Information Security and Privacy Advisory Board

The Mobile Threat Catalogue

National Cybersecurity Center of Excellence
October 28, 2016

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ABOUT THE NCCOE

STRATEGY

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

WHO WE ARE

SPONSORS

Advise and facilitate the center’s strategy

- White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- State of Maryland

TEAM MEMBERS

Collaborate to build real-world cybersecurity capabilities for end users

- NCCoE
- MITRE National Cybersecurity FFRDC
- Tech firms
- Industry
- Academia
- Government
- Project managers
- Project-specific collaborators
- National Cybersecurity Excellence Partners (NCEP)

END USERS

Work with center on use cases to address cybersecurity challenges

- Business sectors
- Individuals
- Academia
- Government
- Cybersecurity IT community
- Systems integrators

NATIONAL CYBERSECURITY EXCELLENCE PARTNERS

Akamai

ca technologies

CISCO

FireEye

Hewlett Packard Enterprise

HYTRUST

ID/DataWeb

intel

JUNIPER NETWORKS

Lookout

Microsoft

NEXTLABS

paloalto NETWORKS

Ping Identity

Pulse Secure

redhat

RSA

splunk>

Symantec

TiD

tripwire

Twistlock Security, built for containers

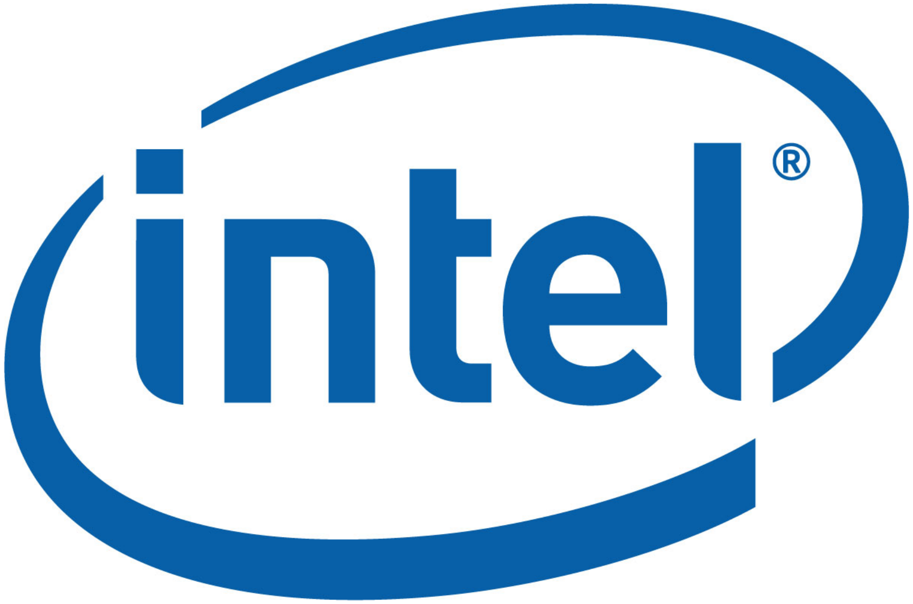
VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

VENAFI

vmware

PREVIOUS MOBILE EFFORTS

SP 1800-4 PARTNERS

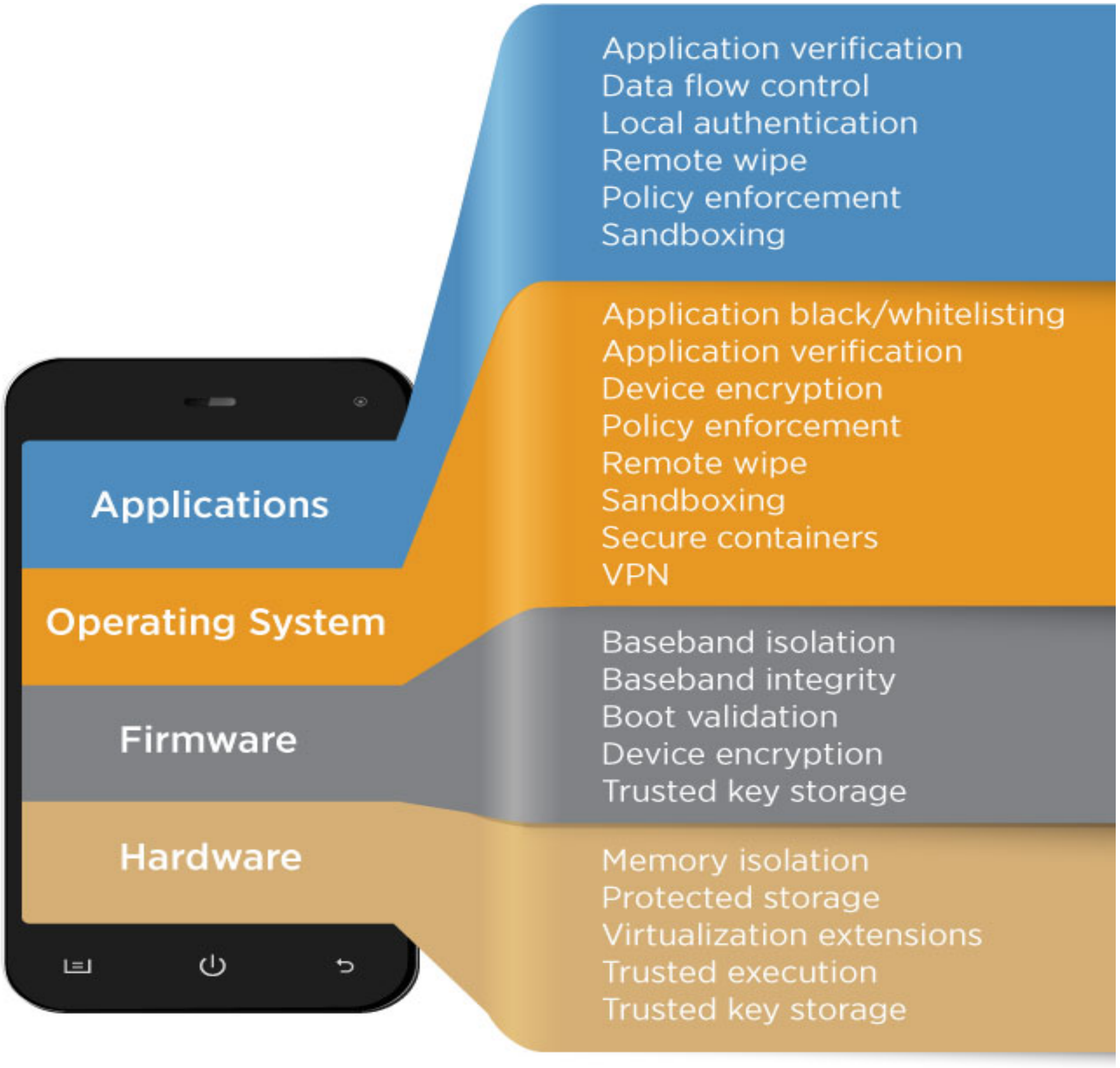


PROJECT GOALS

To demonstrate commercially available technologies that provide protection to both organization-issued and personally-owned mobile platforms, thereby:

