Mobile Security R&D

Mobile Security
R&D Program Guide
Volume 1

Homeland
Security

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

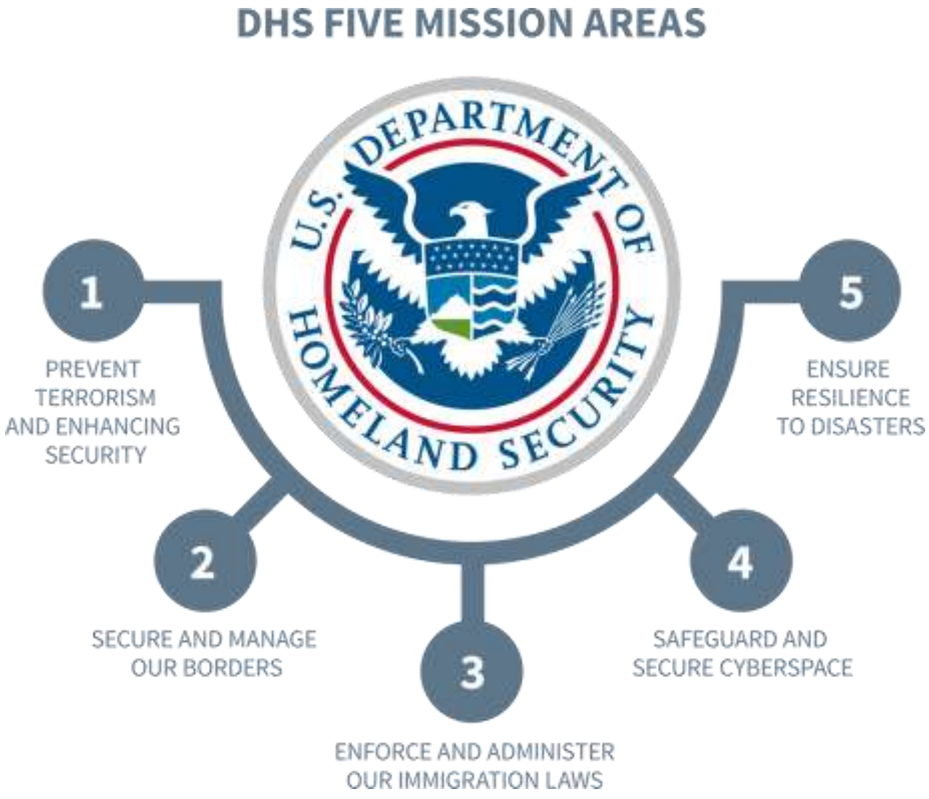
Homeland
Security
Science and Technology

Douglas Maughan

Science and Technology Directorate

S&T MISSION

To deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise.



