# National Cybersecurity Center of Excellence

Practical Solutions for Complex Cybersecurity Challenges

## Mobile Device Security and Privacy

Gema Howell and Julie Snyder

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

# WELCOME!

This meeting is being recorded.

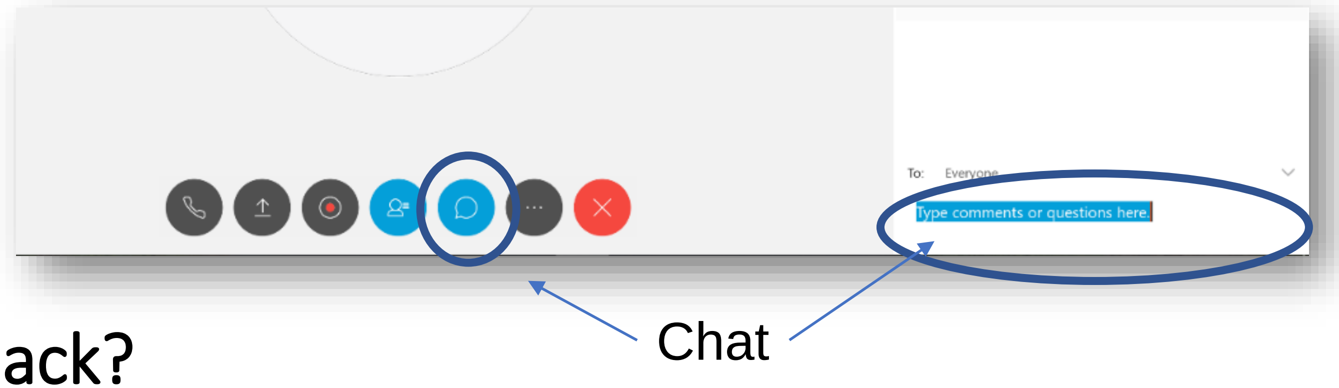
Please use the Q&A window to submit questions throughout this event.

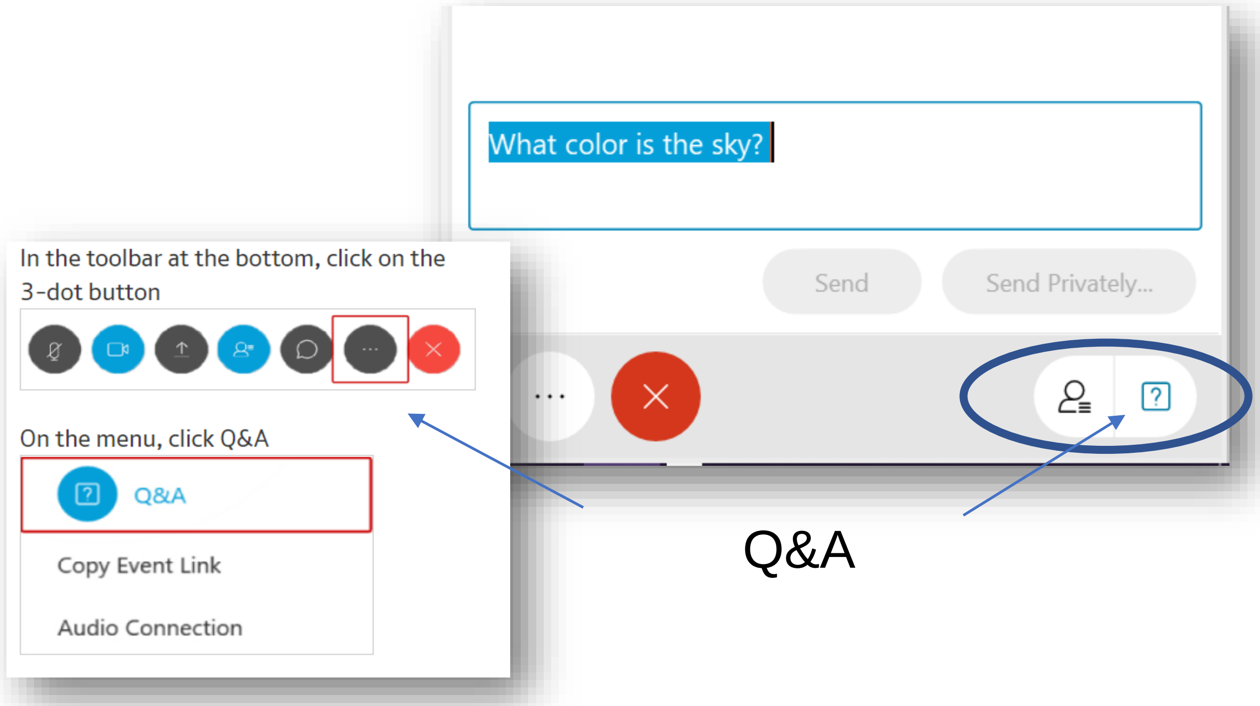
Would you like to provide your feedback? During the webinar, we are asking questions that will be individually recorded.

