Federal Mobility: A Year in Review

Link: https://www.dhs.gov/csd-mobile
Link: https://www.dhs.gov/publication/csd-mobile-device-security-study

Homeland Security
Science and Technology

Vincent Sritapan

Cyber Security Division
Science and Technology Directorate

DHS Report to Congress May'17

Consolidated Appropriations Act, 2016, Division N— Cybersecurity Act of 2015

Title IV, Section 401, Study on Mobile Device Security*

Subsection (a)

(1) Directs the DHS Secretary, in consultation with NIST, to complete a **study on threats relating to the security of the mobile devices** of the federal government

(2) Requires submission of an unclassified **report** (with a classified annex if needed) to Congress **within one year of the Act's passage**

Subsection (b)*

(1) Evolution of mobile security techniques from a desktop-centric approach, and adequacy of these techniques to meet current mobile security challenges

(2) Effect such threats may have **on the cybersecurity of the information systems and networks of the federal government**

(3) Recommendations for addressing the threats **based on industry standards and best practices**

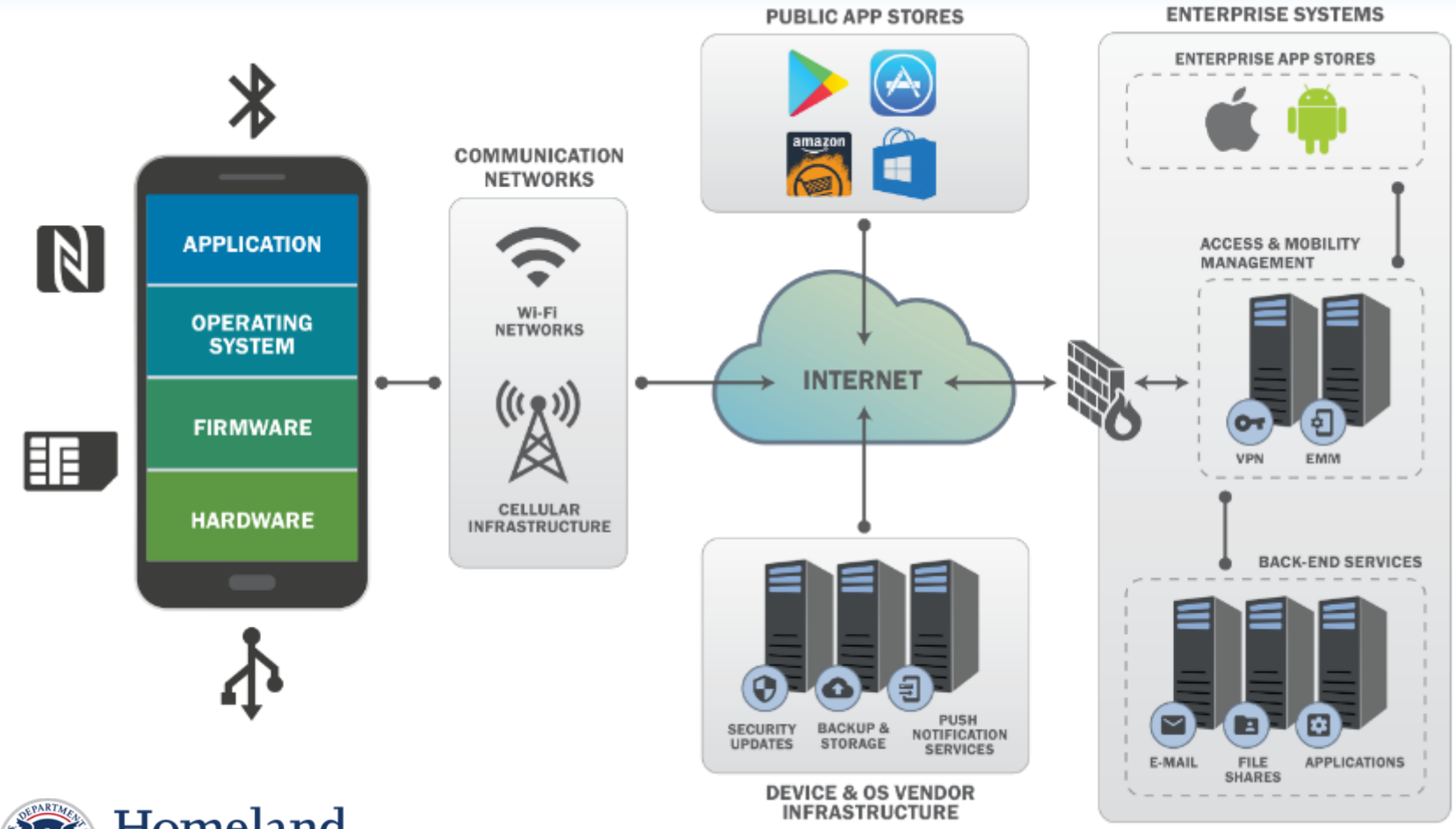
(4) Deficiencies in the current authorities of the Secretary that may inhibit the ability of the Secretary to address mobile device security throughout the federal government

