user-based metrics testing, end-to-end encryption, data tunneling and vulnerability analysis of mobile apps.

Mobile Device Management Requirements

To effectively develop and implement a first responder MDM solution, DHS S&T and participating public safety agencies assessed their mission needs for the situational awareness systems and arrived at the following requirements:

- Assess mobile apps for software risk to ensure that developers address vulnerabilities prior to deployment;
- Authenticate user identity;
- Secure data end-to-end;
- Develop user profiles for groups of users;
- Assign user profiles to specific users;
- Support shared devices within agencies or "bring-your-own-devices" (BYOD);
- Remotely install, modify or delete applications on mobile devices;
- Remotely shut down mobile devices in the event of loss or compromise; and
- Track mobile usage, health and status.

Baseline Assessment of Existing Capabilities

Participating public safety agencies did not have baseline MDM capabilities. Neither Harris County nor the Port of Houston issued mobile devices to their responders except for a few Special Operations teams and senior leadership, so they had no need to implement MDM. Harris County did have a stock of Sonim XP8 smartphones for issuance during special events but did not have MDM for those devices. NGFR's use of MDM during the OpEx exposed all twelve participating public safety agencies to using mobile devices in everyday emergency response and to the capabilities and benefits of a robust MDM solution.

Mobile Device Management Evaluated During the OpEx

DHS S&T implemented MDM during the OpEx to enable the NGFR team and participating first responders to:

- Assess mobile apps for software risk to ensure that developers address vulnerabilities prior to deployment;
- Develop user profiles for groups of users;
- Assign user profiles to specific users;
- Remotely install, modify or delete applications on mobile devices;
- Remotely shut down mobile devices in the event of loss or compromise; and
- Track mobile usage, health and status.

These requirements were fulfilled with the use of several software packages that were integrated into a system named SENsor Secure Enterprise Infrastructure (SENSEI). This system was jointly developed by Metronome, MobileIron and Kryptowire and funded by DHS S&T. The SENSEI system is composed of the following software packages:

- MobileIron's "MobileIronGo" provided mobile device and application management and configuration;
- Metronome's "eCloak" provided additional mobile device attestation and scheduled, user-based metrics testing; and
- Kryptowire provided vulnerability analysis of mobile apps prior to making them available for installation via the MDM.

Figure 6 details the architecture of the SENSEI system, showing the various communication paths. The gray solid lines with arrows depict back-end communication paths such as between wrapped mobile apps

and back-end systems through the virtual private network (VPN) (MobileIron Sentry). The blue dotted lines with arrows depict communication paths initiated by a user over the internet such as the first responder using a wrapped app on a mobile device. It also depicts the communication path initiated by a system administrator viewing the SENSEI web dashboard, App Vetting (Kryptowire) and MDM Cloud systems.