Answering the questions is completely optional.

Have additional comments? Email us your thoughts at:

mobile-nccoe@nist.gov




In the toolbar at the bottom, click on the 3-dot button

On the menu, click Q&A

What color is the sky?

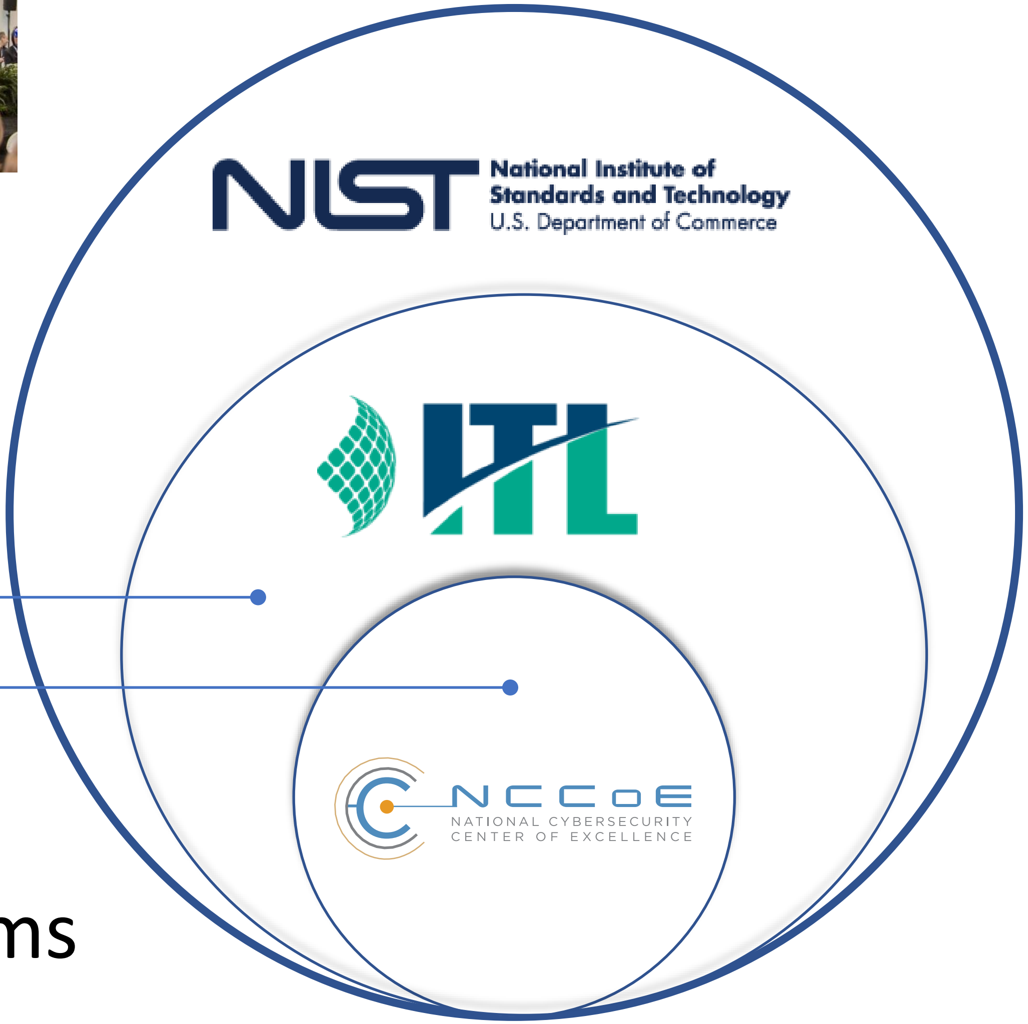
# OPENING QUESTION #1: UNDERSTANDING OUR AUDIENCE

Are you familiar with the NCCoE and the work products that we produce?