(5) Plan for accelerated adoption of secure mobile device technology by DHS

Homeland Security
Science and Technology

**Excludes National Security Systems and DoD and IC systems and networks*

Mobile Ecosystem



Homeland Security
Science and Technology

Mobile Security Threats by Category

Mobile Device Technology Stack	▪ Compromised Cloud System Credentials ▪ Delays in Security Updates ▪ Deliberate Bootloader Exploitation ▪ Exploitation of OS or Baseband Vulnerabilities ▪ Jailbreak/Rooting ▪ Supply Chain Compromise ▪ TEE/Secure Enclave Exploitation
Mobile Networks	▪ Data/Voice Eavesdropping ▪ Data/Voice Manipulation ▪ Denial of Service/Jamming ▪ Device and Identity Tracking ▪ Interference with 911 Calls ▪ Rogue Base Stations & Wi-Fi Access Points
Device Physical Access	▪ Attacks on Enterprise PCs ▪ Device Loss or Theft ▪ Malicious Charging Station ▪ Physical Tampering
Mobile Applications	▪ Exploit Public Mobile App Store ▪ Exploitation of Vulnerable App ▪ Insecure App Development Practices ▪ Malicious and/or Privacy-Invasive Practices ▪ Malware, Ransomware ▪ Vulnerable Third-Party Libraries
Mobile Enterprise	▪ Bypass App Vetting ▪ Compromised EMM/MDM System or Admin Credentials ▪ Compromised Enterprise Mobile App Store or Developer Credentials ▪ EMM/MDM System Impersonation ▪ Man-in-the-Middle Attacks on Devices

Best Practices and Standards

Enterprise Mobility Program	• Mobile Computing Decision Framework (MTTT) • Federal Mobile Computing Security Baseline (DHS, DoD, NIST) • Mobile Security Reference Architecture (DHS, DoD, NIST) • NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure Draft (NIST) • Security Guidance for Critical Areas of Mobile Computing (Cloud Security Alliance) • Privacy Policy for DHS Mobile Apps (DHS)
Mobile Device Technology Stack	• NIST SP 800-164 (Draft): Guidelines on Hardware-Rooted Security in Mobile Devices (NIST) • NIST SP 800-88r 1: Guidelines for Media Sanitization (NIST) • NISTIR 7981 Mobile, PIV, and Authentication (NIST) • NIST SP 800-121r1 Guide to Bluetooth Security (NIST) • Mobile Device Security a Comparison of Platforms (Gartner) • NIAP Protection Profile for Mobile Device Fundamentals 3.0 (NIAP) • Specification for Trusted Execution Environment/Specification for Secure Element Management (Global Platform) • Specifications for Trusted Platform Module (Trusted Computing Group)
Mobile Enterprise	• NIST SP 1800-4 Practice Guide: Mobile Device Security (NIST NCCoE) • NIST SP 800-124r1: Guidelines for Managing the Security of Mobile Devices in the Enterprise (NIST) • Commercial Solutions for Classified Mobile Access Capability Package (NIAP) • NIAP Protection Profile for Mobile Device Management Version 2.0 (NIAP) • NIAP Protection Profile - Extended Package for Mobile Device Management Agents 2.0 (NIAP)
Mobile Applications	• NIST SP 800-163: Vetting the Security of Mobile Applications • Adoption of Commercial Mobile Applications within the Federal Government (CIO Council) • NIST SP 1800-1 Practice Guide: Securing Electronic Health Records on Mobile Devices (NIST NCCoE) • NISTIR 8136: (Draft) Mobile Application Vetting Services for Public Safety (NIST) • Mobile Application Single Sign-On for Public Safety and First Responders (NIST NCCoE) • Open Web Application Security Project - Mobile Security Project (OWASP) • Mobile Application Security Testing Initiative (Cloud Security Alliance) • NIAP Protection Profile for Application Software (NIAP)
Mobile Networks	• NIST SP 800-187 Guide to LTE Security • SS7 Interconnect Security Monitoring Guidelines (GSMA)