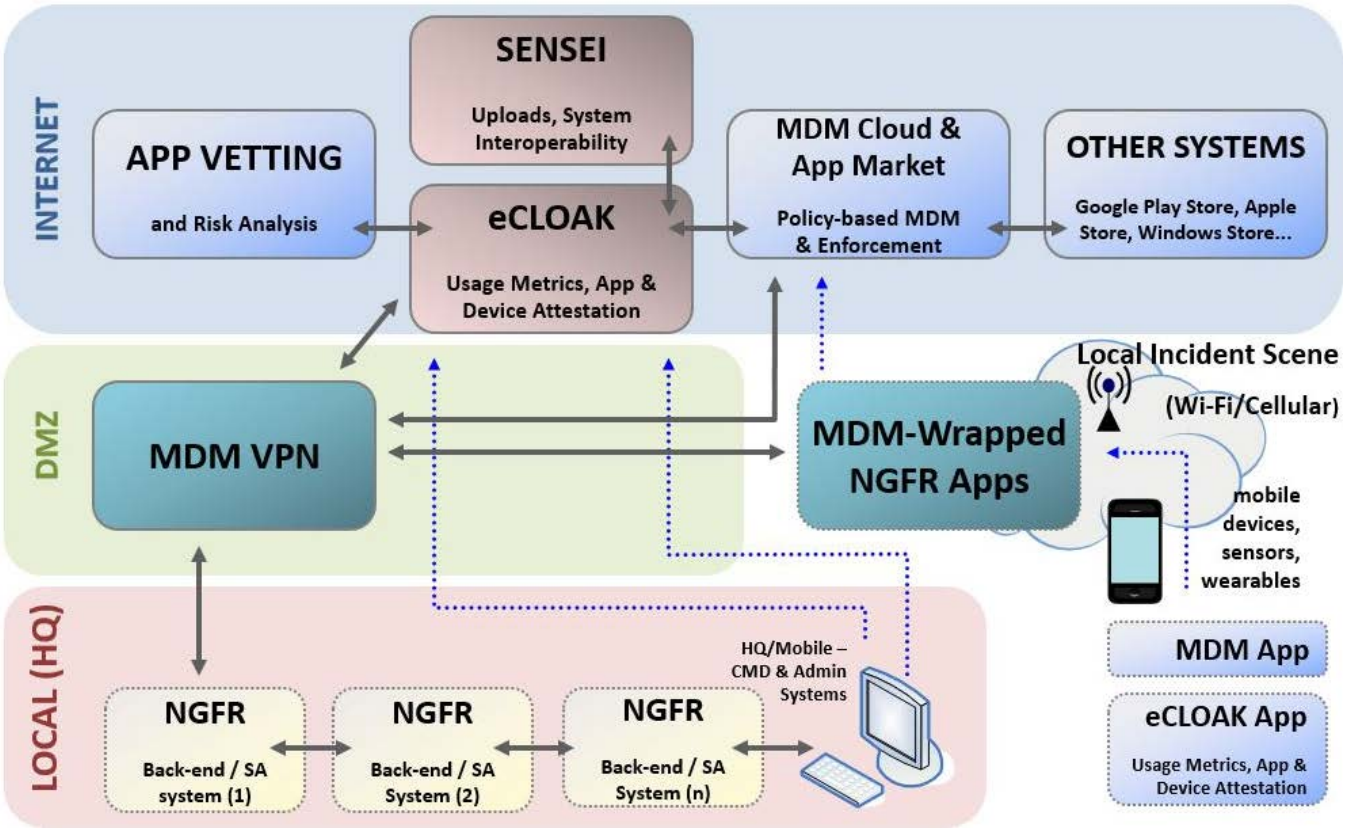

Figure 6. SENSEI Diagram

The comprehensive SENSEI solution was presented and offered to all the OpEx performers as a complete end-to-end solution for ensuring the security, management, identification and disposition of mobile device endpoints. The solution adds enterprise level security capabilities for:

- Managed device and apps;
- Encrypted mobile security;
- App analysis and validation;
- Assured identity; and
- Device and user attestation.

Furthermore, the SENSEI solution protects data at rest (DAR) by wrapping the app where it resides in a secure container whose data is encrypted and protected from unauthorized access. Conversely, data in transit (DIT) is secured using the MobileIron Sentry (VPN tunneling) between wrapped apps and back-end servers.

However, a fully integrated SENSEI solution was not implemented for the OpEx because the performers only had enough time and resources committed to complete their primary development and integration efforts. Therefore, none of the performers (mobile application providers) submitted their apps to be

wrapped nor did back-end services vendors “front” or position their servers with MobileIron Sentry. The portions of the SENSEI solution that were implemented for the OpEx were:

- Mobile app risk assessment;
- Enrollment and configuration of mobile devices; and
- App distribution.

The mobile app risk assessment required that the performers (mobile application providers) submit their apps to be vetted and analyzed for any vulnerabilities. The SENSEI dashboard shown in Figure 7 shows the list of submitted apps, risk assessment status and the apps that have been enrolled in MDM.