DHS FIVE MISSION AREAS

1 PREVENT TERRORISM AND ENHANCING SECURITY

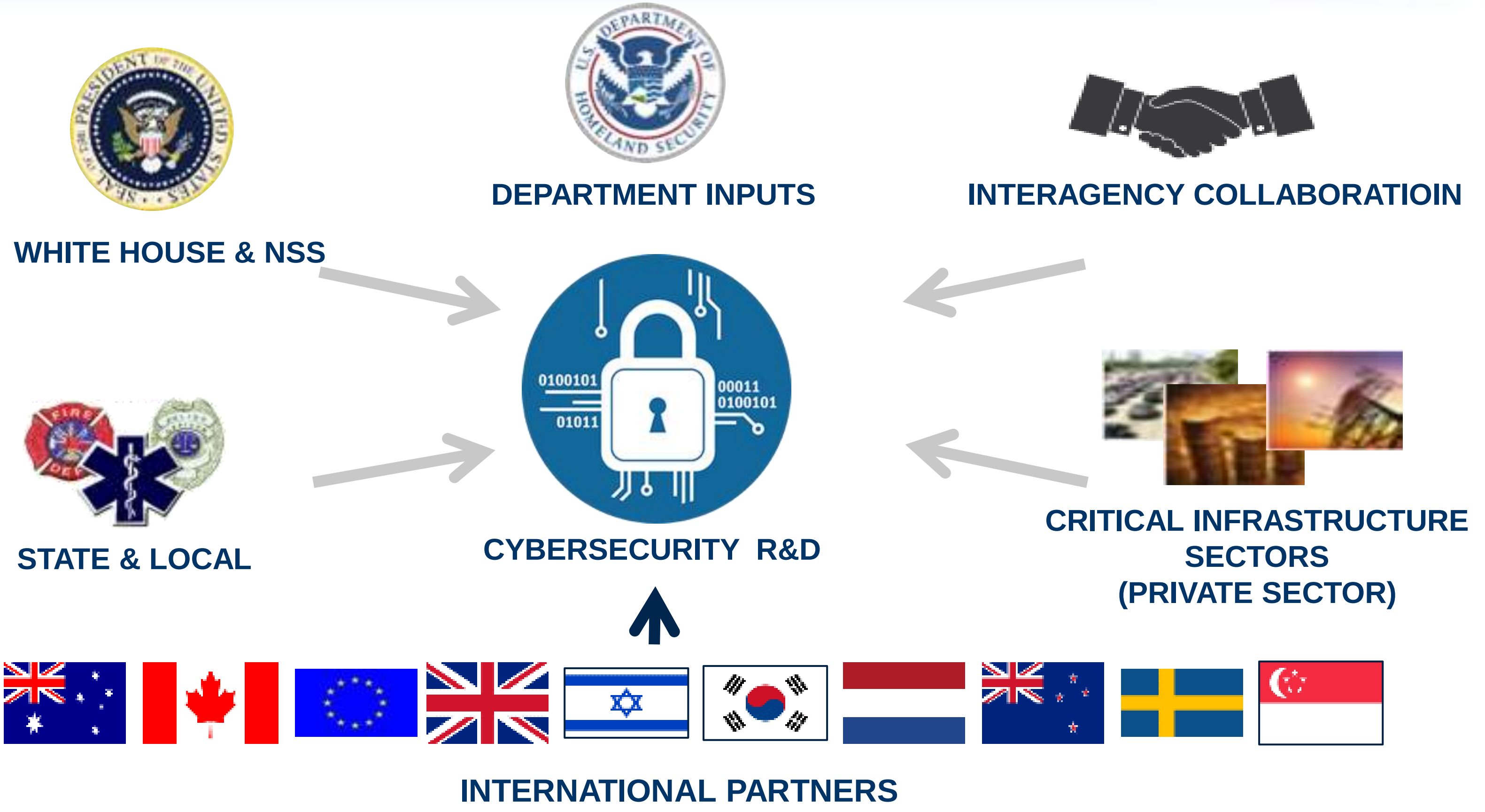
2 SECURE AND MANAGE OUR BORDERS

3 ENFORCE AND ADMINISTER OUR IMMIGRATION LAWS

4 SAFEGUARD AND SECURE CYBERSPACE

5 ENSURE RESILIENCE TO DISASTERS

Background: Research Requirement Inputs



WHITE HOUSE & NSS

DEPARTMENT INPUTS

INTERAGENCY COLLABORATIOIN

STATE & LOCAL

CYBERSECURITY R&D

CRITICAL INFRASTRUCTURE SECTORS (PRIVATE SECTOR)

INTERNATIONAL PARTNERS

Homeland Security

Science and Technology

Security of Mobile Computing

- Published "Study on Mobile Device Security"

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

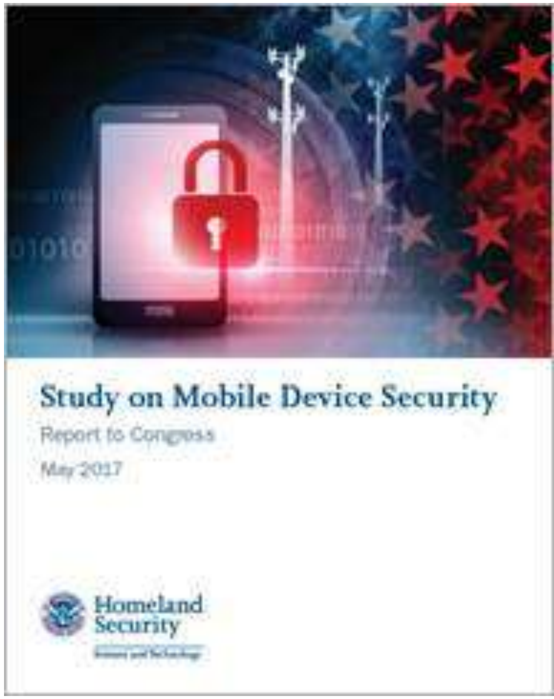
(2) **Effect** such threats may have **on the cybersecurity of the information systems and networks of the federal government**