DHS Next Steps

- To address these areas of concern DHS proposes the following:
  - **FISMA metrics** should be enhanced to focus on securing mobile devices through the Federal CIO Council's Mobile Technology Tiger Team (MTTT). Metrics for consideration include mobile operating systems, mobile device authentication methods, and volume of mobile device user traffic not going through the agency's Trusted Internet Connection.
  - The DHS **CDM program** should address the **security of mobile devices and applications** with capabilities that are at parity with other network devices (e.g., workstations and servers), and NPPD's definition of critical infrastructure should include mobile network infrastructure
  - DHS S&T HSARPA Cyber Security Division should continue its work in **Mobile Application Security** to ensure the secure use of mobile applications for government use.

Next Steps (continued)

- Additional topics that need a response by the federal government:
  - The U.S. government should continue and enhance its active participation in international standards bodies so it can represent America's national interest with the private sector in the development of consensus-based voluntary mobile security standards and best practices.
  - Continued development of the NIST draft *Mobile Threat Catalogue* with additional cooperation from industry and the inclusion of emerging threats and defenses and additional risk metrics for mobile threats.
  - Federal departments and agencies should develop policies and procedures regarding Government use of mobile devices overseas based on threat intelligence and emerging attacker tactics, techniques, and procedures.

Progress Review

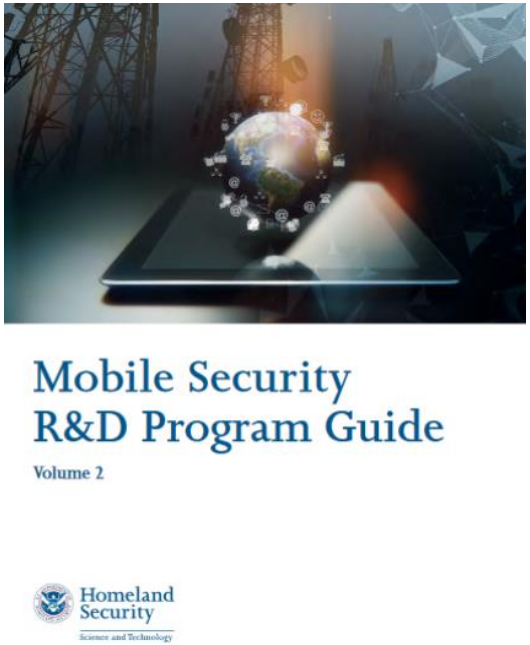
- FISMA FY18 includes Mobile Assets (Completed)
- Mobile for CDM in FY18+ (In Progress)
- govCAR SPIN 5 – Mobile Security Architecture Review (In Progress)
- DHS S&T's Mobile App Security R&D efforts underway since FY17+
- DHS Enterprise Policy Addressing International Travel with Mobile Devices; Other D/A's also addressing this challenge
- Standards and Guidance: NIST SP 800-163 Revision Open Public Comment, NIST 800-124 Revision Coming, NIST 1800-4 add-ons (handbook) FY19+
- More TBD…

Next Steps – Come to Breakout Session

Homeland Security
Science and Technology

Mobile Security R&D Program Areas

- Mobile Device Security
- Mobile Application Security
- Mobile Network Infrastructure