- **Securely enabling basic email, calendar and contacts**
- Enabling users to work inside and outside the corporate network with a securely configured mobile device
- Allowing for granular control over the enterprise network boundary
- Minimizing the impact on function

DESIRABLE SECURITY CHARACTERISTICS



Applications

- Application verification
- Data flow control
- Local authentication
- Remote wipe
- Policy enforcement
- Sandboxing

Operating System

- Application black/whitelisting
- Application verification
- Device encryption
- Policy enforcement
- Remote wipe
- Sandboxing
- Secure containers
- VPN

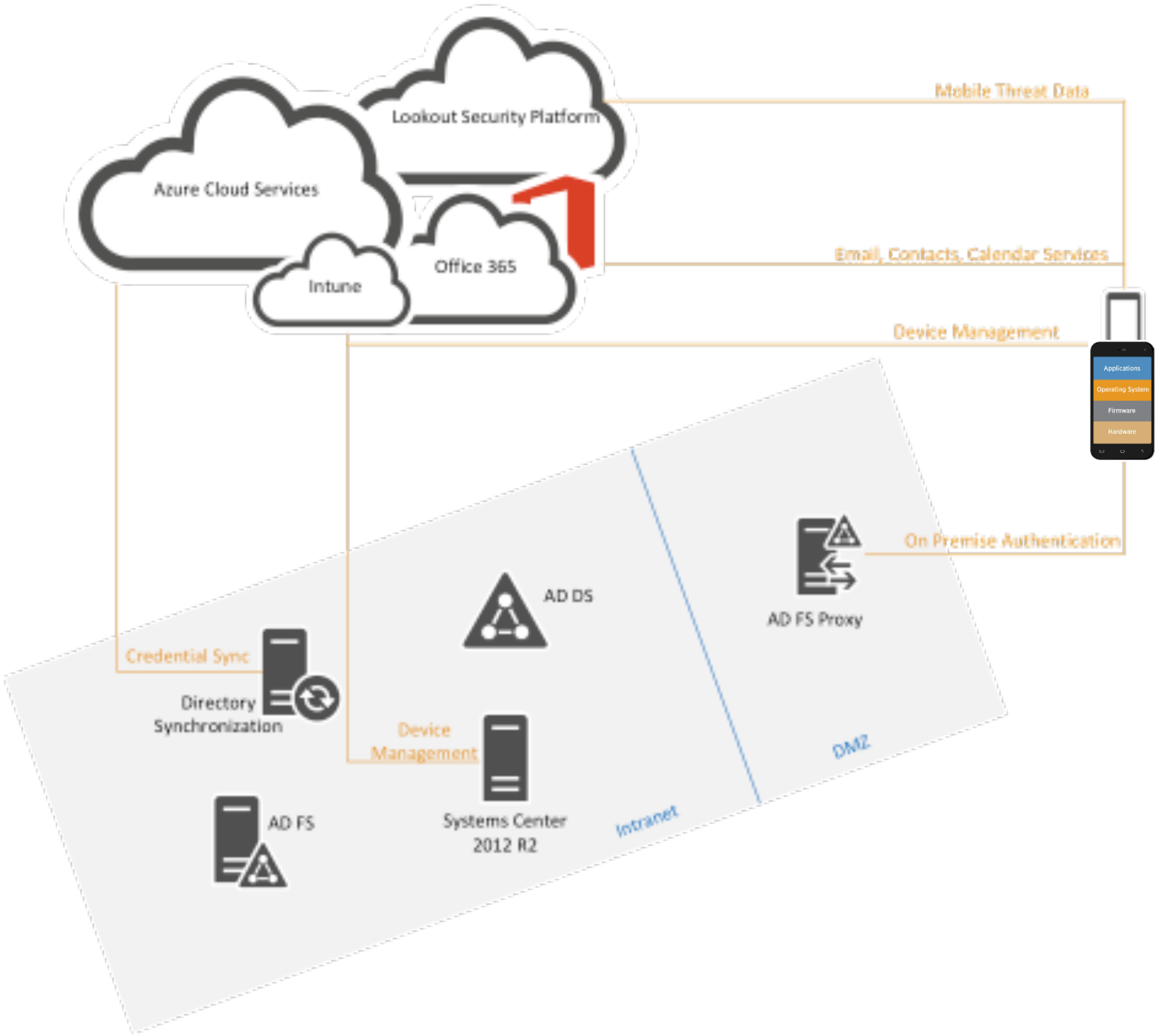
Firmware

- Baseband isolation
- Baseband integrity
- Boot validation
- Device encryption
- Trusted key storage

Hardware

- Memory isolation
- Protected storage
- Virtualization extensions
- Trusted execution
- Trusted key storage

EMM DEPLOYMENT



MOBILE THREAT CATALOGUE

CATALOGUE INTRO

SP 1800-4 Public Comment

- Many respondents highlighted a need for a more robust threat model
- Additional risks and mitigations were provided

Saw a Need to Collect This Information

- Incorporate 1800-4 public comment information
- Perform a baseline review of:
  - threat landscape
  - mobile security literature
  - industry practices
  - enterprise protections provided by industry