(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

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



Study on Mobile Device Security

Report to Congress

May 2017

Homeland Security

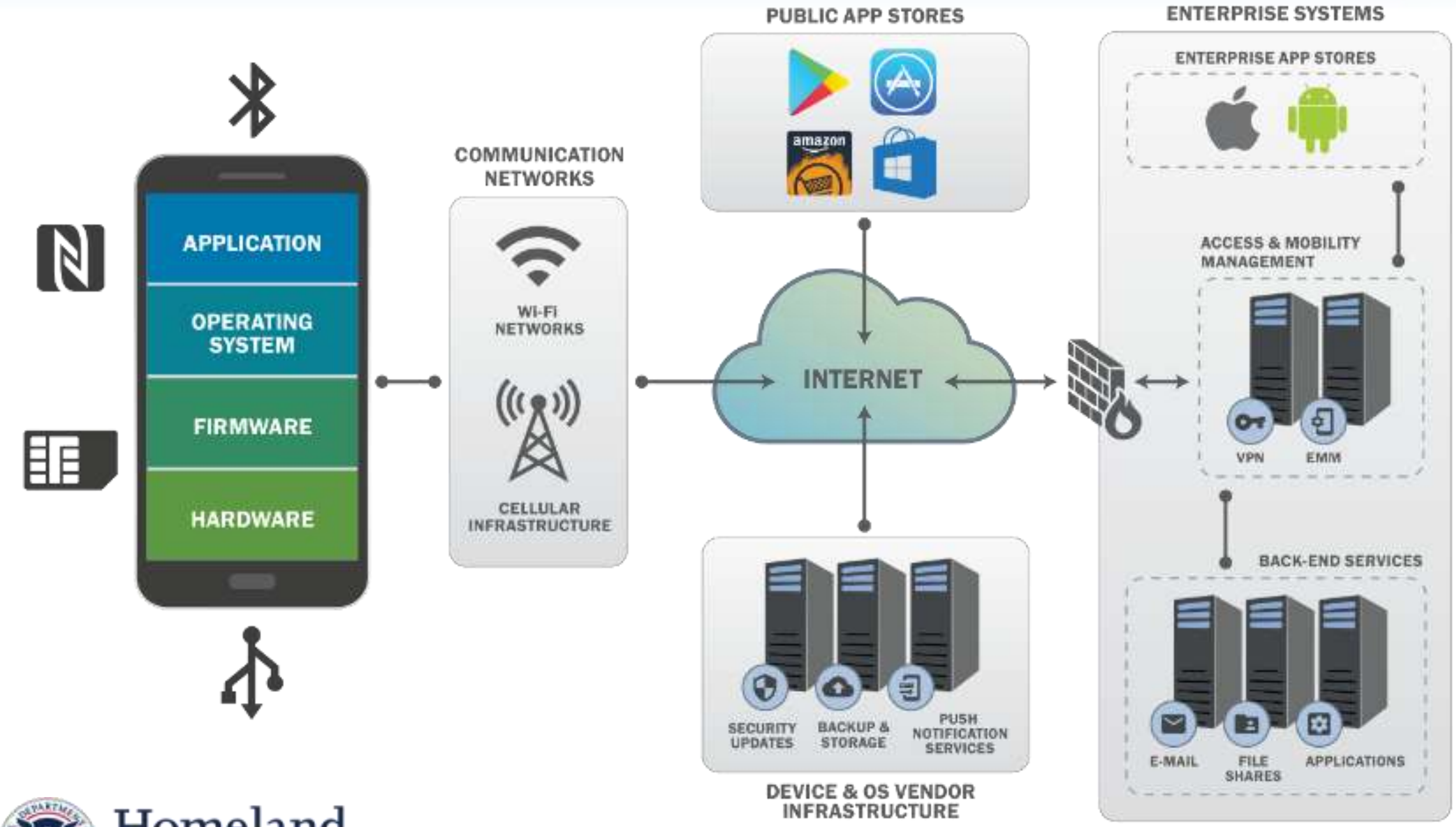
Science and Technology

Homeland Security

Science and Technology

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

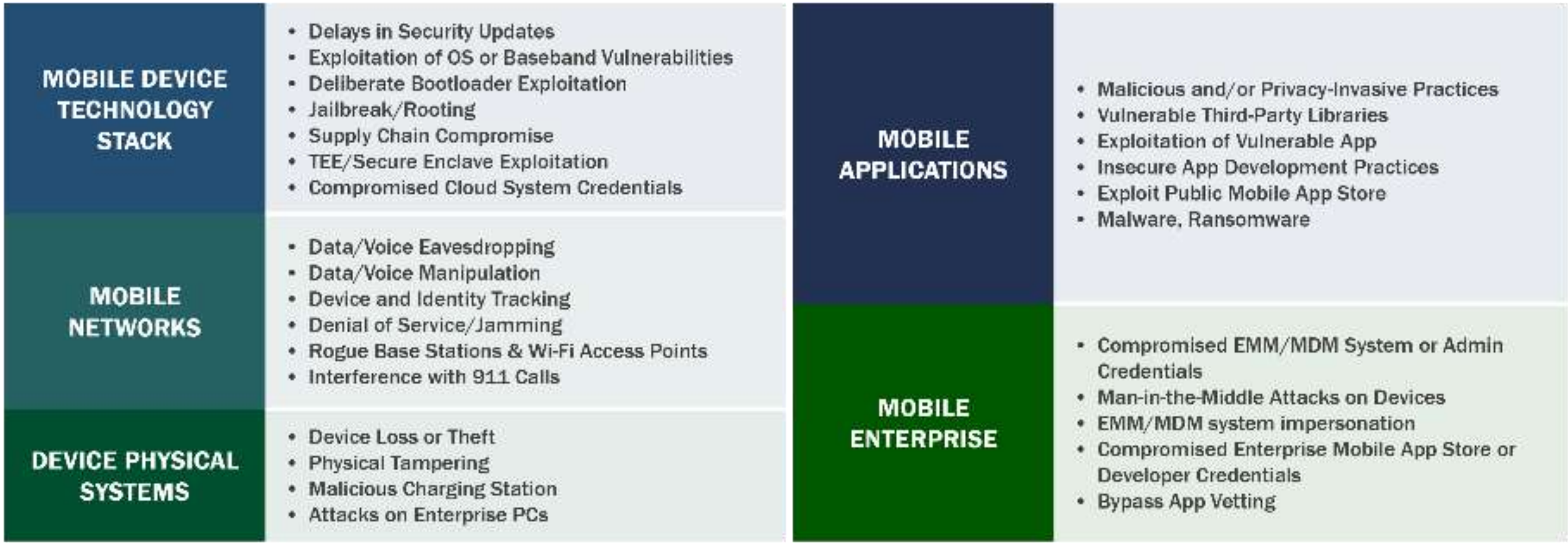
Mobile Ecosystem



Homeland Security

Science and Technology

Mobile Security Threats by Category



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

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).

DHS Next Steps

- To address these areas of concern DHS has proposed 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 will continue its work in **Mobile Application Security** to ensure the secure use of mobile applications for government use.

Next Steps (continued)