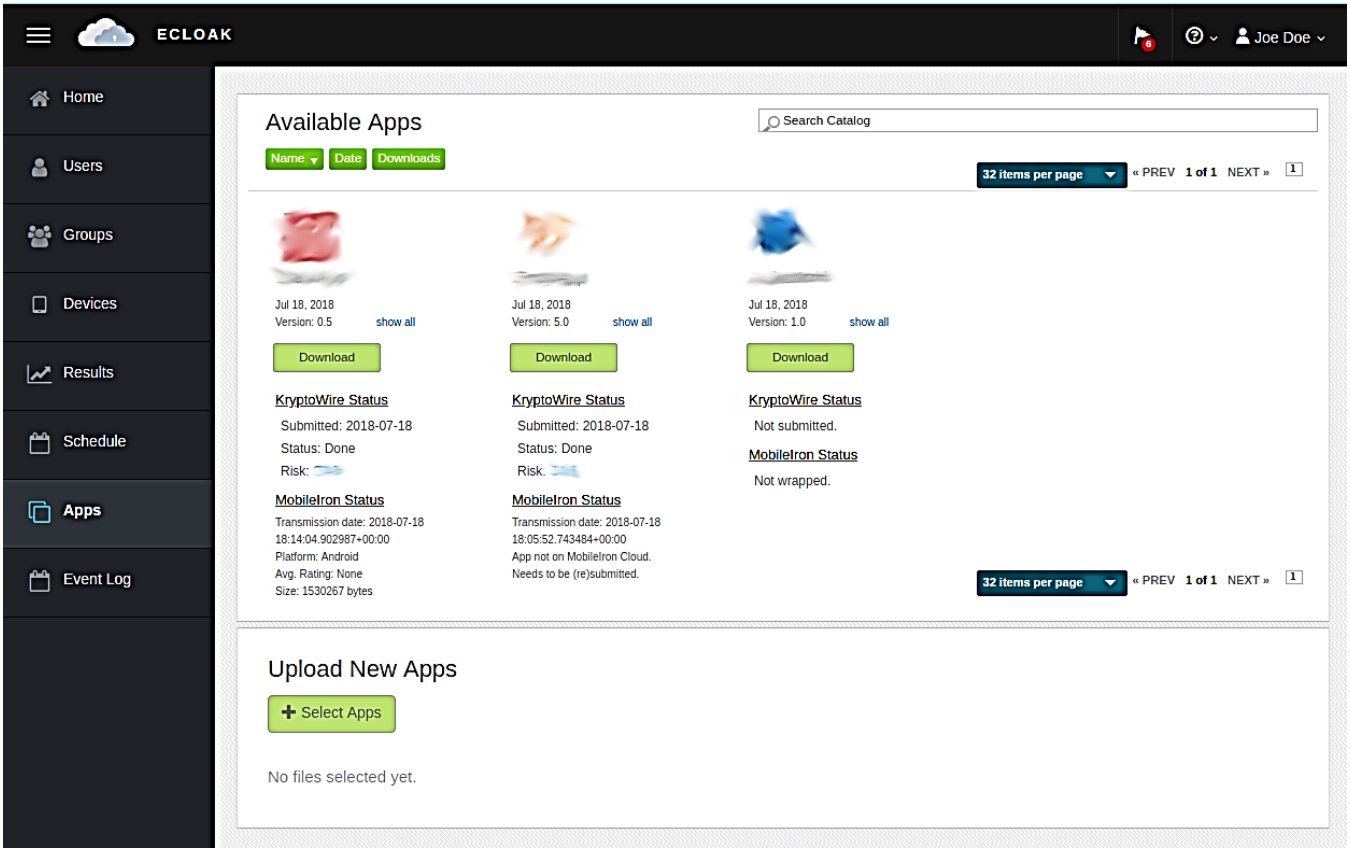

Figure 7. SENSEI Dashboard

Performers that submitted their apps to SENSEI received a confidential security analysis report, which included, but was not limited to, use of proper encryption practices, unnecessary access of sensitive data and malware scans. Figure 8 shows a summary of the risk assessment report.

Figure 8. Risk Assessment Summary Report

Over 60 Sonim XP8's and a dozen Apple iPads were enrolled in MDM and configured for the OpEx. The Android devices were effortlessly enrolled in MDM through the merits of Android Enterprise and QR code provisioning directly after a default factory reset. This led to an automatic installation of the MobileIron Go application where the user was then able to log on to the MobileIron account using his/her login name and password. The end user did not have to enter Google account information as it was previously created by MobileIron during the initial setup of the MDM configuration for the OpEx.

Once the devices were enrolled, the devices were managed using the MobileIron Cloud website. The MobileIron MDM dashboard, as shown in Figure 9, shows the mobile device by OS type, users by invitation state and devices by phone model type. The dashboard view is user defined utilizing widgets based on a dropdown selection of categories and fields such as devices, users, etc.