CATALOGUE DEVELOPMENT

DHS Study on Mobile Security

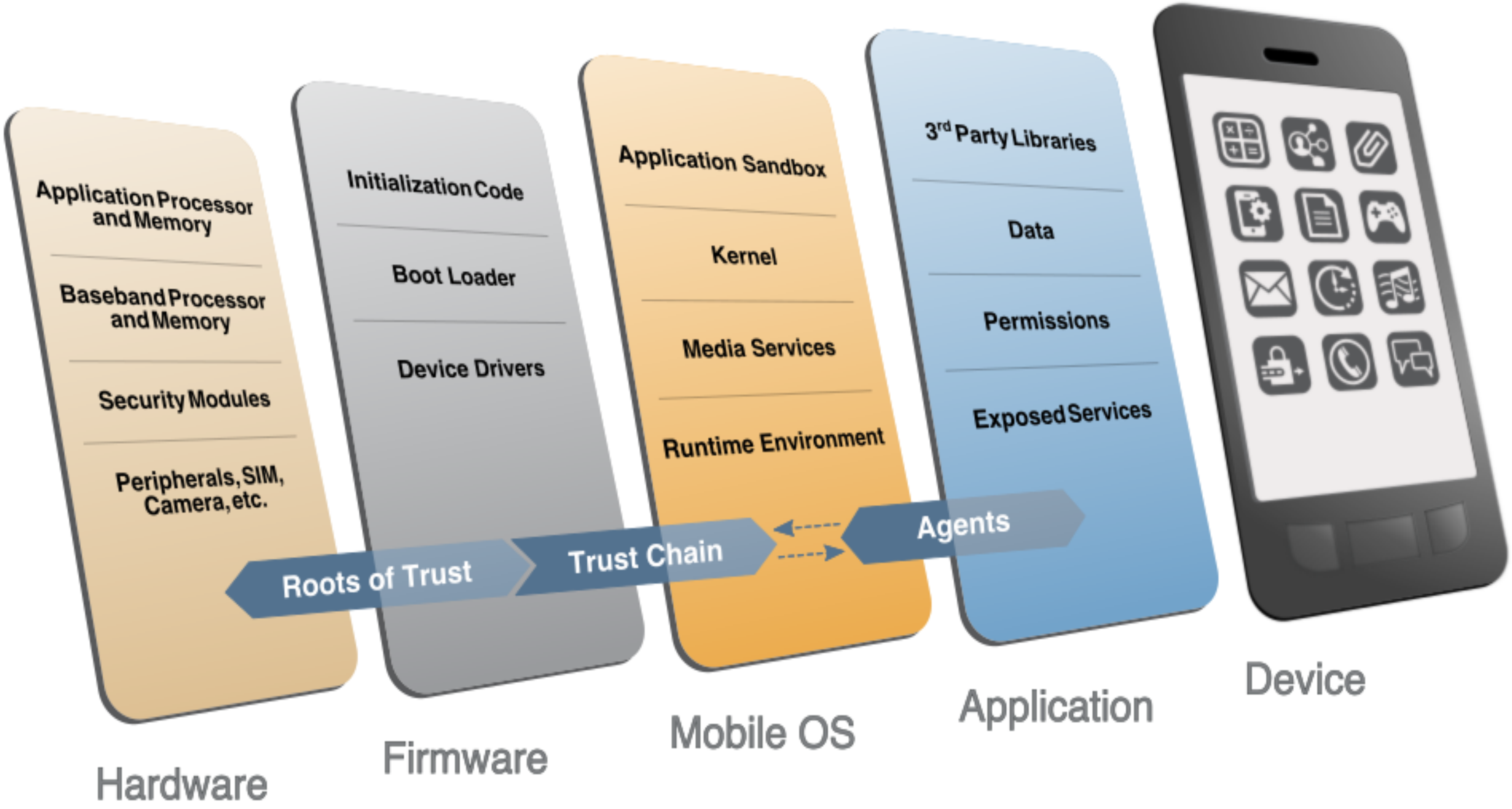
- Opportunity for collaboration
- Created in conjunction with the DHS Mobile Security Working Group
- Incorporating feedback from the GSA RFI on Mobile Threats & Defenses
- Incorporating feedback from DHS 1 on 1 meetings with industry

Mobile Threat Catalogue Purpose

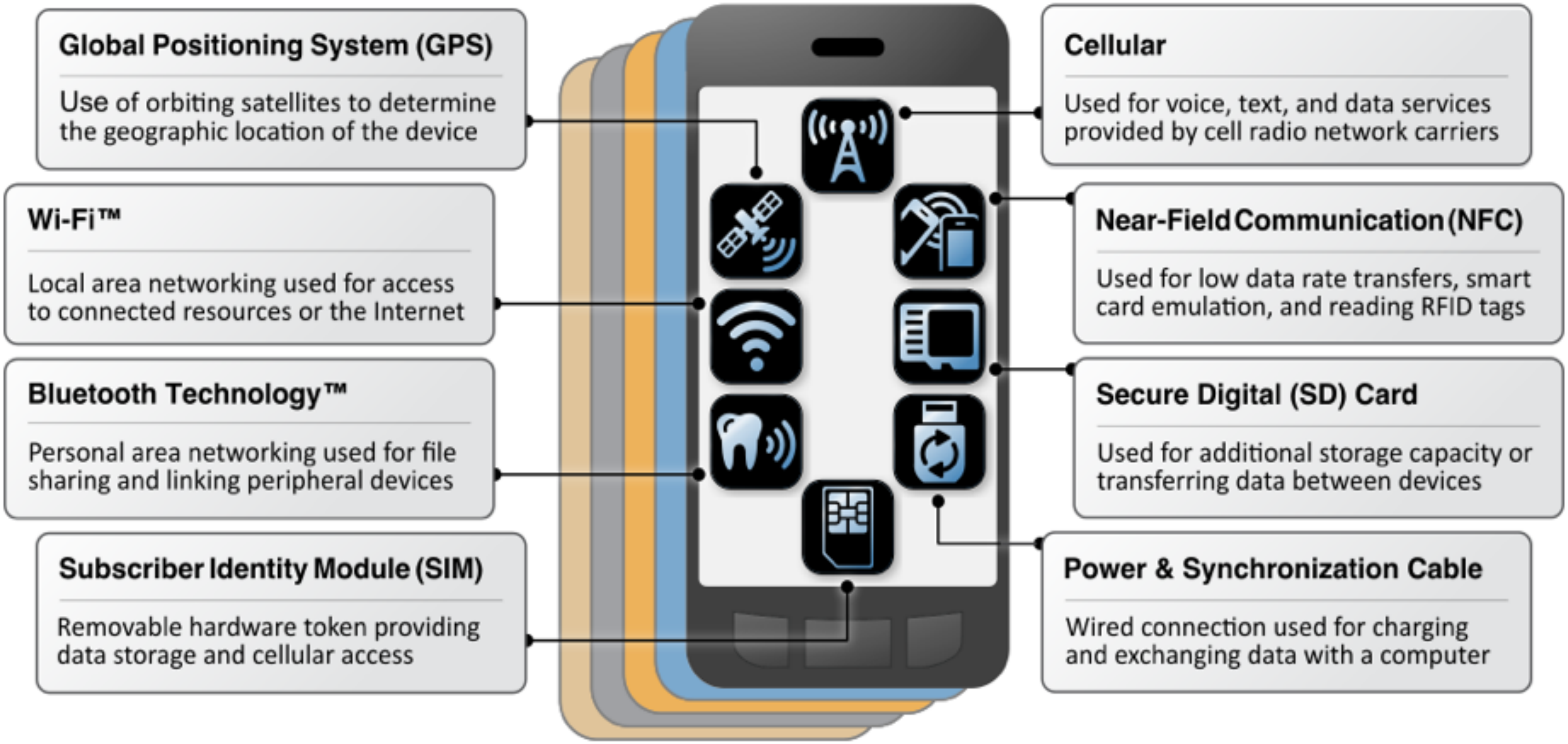
- Identify threats to devices, applications, networks, & infrastructure
- Collect countermeasures that IT security engineers can deploy to mitigate threats
- Inform risk assessments
- Build threat models
- Enumerate attack surface for enterprise mobile systems
- Assist in standards mapping activities