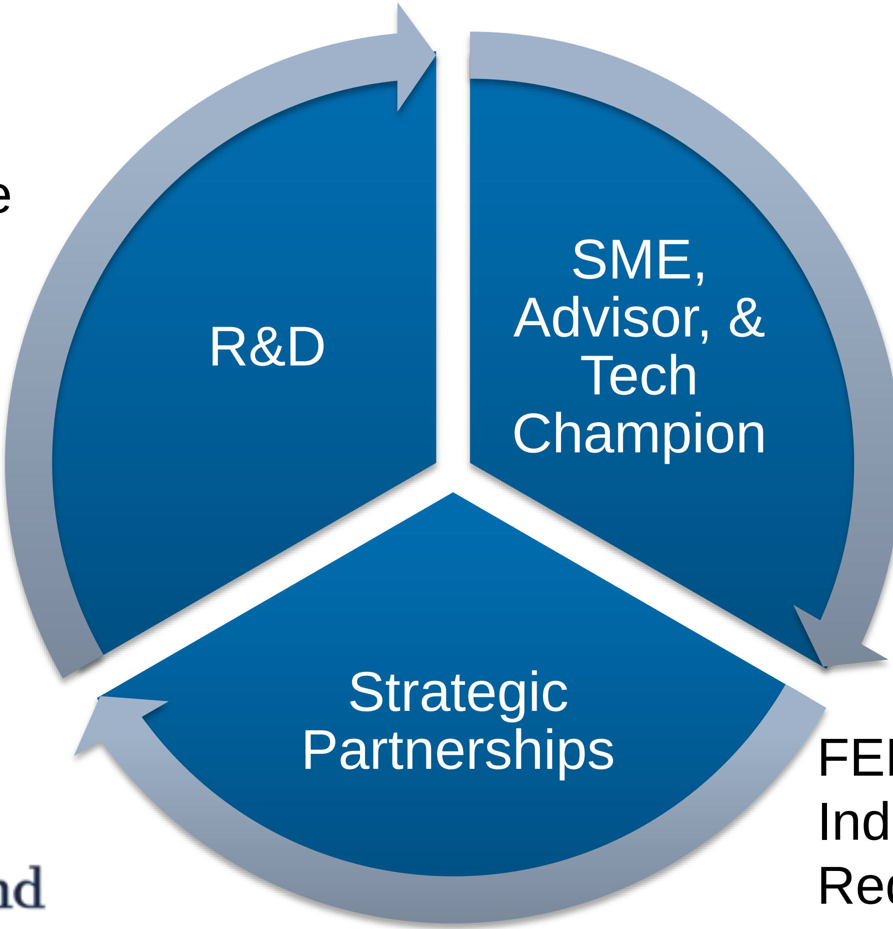
- Additional topics that need a response by the federal government:
  - The U.S. government should continue and enhance its active participation in international standards bodies so it can represent America's national interest with the private sector in the development of consensus-based voluntary mobile 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.