Homeland Security
Science and Technology

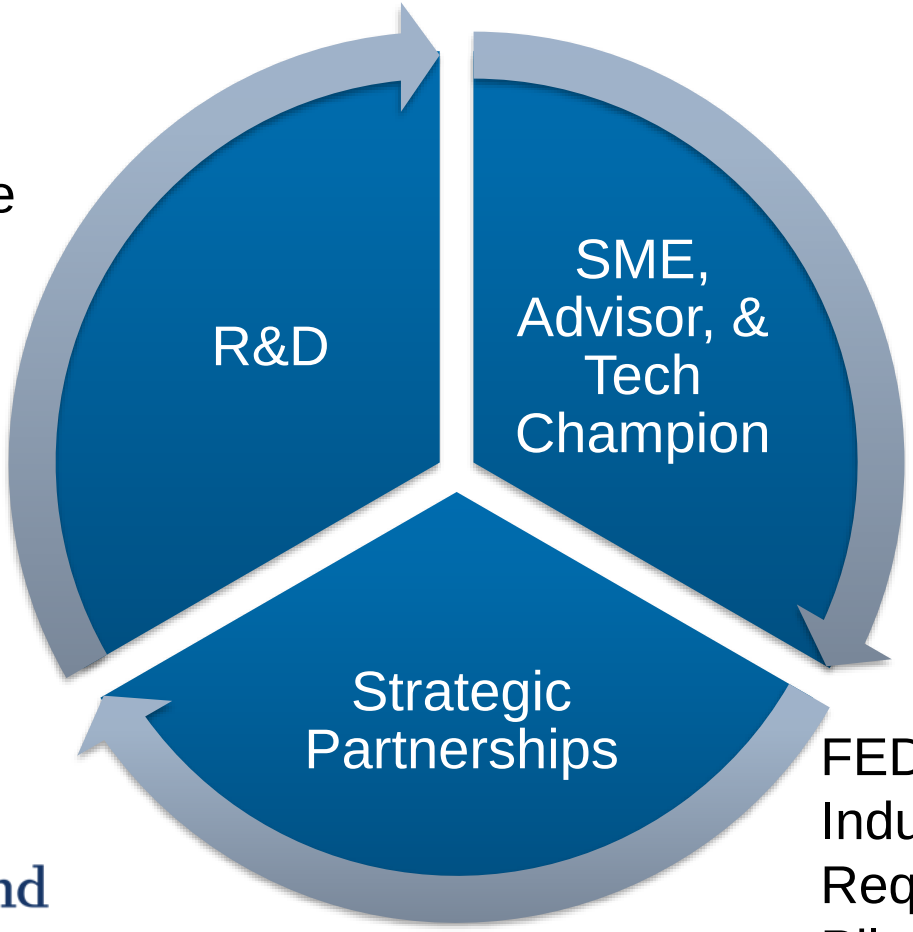
https://www.dhs.gov/publication/mobile-r-d-guide

Mobile Security R&D Approach

"Accelerating the adoption of secure mobile technologies by the Department, the government, and the global community"