- A: Yes
- B: A little
- C: No

# WHO WE ARE

As part of the NIST family, the NCCoE has access to a foundation of **expertise, resources, relationships,** and **experience**


NIST National Institute of Standards and Technology U.S. Department of Commerce
ITL
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Information Technology Laboratory

Applied Cybersecurity Division

A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

# OUR GOALS

**Improve cybersecurity** for businesses and commerce

**Lower the learning curve** for cybersecurity

**Spark innovation** in secure technology

# NCCOE PRINCIPLES

### Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

### Modular

Develop components that can be substituted with alternates that offer equivalent input-output specifications

### Repeatable

Provide detailed guidance including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

### Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

### Usable

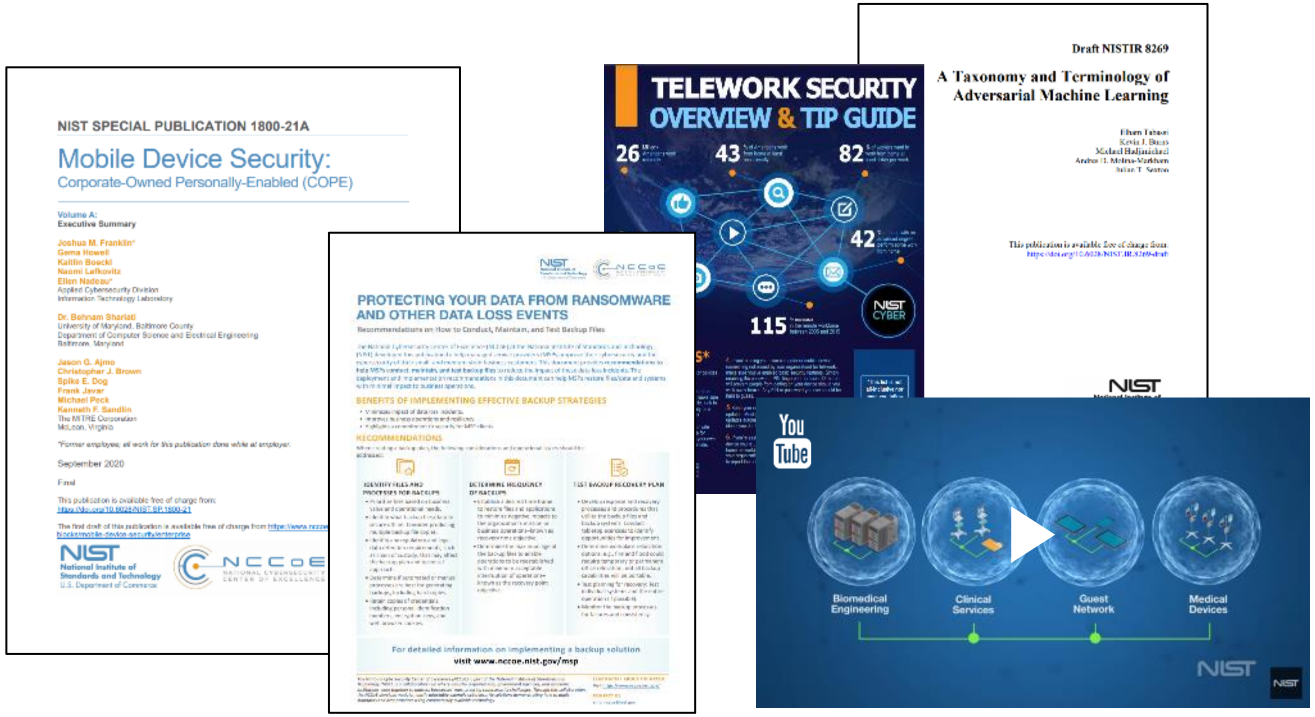
Design blueprints that end users can cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

### Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

# NIST PRODUCTS

**Practical**, **user-friendly** resources demonstrating **standards-based** approaches to cybersecurity matched to business needs



NIST SPECIAL PUBLICATION 1800-21A

Mobile Device Security:
Corporate-Owned Personally-Enabled (COPE)

Volume A:
Executive Summary

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Applied Cybersecurity Division
Information Technology Laboratory

Dr. Behnam Shariati
University of Maryland, Baltimore County
Department of Computer Science and Electrical Engineering
Baltimore, Maryland

Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin
The MITRE Corporation
McLean, Virginia

*Former employee; all work for this publication done while at employer.