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

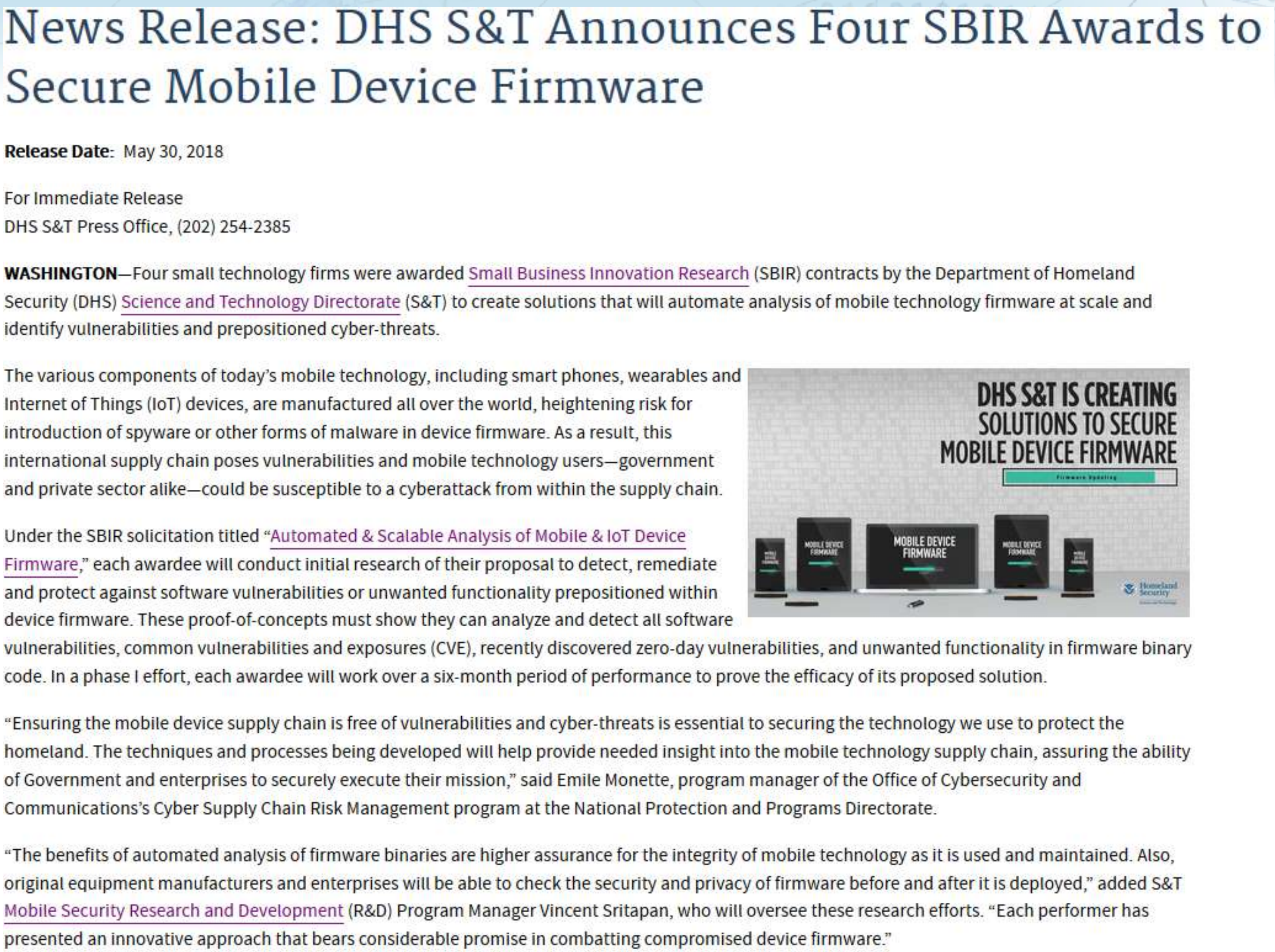
LRBAA & BAAs, OTS



Landscape Awareness
Lead Mobility CoP
Impact Policy
Support Procurement
Outreach

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

Firmware 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.

DHS S&T IS CREATING SOLUTIONS TO SECURE MOBILE DEVICE FIRMWARE
Firmware Updating
MOBILE DEVICE FIRMWARE
Homeland Security