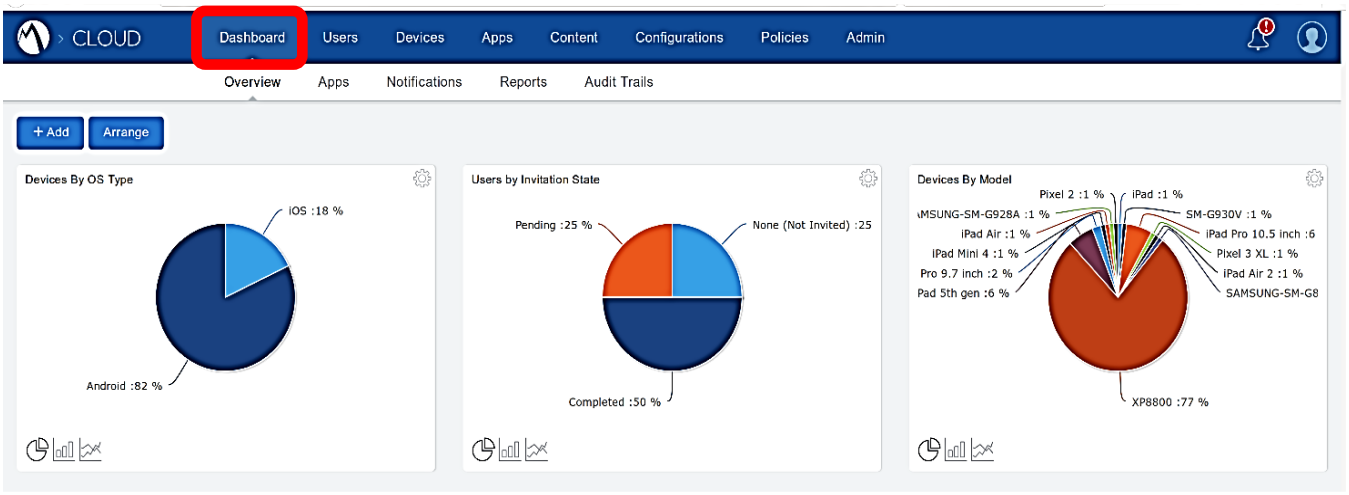

Figure 9. MobileIron MDM Dashboard

The MobileIron MDM Cloud website includes additional webpages to view or manage other features such as the "Devices," "Users," "Apps," "Content," "Policies," etc. Figure 10 shows the screenshot of the MobileIron MDM Cloud "Devices" webpage where, for example, the administrator can manage devices by assigning the device to a user, locking, unlocking, wiping, retiring, etc.