Develop innovative secure mobile technologies

LRBAA & BAAs, OTS

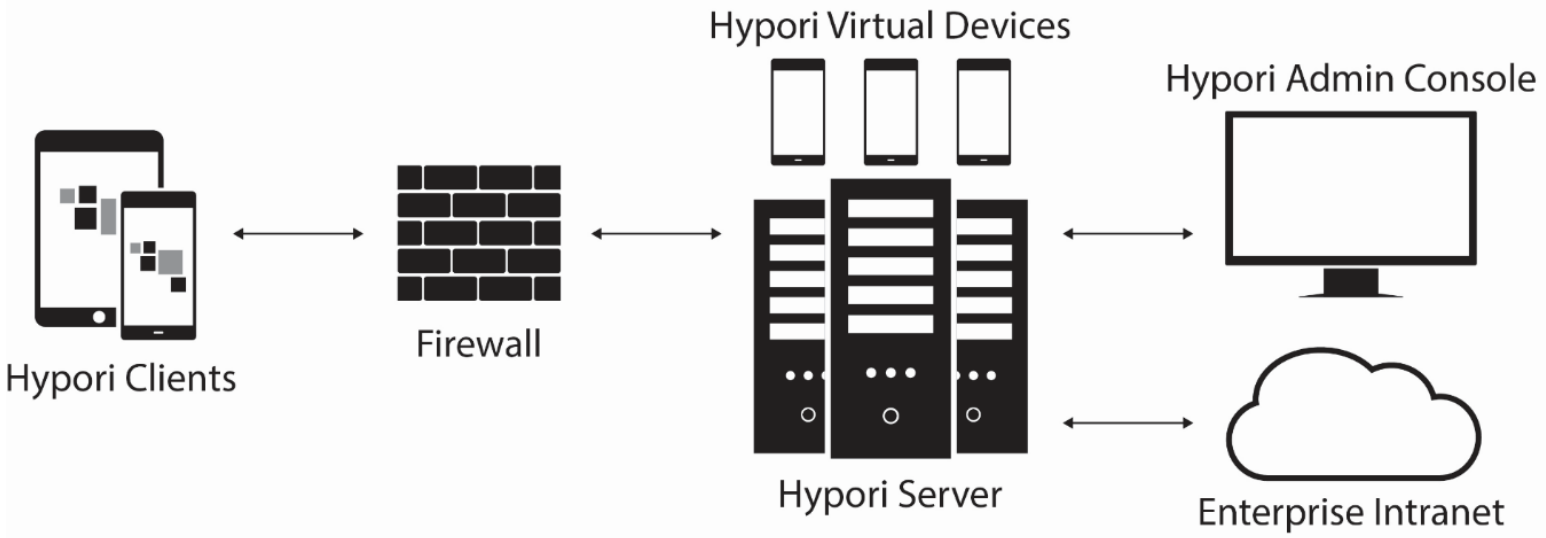


Landscape Awareness
Lead Mobility CoP
Impact Policy
Support Procurement
Outreach

FED CIO Council/MTTT
Industry Associations
Requirements NIST/NIAP
Pilots & Transition Partners

Homeland Security
Science and Technology

Virtual Mobile Infrastructure



by Intelligent Waves

- Bluetooth Management for virtualized device
- PKI authentication
- NIAP Protection Profile – Certified iOS/Android
- Pilots for specific stakeholders (BYOD, Tablets)

Homeland Security
Science and Technology

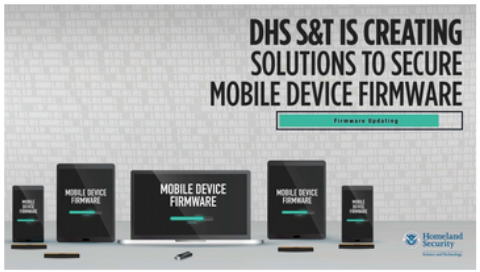
Firmware 'Device' Security

News Release: DHS S&T Announces Four SBIR Awards to Secure Mobile Device Firmware

Release Date: May 30, 2018

For Immediate Release
DHS S&T Press Office, (202) 254-2385

WASHINGTON—Four small technology firms were awarded Small Business Innovation Research (SBIR) contracts by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) to create solutions that will automate analysis of mobile technology firmware at scale and identify vulnerabilities and prepositioned cyber-threats.



The various components of today's mobile technology, including smart phones, wearables and Internet of Things (IoT) devices, are manufactured all over the world, heightening risk for introduction of spyware or other forms of malware in device firmware. As a result, this international supply chain poses vulnerabilities and mobile technology users—government and private sector alike—could be susceptible to a cyberattack from within the supply chain.

Under the SBIR solicitation titled "Automated & Scalable Analysis of Mobile & IoT Device Firmware," each awardee will conduct initial research of their proposal to detect, remediate and protect against software vulnerabilities or unwanted functionality prepositioned within device firmware. These proof-of-concepts must show they can analyze and detect all software vulnerabilities, common vulnerabilities and exposures (CVE), recently discovered zero-day vulnerabilities, and unwanted functionality in firmware binary code. In a phase I effort, each awardee will work over a six-month period of performance to prove the efficacy of its proposed solution.

"Ensuring the mobile device supply chain is free of vulnerabilities and cyber-threats is essential to securing the technology we use to protect the homeland. The techniques and processes being developed will help provide needed insight into the mobile technology supply chain, assuring the ability of Government and enterprises to securely execute their mission," said Emile Monette, program manager of the Office of Cybersecurity and Communications's Cyber Supply Chain Risk Management program at the National Protection and Programs Directorate.

"The benefits of automated analysis of firmware binaries are higher assurance for the integrity of mobile technology as it is used and maintained. Also, original equipment manufacturers and enterprises will be able to check the security and privacy of firmware before and after it is deployed," added S&T Mobile Security Research and Development (R&D) Program Manager Vincent Sritapan, who will oversee these research efforts. "Each performer has presented an innovative approach that bears considerable promise in combatting compromised device firmware."

Homeland Security
Science and Technology

https://www.dhs.gov/science-and-technology/news/2018/05/30/news-release-st-announces-four-sbir-awards-secure-mobile