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.

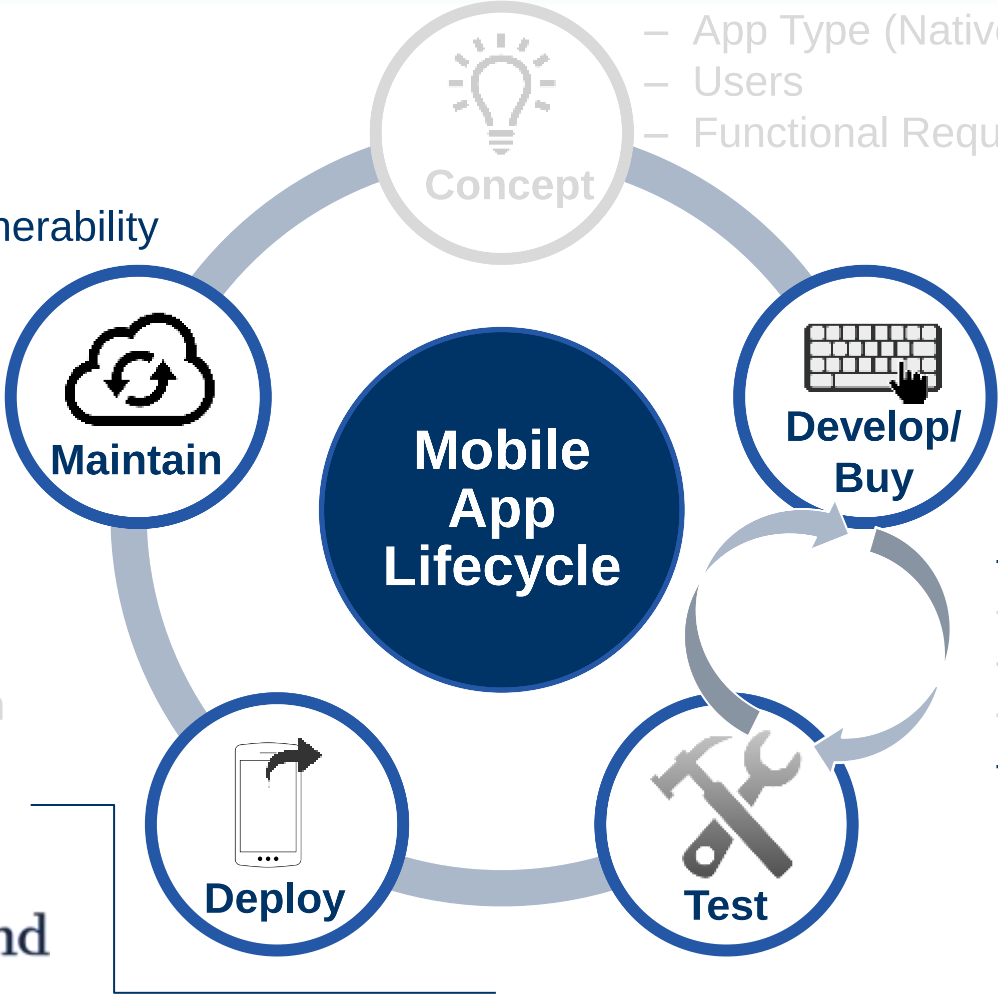
"Ensuring the mobile device supply chain is free of vulnerabilities and cyber-threats is essential to securing the technology we use to protect the homeland. The techniques and processes being developed will help provide needed insight into the mobile technology supply chain, assuring the ability of 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."