THREAT CATEGORIES

DEVICE TECHNOLOGY STACK



NETWORK INTERFACES



Global Positioning System (GPS)

Use of orbiting satellites to determine the geographic location of the device

Wi-Fi™

Local area networking used for access to connected resources or the Internet

Bluetooth Technology™

Personal area networking used for file sharing and linking peripheral devices

Subscriber Identity Module (SIM)

Removable hardware token providing data storage and cellular access

Cellular

Used for voice, text, and data services provided by cell radio network carriers

Near-Field Communication (NFC)

Used for low data rate transfers, smart card emulation, and reading RFID tags

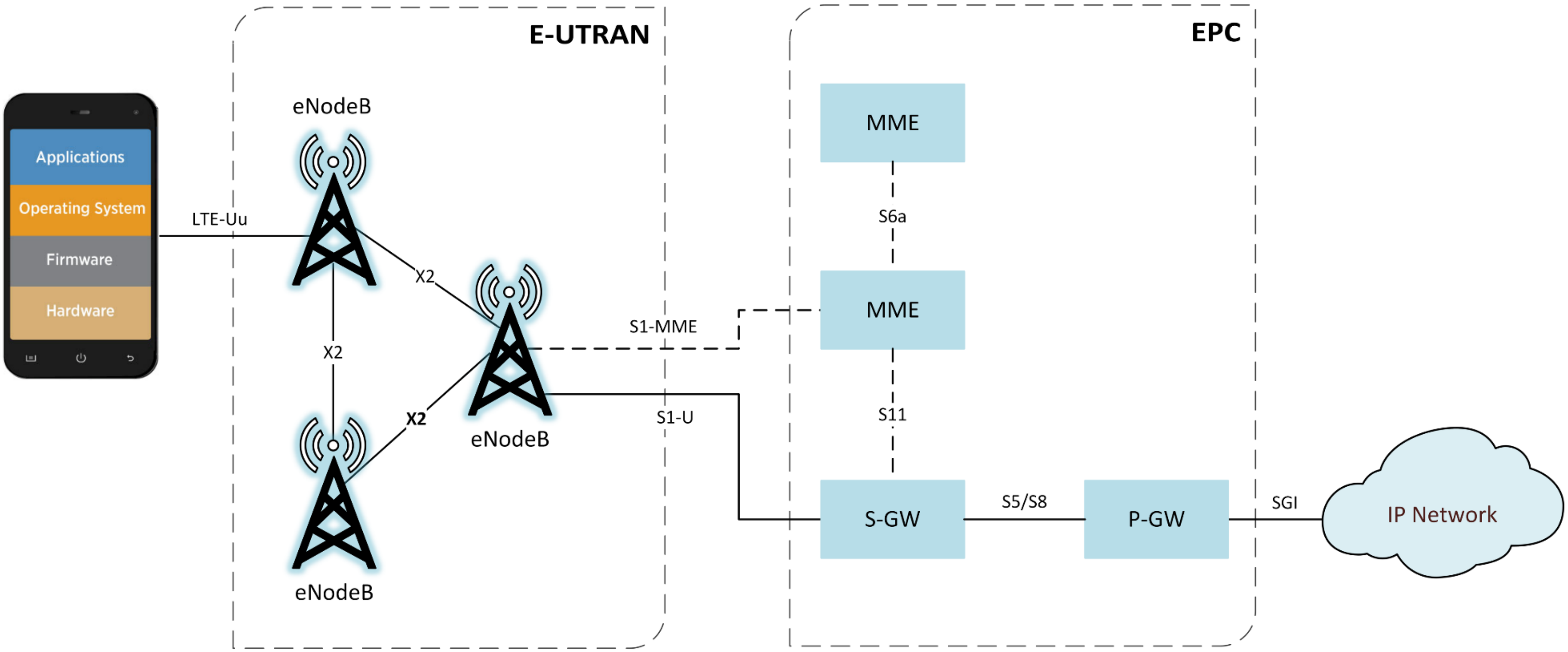
Secure Digital (SD) Card

Used for additional storage capacity or transferring data between devices

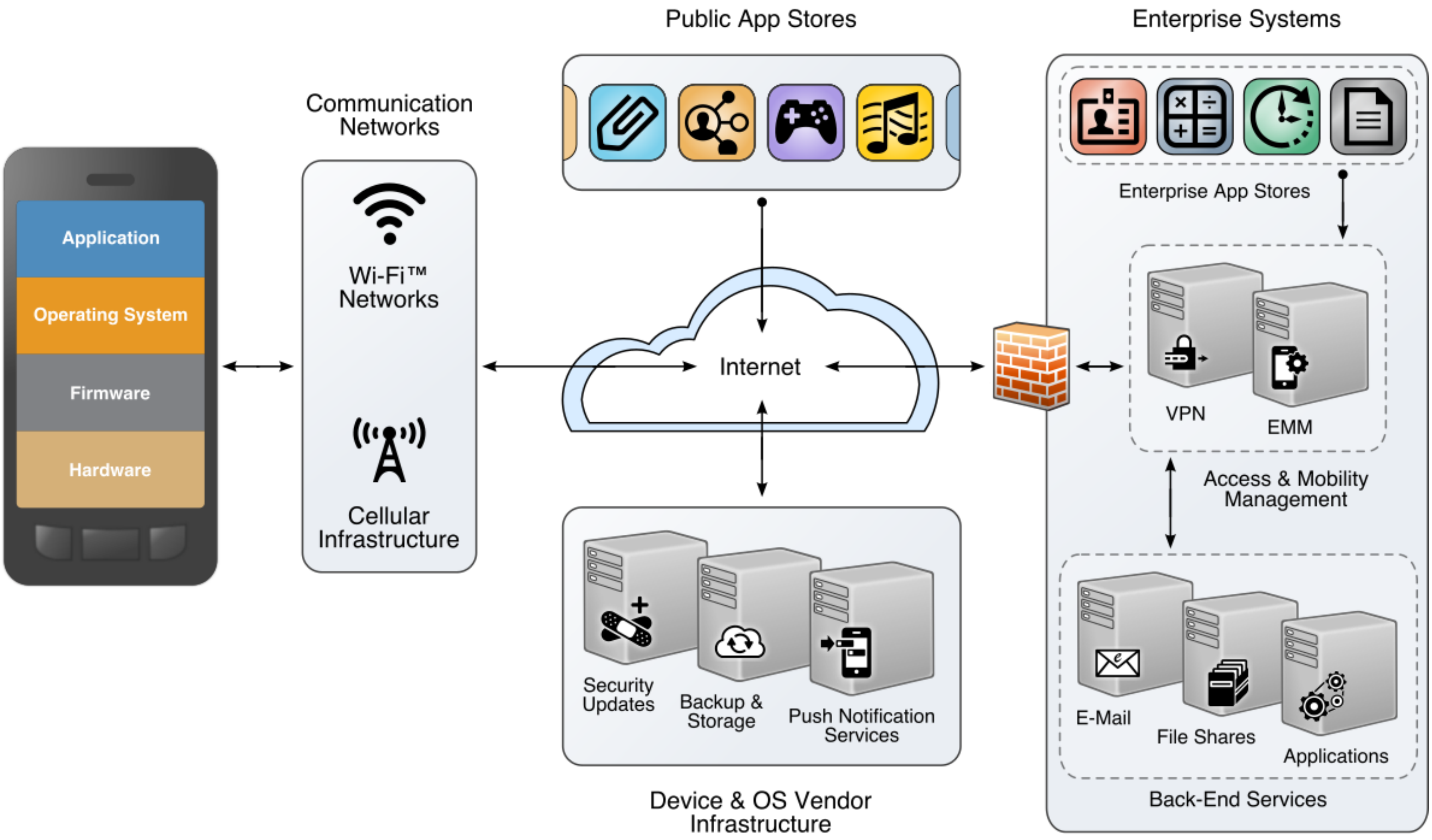
Power & Synchronization Cable

Wired connection used for charging and exchanging data with a computer

MOBILE NETWORK INFRASTRUCTURE



MOBILE ECOSYSTEM



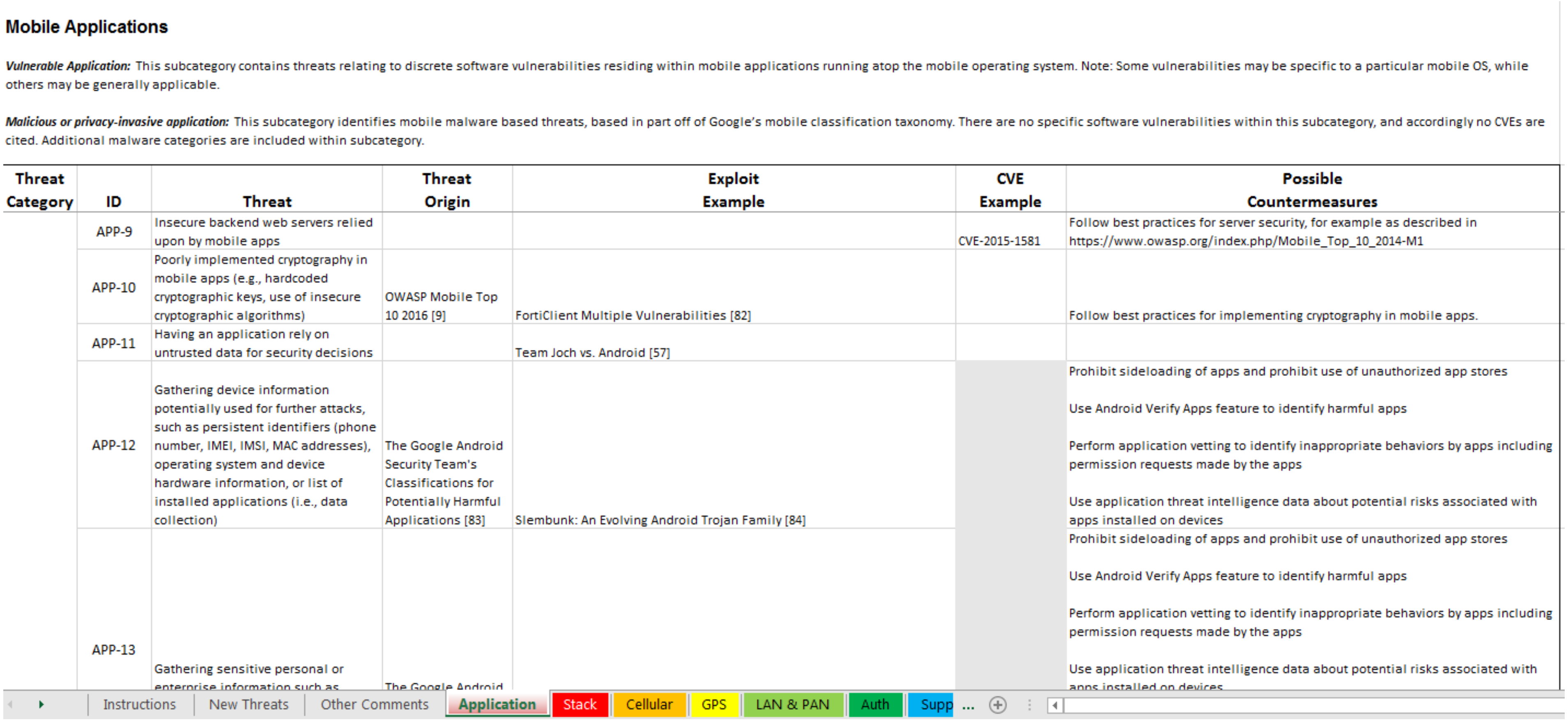
Additional Information on Categories

- Created broad threat categories and subcategories
- Identified the following information for each threat:
  - **Threat Category:** The major topic area pertaining to this threat. Topic areas are further divided when necessary.
  - **Threat Origin:** Reference to the source material used to initially identify the threat.
  - **Exploit Example:** A reference to examples of specific instances of this threat.
  - **Common Vulnerability and Exposure (CVE) Reference:** A specific vulnerability located within the National Vulnerability Database (NVD).
  - **Countermeasure:** Security controls or mitigations identified to reduce the impact of a particular threat.
- Links to reference materials (talks, publications, academic papers) included

THREAT CATEGORIES

Broad Threat Categories:

- Vulnerable Application
- Malicious or Privacy-invasive Application
- Operating System
- Mobile boot firmware
- SIM / USIM / UICC
- Device drivers
- Isolated Execution Environments
- Baseband firmware security
- Network Threats
    - WiFi, Bluetooth
    - NFC, Cellular
- Authentication
    - User to device, User or device to remote service
- Supply Chain
- Physical Access
- Mobile Ecosystem
- GPS
- Enterprise Mobility Management
- Private Mobile Application Stores
- Mobile Payment
- Cellular infrastructure