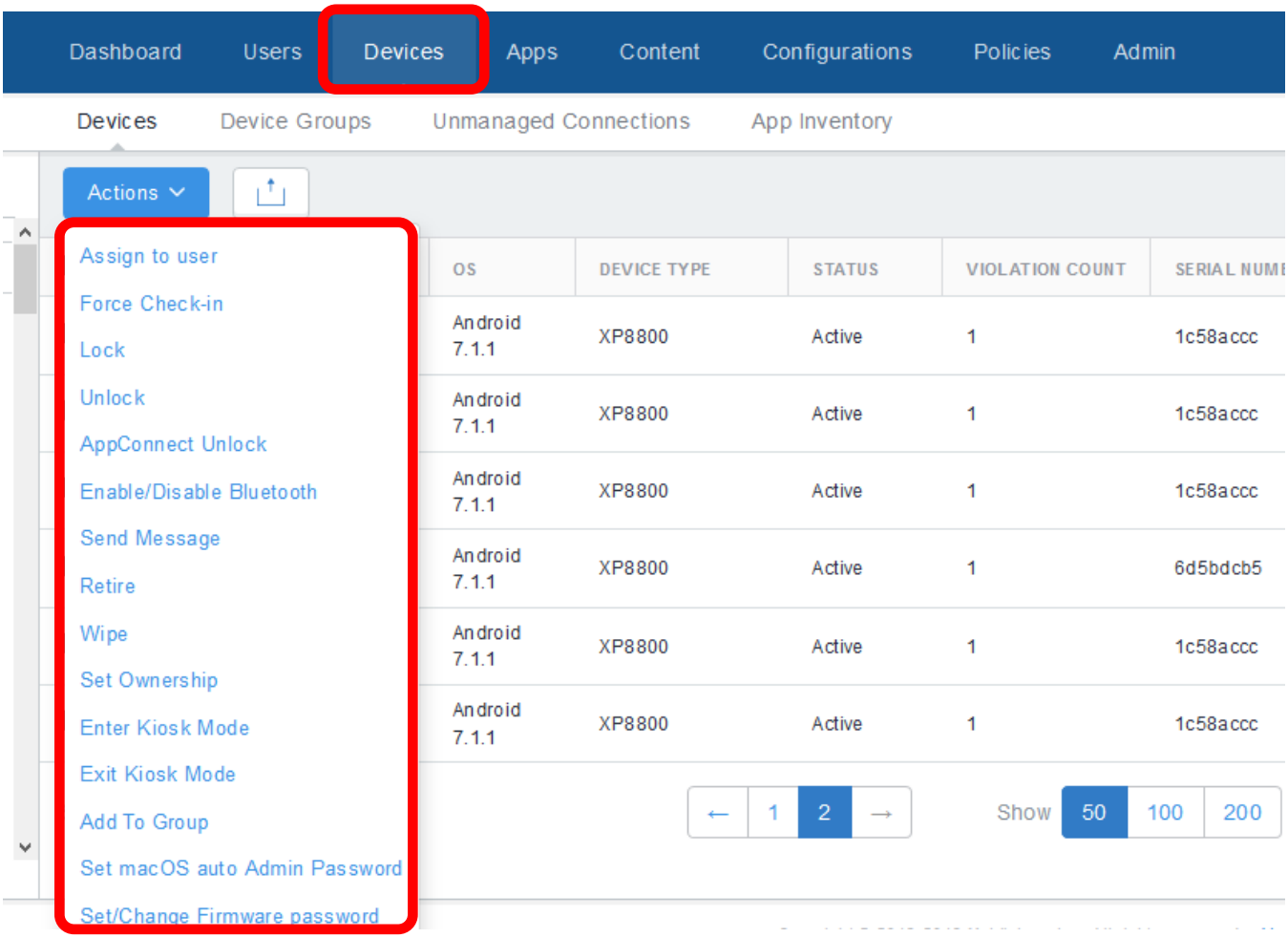

Figure 10. MobileIron MDM Cloud website

The apps selected for the NGFR – Harris County OpEx were pushed out to the mobile devices for automatic installation and were also made available on the MobileIron marketplace. The devices were then configured with all the recommended settings, specific app configurations and login credentials. The selected apps including the native apps such as "Dialer," "Messages," "Settings" and "Camera" were configured to be in "kiosk" mode for the OpEx, shown in Figure 11. This meant no other apps other than the selected apps could be accessed without using a pin code to exit "kiosk" mode. OpEx apps included:

- TRX NEON Personnel Tracker
- Chrome
- Intrepid Response
- Haystax Constellation (or Mobile Indicator)
- WAMS
- N5 OpEx
- Intrepid Connect (Moxtra)
- Dialer

- Messages
- Camera
- Settings

Metronome independently conducted two sets of tests during the OpEx. The first test was to verify that wrapped applications can communicate with back-end systems protected by MDM VPN. The second test was to verify that SENSEI's security capabilities do not affect the transmission of MQTT. MQTT is one of the NGFR proposed solutions for moving data over the application layer protocol as described in the NGFR Integration Handbook.

Metronome conducted the first test using two of their own wrapped apps and sending geolocation data to a protected back-end server. The geolocation capabilities were added to simulate sensor data being sent to situational awareness apps like what was done for the OpEx. The second test involved using a wrapped MQTT-based chat messaging app to communicate with a server running behind MobileIron Sentry (VPN server) to verify SENSEI's security capabilities do not affect MQTT transmission.

Figure 11. MobileIron Kiosk Mode

OpEx RESULTS

The OpEx successfully demonstrated both the advantages of mobile device management solutions and their shortfalls as currently implemented. All of the requirements were fulfilled with the delivered capabilities, but with varying degrees of success. The feedback from participating first responders was overwhelmingly favorable.

The Incident Commander, other command staff and first responders were very pleased to be able to view the location of all participating first responders and sensor data on their smartphones, tablets and monitors. In addition, the Port of Houston and Harris County dispatchers who provided dispatcher services for the event were able to see the location of each first responder and their sensor data across the incident area, which the OpEx data integration work made possible. It was particularly important that they could see data from multiple response agencies and multiple jurisdictions in one place, which met several local requirements identified during the Hurricane Harvey after action review.