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

Mobile App Security R&D TTA II

Security in Mobile App Development



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

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

- App Vetting
- Authorization Decision
- App Store Deployment

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

Homeland Security

Science and Technology

Why Look for Cyber Threats?

- Aggressive data collection
  - Exfiltration of sensitive user-data to China (Adups)
  - Sensitive data collection (OnePlus 5)
- Remote system compromise
  - System compromise from insecure network communications (Ragentek)
- User data disclosure due to vendor modifications
  - Samsung leaking log data (CVE-2017-7978)
  - MediaTek leaking log data (CVE-2016-10135)
- Local “root” privilege escalation
  - Alcatel A30 (former Amazon Prime Exclusive Device)
  - Leagoo P1
  - Privileged EngineerMode app (OnePlus 5)
  - Android 4.4 devices with a MediaTek chipset

Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say

点击查看本文中文版

By MATT APUZZO and MICHAEL S. SCHMIDT NOV. 15, 2016

RELATED COVERAGE

BITS SPECIAL SECTION
Software as Weaponry in a Computer-Connected World

F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says

Homeland Security
Science and Technology

Android Devices on US Carriers - Vulnerabilities

- ZTE Blade Spark (sold by AT&T)
  - Write modem and logcat logs to external storage
- LG Phoenix 2 (sold by AT&T)
  - Write logcat logs to app’s private directory
  - Lock user out of their device
- Asus ZenFone V Live (sold by Verizon)
  - Command execution as `system` user
  - Take and write screenshot to external storage
- ZTE Blade Vantage (sold by Verizon)
  - Write modem and logcat logs to external storage
- Essential Phone (sold by Sprint)
  - Programmatic factory reset
- Coolpad Defiant (sold by T-Mobile)
  - Send, read, and modify text messages
  - Programmatic factory reset
  - Obtain phone numbers of contacts
- T-Mobile Revvl Plus (Coolpad) (sold by T-Mobile)
  - Send, read, and modify text messages
  - Programmatic factory reset
  - Obtain phone numbers of contacts
- ZTE ZMAX Pro (sold by T-Mobile)
  - Send, read, and modify text messages
  - Programmatic factory reset
  - Obtain phone numbers of contacts
  - Write modem and logcat log to external storage
- LG G6 (sold by Multiple Carriers)
  - Lock user out of their device
  - Write logcat logs to app’s private directory
- ZTE ZMAX Champ (sold by Total Wireless)
  - Write modem and logcat logs to external storage
  - Programmatic factory reset
  - Make device continually crash in recovery mode (brick device)

Homeland Security

Science and Technology

Homeland
Security

Science and Technology