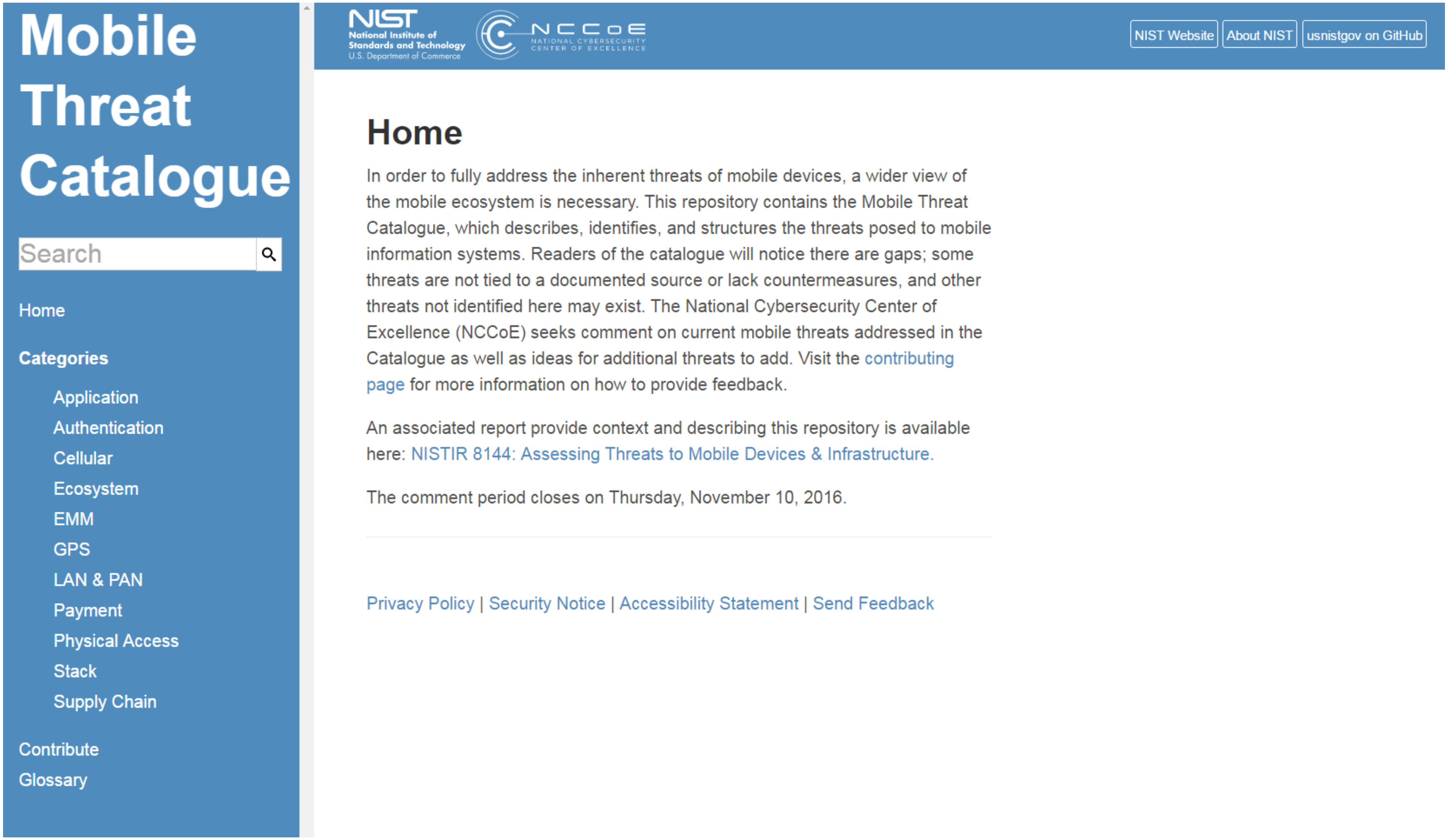
Mobile Applications

Vulnerable Application: This subcategory contains threats relating to discrete software vulnerabilities residing within mobile applications running atop the mobile operating system. Note: Some vulnerabilities may be specific to a particular mobile OS, while others may be generally applicable.

Malicious or privacy-invasive application: This subcategory identifies mobile malware based threats, based in part off of Google's mobile classification taxonomy. There are no specific software vulnerabilities within this subcategory, and accordingly no CVEs are cited. Additional malware categories are included within subcategory.

Threat Category	ID	Threat	Threat Origin	Exploit Example	CVE Example	Possible Countermeasures
	APP-9	Insecure backend web servers relied upon by mobile apps			CVE-2015-1581	Follow best practices for server security, for example as described in https://www.owasp.org/index.php/Mobile_Top_10_2014-M1
	APP-10	Poorly implemented cryptography in mobile apps (e.g., hardcoded cryptographic keys, use of insecure cryptographic algorithms)	OWASP Mobile Top 10 2016 [9]	FortiClient Multiple Vulnerabilities [82]		Follow best practices for implementing cryptography in mobile apps.
	APP-11	Having an application rely on untrusted data for security decisions		Team Joch vs. Android [57]		
	APP-12	Gathering device information potentially used for further attacks, such as persistent identifiers (phone number, IMEI, IMSI, MAC addresses), operating system and device hardware information, or list of installed applications (i.e., data collection)	The Google Android Security Team's Classifications for Potentially Harmful Applications [83]	Slembunk: An Evolving Android Trojan Family [84]		Prohibit sideloading of apps and prohibit use of unauthorized app stores Use Android Verify Apps feature to identify harmful apps Perform application vetting to identify inappropriate behaviors by apps including permission requests made by the apps Use application threat intelligence data about potential risks associated with apps installed on devices
	APP-13	Gathering sensitive personal or enterprise information such as	The Google Android			Prohibit sideloading of apps and prohibit use of unauthorized app stores Use Android Verify Apps feature to identify harmful apps Perform application vetting to identify inappropriate behaviors by apps including permission requests made by the apps Use application threat intelligence data about potential risks associated with apps installed on devices