All these expanded capabilities were facilitated by the MDM solutions deployed during the OpEx. Specifically, the major benefits of MDM achieved during the Harris County OpEx include:

- Software updates were automatically pushed to the devices or the user was notified of the updates and did not have to manually search for or download apps. This proved valuable when one vendor updated software between scenario vignettes.
- Kiosk mode ensured that only the required and pre-selected applications were available to the participating first responders.
- Kiosk mode prevented users from inadvertently turning off mobile data on the Sonim XP8. DHS S&T observed during the OpEx rehearsal that someone accidentally turned off mobile data on the Sonim XP8 phone and implemented this change in kiosk mode for the main OpEx.
- Simplified the MDM enrollment of Android mobile devices using Android Enterprise and QR code provisioning.

- Wrapped applications communicated with back-end systems protected by MobileIron Sentry (VPN).
- SENSEI's security capabilities do not affect MQTT-based communications.

Additional information can be found in sources listed in the References and Recommended Reading section. A complete NGFR – Harris County OpEx After Action Report is under development and will be posted at www.dhs.gov/NGFR and available upon request from NGFR@hq.dhs.gov.

IMPLEMENTATION FOR YOUR AGENCY

During the NGFR – Harris County OpEx, DHS S&T deployed an integrated suite of IoT devices and situational awareness platforms that enabled public safety decision makers with real-time incident information. How can your agency apply this case study and best practices to improve your capabilities? DHS S&T has developed the following questions to help your agency and/or all of the public safety agencies in your community determine MDM requirements, current capabilities, target capabilities and implementation considerations.

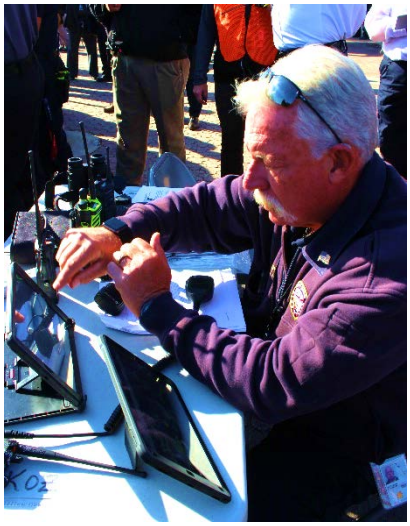

Figure 12. Port of Houston Fire Command Staff Views a Dashboard

One of the most important features of the NGFR – Harris County OpEx was getting the data for responders from different agencies and jurisdictions integrated into a unified situational awareness platform. If your agency regularly responds to multijurisdictional incidents, you would likely benefit from a similar unified multi-agency approach to MDM. Even if different agencies own different brands of equipment, with NGFR integration approaches the data can be shared through common situational awareness platforms. To plan for multijurisdictional interoperability, bring your regular public safety partners to the table when using this guidance to define your approach to MDM and a full suite of situational awareness solutions.

Due to the significant differences between agencies and their capabilities around the country, there is not a one-size-fits-all approach for MDM. However, DHS S&T believes that these questions will help guide your agency and partners towards implementing and deploying mobile device management solutions that are right for your community.

Determine Mobile Device Management Requirements

The first step for your agency is to assess your mobile device management requirements. DHS S&T recommends involving a variety of responders at different levels of command in your requirements discussion to ensure all perspectives are considered. Discussion topics include:

- **Who**: Who has mobile devices that need securing and remote management? Frontline first responders? Incident Commander? Other command staff? Public Safety Answering Point (PSAP) and Dispatcher? Think through all stages of an emergency from 9-1-1 call through conclusion and think about who is using mobile devices throughout the incident.
- **What**: What types of mobile devices require MDM? Do all your agency's mobile devices require MDM, or only some? Would your agency consider bring-your-own-device (BYOD)? What are the devices connecting to internally? What specific apps are needed for specific tasks or to access specific sensors?

- **Where**: Where are MDM solutions needed? Will it be deployed to devices at the edge (incident scene) or mostly used by command at a PSAP or station house? Will the capabilities be easily deployable for significant multijurisdictional incidents or mutual aid situations?
- **When**: Does your agency need MDM on a full-time or part-time basis? Is it a surge capability for major incidents, used to manage everyday incidents, or both? Is a phased approach suitable?