Mobile Threat Defense Research

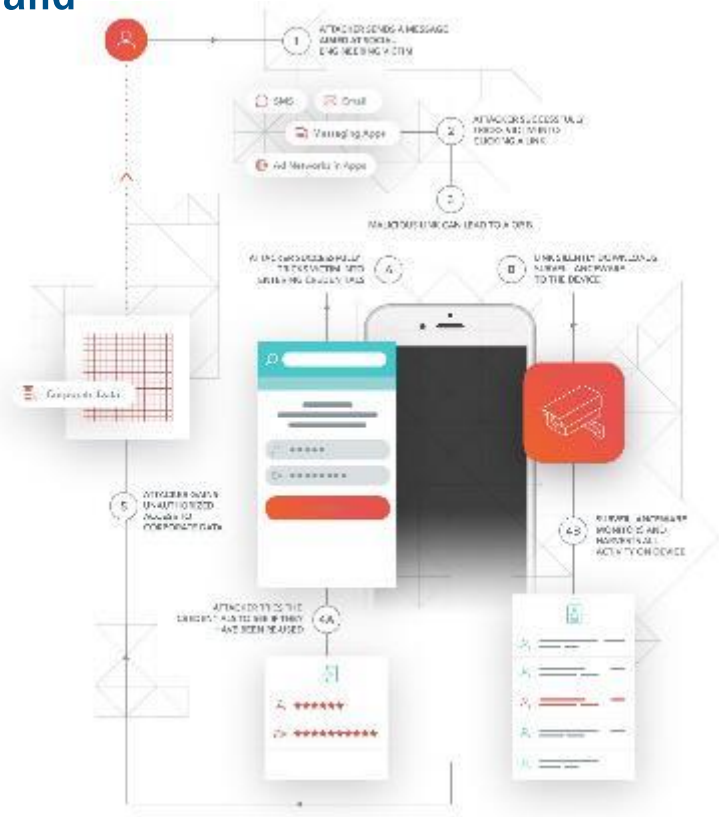
June 2018 Commercialization of Mobile Phishing Protection

Purpose: Address Government needs in Mobile Device and Application Security

Enhancements to Lookout's existing Mobile Endpoint Security Solution

Key Integrations to enable Enterprise Security

- Integration with Enterprise Mobility Management
- User Awareness
- Use of Cloud Based Mobile Threat Intelligence