CATALOGUE



Home

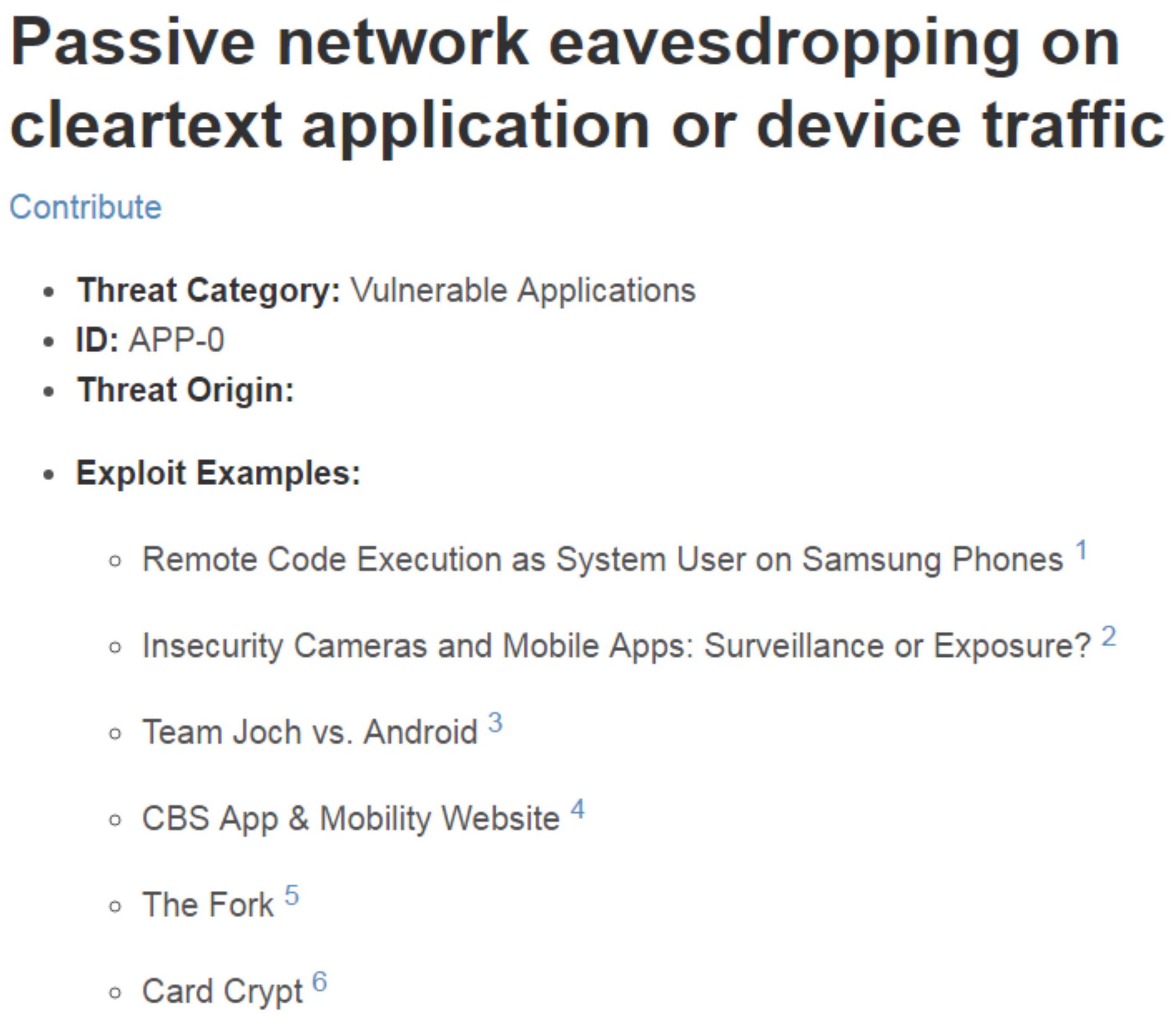
In order to fully address the inherent threats of mobile devices, a wider view of the mobile ecosystem is necessary. This repository contains the Mobile Threat Catalogue, which describes, identifies, and structures the threats posed to mobile information systems. Readers of the catalogue will notice there are gaps; some threats are not tied to a documented source or lack countermeasures, and other threats not identified here may exist. The National Cybersecurity Center of Excellence (NCCoE) seeks comment on current mobile threats addressed in the Catalogue as well as ideas for additional threats to add. Visit the contributing page for more information on how to provide feedback.

An associated report provide context and describing this repository is available here: NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure.

The comment period closes on Thursday, November 10, 2016.

Privacy Policy | Security Notice | Accessibility Statement | Send Feedback

EXAMPLE THREAT



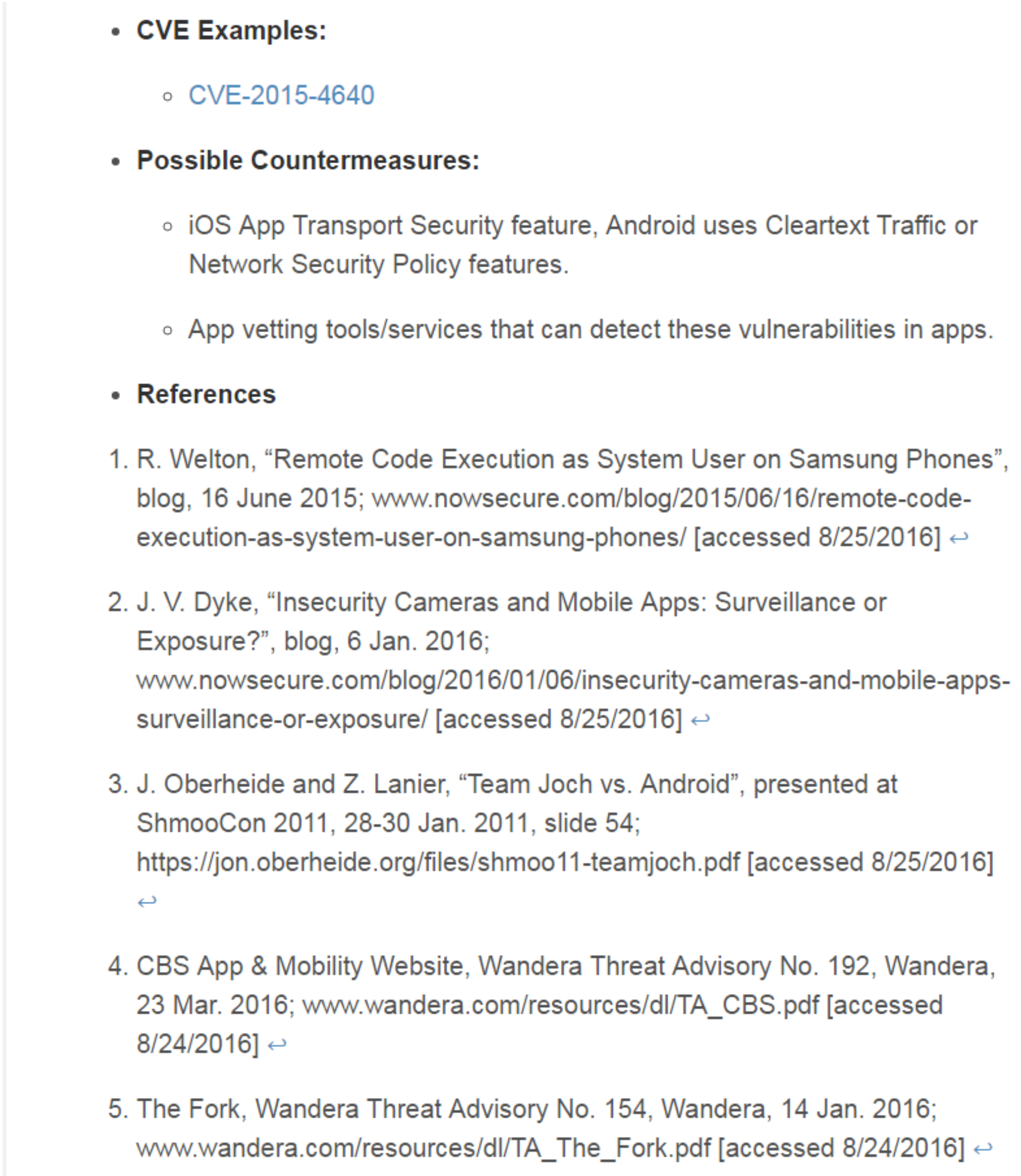
Passive network eavesdropping on cleartext application or device traffic