Identify Current Mobile Device Management Capabilities

The second step is for your agency to determine your current capabilities for mobile device management. Discussion topics include:

- Does your agency currently have an MDM solution, or any of the pieces that would make up an MDM solution (e.g., VPNs, remote device management)?
- What mobile devices does your agency currently have? Are they all on the same operating systems or on multiple operating systems? Does your agency currently permit BYOD?
- How are your mobile devices currently managed and updated?
- Does your agency have the necessary staff and resources to manage MDM, or would you need to either hire additional staff or contract out the effort?
- Given your current capabilities, which of your previously-identified requirements remain unmet?

Identify Mobile Device Management Solutions

Once your agency has determined your MDM requirements and current capabilities, you need to identify which solutions can fulfill those gaps. Your agency should follow internal guidance to evaluate the costs of and functionality provided by each solution to determine which one(s) to select.

First, determine whether your agency will use agency-provided or BYOD based on your requirements:

- If BYOD, will the MDM solution take complete control of the BYOD mobile devices, or have some variety of shared control (i.e., user can add certain apps but not delete agency apps)?
- Does your agency have an inventory system to manage other assets (e.g., laptops, tablets, phones)? If so, do you plan to integrate managed mobile device records into a common database using inventory exports or reports?
- Does your agency have existing authentication/identity servers such as Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory with which the MDM would need to interoperate?

Your agency then needs to prioritize which MDM features to include in a new solution, considering:

- Remote application management
- Kiosk mode or equivalent
- Software application risk analysis
- Virtual private network (VPN)
- End-to-end encryption
- Remote device management
- Device and user attestation
- Device and application health monitoring
- Email and content management

Finally, your agency needs to consider the technical requirements of implementing an MDM solution, including discussing:

- Technical capabilities of agency-provided or bring-your-own-device smartphones, tablets and computers (ruggedization, storage, network access, data plans, processing power).
- Technical capabilities of internet access in the field, including bandwidth for MDM updates.
- Technical support staff for set-up, device management and troubleshooting.

Implement Solutions

Once your agency has selected the mobile devices and mobile device management solutions, you should develop an implementation plan for the system(s). The plan would include processes for:

- Procurement of the software and hardware;
- Installation of the components;
- Configuration of the devices and associated applications;
- Training support personnel on the maintenance of the devices and applications; and
- Training the first responders on using the systems.

After implementing and testing sensor integration, your agency will be able to manage mobile devices remotely with the assurance that the data is secure both at rest and in transit.

SUMMARY

This NGFR case study provided an overview of the NGFR – Harris County OpEx, with a focus on the implementation of mobile device management to augment mission response through information sharing and common operating pictures. It also provided a discussion guide that may help your agency determine requirements, current capabilities, target capabilities and implementation considerations for MDM solutions.

If your agency finds this NGFR case study useful for improving your mobile device management and solution implementation, DHS S&T would greatly appreciate your feedback. Please contact the NGFR team with stories from the field, questions or comments by emailing NGFR@hq.dhs.gov.

Figure 13. OpEx Director Sridhar Kowdley Describes How OpEx Technologies are Deployed

REFERENCES & RECOMMENDED READING

Next Generation First Responder Apex Program (https://dhs.gov/ngfr)

This website provides NGFR Apex program descriptions, updates and knowledge products.

NGFR Integration Handbook (https://dhs.gov//science-and-technology/ngfr/handbook)

This three-part document provides technology developers with a standards-based architecture for developing and integrating interoperable first responder technologies.

NGFR – Harris County OpEx Playbook, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document is the guide that was used to execute the NGFR – Harris County OpEx.

NGFR – Harris County OpEx After Action Report, expected March 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document thoroughly describes the planning, execution and results of the NGFR – Harris County OpEx.

NGFR Case Study: Data Integration, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document describes sensor data integration during NGFR – Harris County OpEx.

NGFR Case Study: Enhanced Situational Awareness, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document describes situational awareness applications during NGFR – Harris County OpEx.

NGFR Case Study: Patient Monitoring, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document describes patient monitoring applications during NGFR – Harris County OpEx.

NGFR Case Study: Sensor and Event Alerts, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document describes standard formats for sensor and event alerts during NGFR – Harris County OpEx.

NGFR Case Study: Sensors, expected February 2020 (will be posted on the DHS NGFR website and available upon request from NGFR@hq.dhs.gov)

This document describes various sensors used during NGFR – Harris County OpEx.