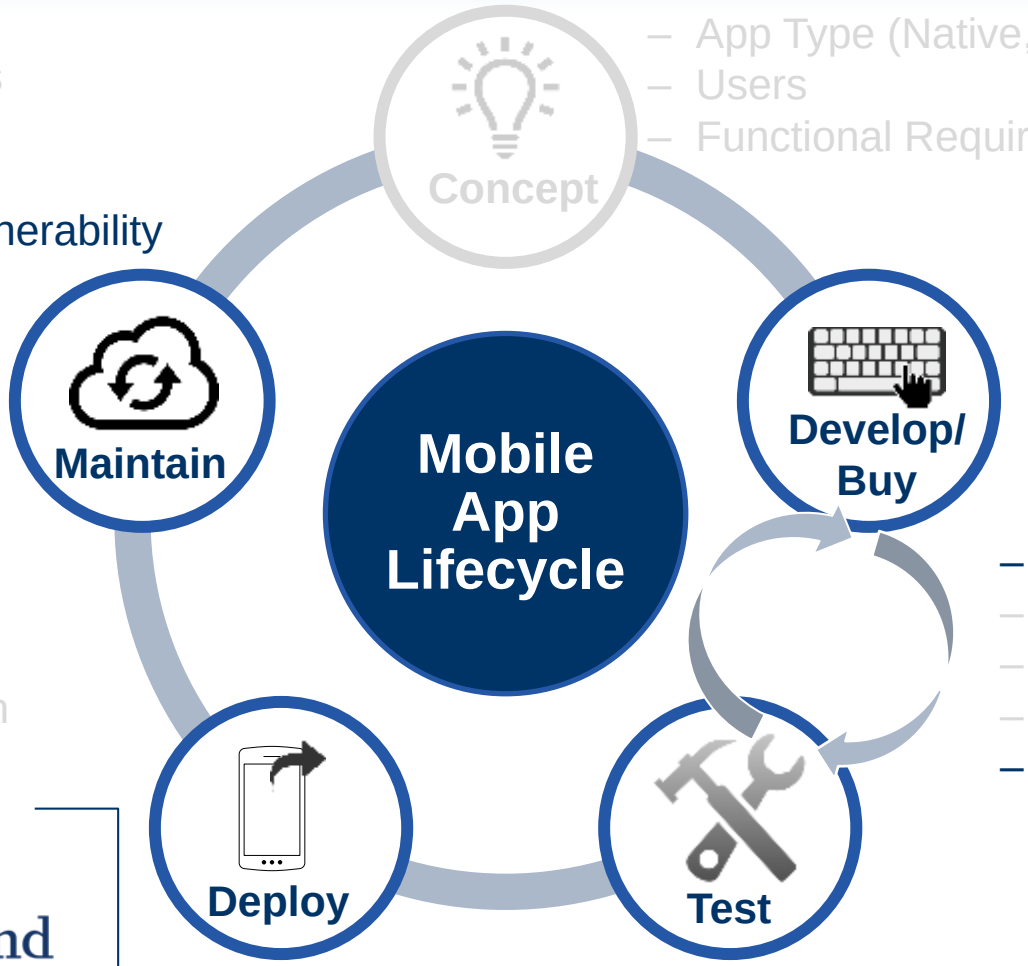
Homeland Security

Science and Technology

Mobile App Security R&D TTA II

Security in Mobile App Development

- Mobile OS Platform
- App Type (Native, HTML)
- Users
- Functional Requirements



- App Updates
- App Security Monitoring
- Threat & Vulnerability Monitoring & Remediation

- App Dev Platform
- Data Requirements
- Authentication
- Usage Environment
- Iterative Testing

- App Vetting
- Authorization Decision
- App Store Deployment

Homeland Security
Science and Technology

Secure Mobile App Development

- APCERTO with Kony
  - Security Platform Integration
  - Documentation
  - Integration with EMM/App Vetting Tools
  - Pilot & partnership opportunities
- Red Hat with Kryptowire
  - Security Templates
  - Integration with App Vetting
  - Documentation
  - Pilot & partnership opportunities
- Progeny with Xamarin
  - Secure Libraries
  - Documentation
  - Toolkit/IDE Integration
  - Pilot & partnership opportunities

Homeland Security
Science and Technology

FY19 and Beyond

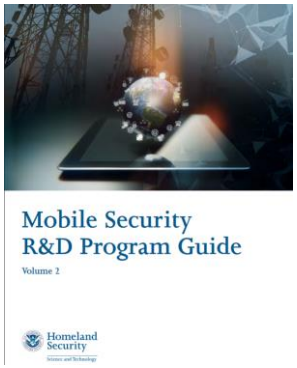
- Security & Resiliency of Mobile Network Infrastructure
  - 5G Security R&D/Impact to Government & Critical Communications
  - Enterprise Visibility and Management of Mobile Network Traffic
  - Mitigations for Legacy Protocol Vulnerabilities/Threats (SS7/Diameter)

Contact Info

Vincent Sritapan
DHS Science & Technology Directorate
Vincent.Sritapan@hq.dhs.gov
dhs.gov/csd-mobile

Delivered to Congress May 2017

Published April 2018



Homeland Security
Science and Technology

Follow us at dhsscitech

Homeland Security

Science and Technology

Homeland Security
Science and Technology

FISMA inclusion of Mobile Assets

	GFE	Non-GFE (e.g. Bring Your Own Device (BYOD) Assets)
Number of mobile devices.	Metric 1.3.1.	Metric 1.3.2.
Number of mobile assets operating under enterprise-level mobile device management that includes, at a minimum, agency defined user authentication requirements on mobile devices and the ability to remotely wipe and/or remove agency data from the devices.	Metric 1.3.3.	Metric 1.3.4.

Mobile Devices			
Windows Mobile (all versions)			
Apple iOS (all versions)			
Android OS (all versions)			
Blackberry OS (all versions)			

Homeland Security
Science and Technology

Primary Mobile Threat Types

Threat	Definition	Examples
Denial of Service	Deny or degrade service to users	Jamming of wireless communications, overloading networks with bogus traffic, ransomware, theft of mobile device or mobile services.
Geolocation	Unauthorized physical tracking of user	Passively or actively obtaining accurate three-dimensional coordinates of target, possibly including speed and direction.
Information Disclosure	Unauthorized access to information or services	Interception of data in transit; leakage or exfiltration of user, app, or enterprise data; tracking of user location; eavesdropping on voice or data communications; surreptitiously activating the phone's microphone or camera to spy on the user.
Spoofing	Impersonating something or someone	Email or SMS message pretending to be from boss or colleague (social engineering), fraudulent Wi-Fi access point or cellular base station mimicking a legitimate one.
Tampering	Modifying data, software, firmware, or hardware without authorization	Modifying data in transit, inserting tampered hardware or software into supply chain, repackaging legitimate app with malware, modifying network or device configuration (e.g., jailbreaking or rooting a phone).