Contribute

- **Threat Category:** Vulnerable Applications
- **ID:** APP-0
- **Threat Origin:**

- **Exploit Examples:**
  - Remote Code Execution as System User on Samsung Phones [1]
  - Insecurity Cameras and Mobile Apps: Surveillance or Exposure? [2]
  - Team Joch vs. Android [3]
  - CBS App & Mobility Website [4]
  - The Fork [5]
  - Card Crypt [6]

EXAMPLE THREAT



- **CVE Examples:**
  - CVE-2015-4640
- **Possible Countermeasures:**
  - iOS App Transport Security feature, Android uses Cleartext Traffic or Network Security Policy features.
  - App vetting tools/services that can detect these vulnerabilities in apps.
- **References**

1. R. Welton, “Remote Code Execution as System User on Samsung Phones”, blog, 16 June 2015; www.nowsecure.com/blog/2015/06/16/remote-code-execution-as-system-user-on-samsung-phones/ [accessed 8/25/2016] ↩

2. J. V. Dyke, “Insecurity Cameras and Mobile Apps: Surveillance or Exposure?”, blog, 6 Jan. 2016; www.nowsecure.com/blog/2016/01/06/insecurity-cameras-and-mobile-apps-surveillance-or-exposure/ [accessed 8/25/2016] ↩

3. J. Oberheide and Z. Lanier, “Team Joch vs. Android”, presented at ShmooCon 2011, 28-30 Jan. 2011, slide 54; https://jon.oberheide.org/files/shmoo11-teamjoch.pdf [accessed 8/25/2016] ↩

4. CBS App & Mobility Website, Wandera Threat Advisory No. 192, Wandera, 23 Mar. 2016; www.wandera.com/resources/dl/TA_CBS.pdf [accessed 8/24/2016] ↩

5. The Fork, Wandera Threat Advisory No. 154, Wandera, 14 Jan. 2016; www.wandera.com/resources/dl/TA_The_Fork.pdf [accessed 8/24/2016] ↩

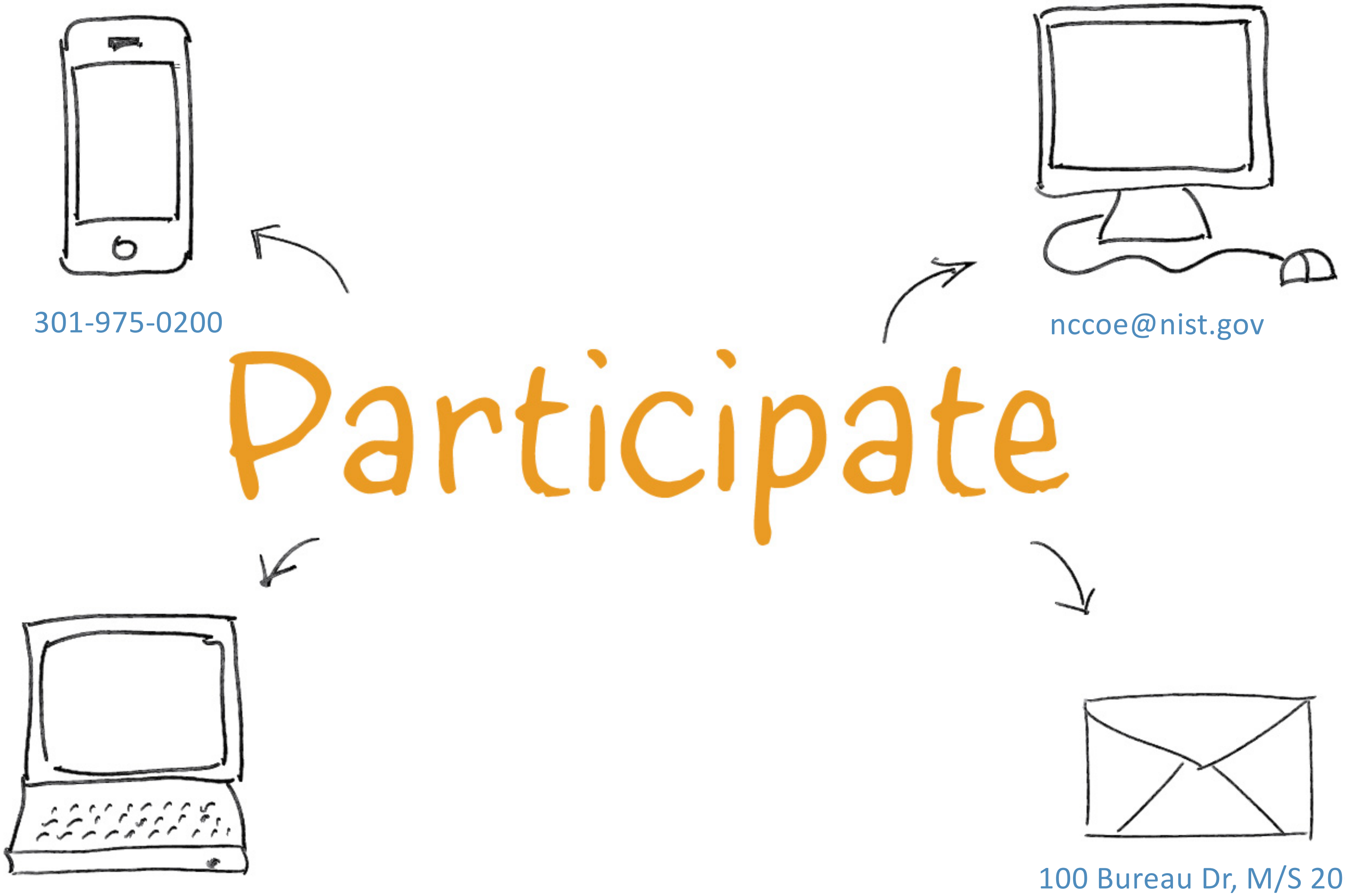
CONCLUSION

Companion NISTIR, Provides Context for the Catalogue

- NISTIR 8144: Assessing Threats to Mobile Devices & Infrastructure
- The catalogue and NISTIR 8144 available on NCCoE and CSRC
- Gathering feedback from academia, industry, and government
    - Comment period closes Nov. 10

Next Steps

- Vet the catalogue with industry
- Incorporate public comment and other feedback
- Send to Congress
- Incorporate catalogue into NCCoE Mobile Device Security project/program area



Participate

301-975-0200

nccoe@nist.gov

http://nccoe.nist.gov

100 Bureau Dr, M/S 2002
Gaithersburg, MD 20899