September 2020

Final

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-21

PROTECTING YOUR DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS

Recommendations on How to Conduct, Maintain, and Test Backup Files

BENEFITS OF IMPLEMENTING EFFECTIVE BACKUP STRATEGIES

RECOMMENDATIONS

IDENTIFY FILES AND PROCESSES FOR BACKUPS

DETERMINE FREQUENCY OF BACKUPS

TEST BACKUP RECOVERY PLAN

For detailed information on implementing a backup solution visit www.nccoe.nist.gov/msp

TELEWORK SECURITY OVERVIEW & TIP GUIDE

Draft NISTIR 8269

A Taxonomy and Terminology of Adversarial Machine Learning

Elham Tabassi
Kevin J. Burns
Michael Hadjimichael
Andres D. Molina-Markham
Julian T. Sexton

This publication is available free of charge from: https://doi.org/10.6028/NISTIR.8269-draft

www.nccoe.nist.gov/library

- Cybersecurity Practice Guides
- Tip Sheets
- Short Form Papers
- Short Videos
- Learning Series Webinars

# IMPACT: WORK FROM ANYWHERE

## Minimizing your risks to working anywhere, anytime, from any device

- Mobile Device Security
- Applications of the NIST Privacy Framework
- Working Anytime, Anywhere: The Evolution of Telework

# OPENING QUESTION #2: UNDERSTANDING OUR AUDIENCE

How many are planning to upgrade / improve your mobile device infrastructure in the next year?

- A: Beginning upgrades or improvements in the next year
- B: Not upgrading or improving in the next year
- C: Could be in the works. It has been talked about / we are considering it

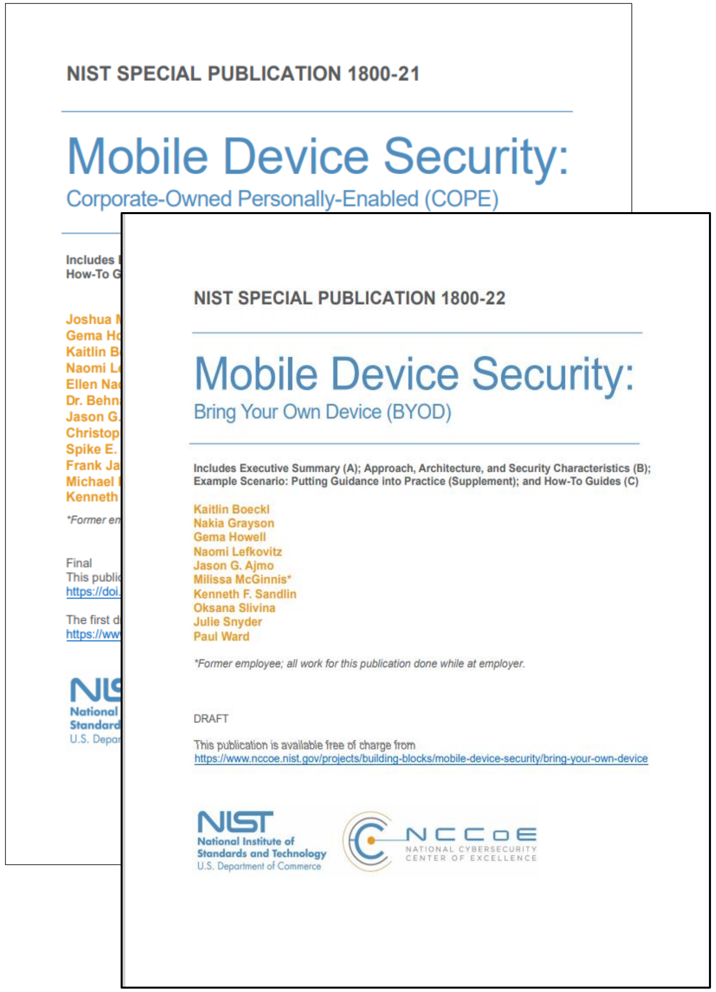
# OUR AGENDA TODAY

## Latest NIST Mobile Device Security Special Publications (SPs)

- Corporate-Owned Personally -Enabled
- **Bring Your Own Device**

## How can we help You?

- We’d like to hear from You!
- What mobile device security and privacy areas can we focus on in the future?
- Email us at [mobile-nccoe@nist.gov](mailto:mobile-nccoe@nist.gov)



NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security:
Corporate-Owned Personally-Enabled (COPE)

Includes
How-To G

Joshua
Gema Ho
Kaitlin B
Naomi Le
Ellen Na
Dr. Behn
Jason G.
Christop
Spike E.
Frank Ja
Michael
Kenneth

*Former em

Final
This public
https://doi.

The first d
https://ww

NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security:
Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

*Former employee; all work for this publication done while at employer.

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# MOBILE DEVICE SECURITY NIST SP 1800-21

## NIST SP 1800-21 Mobile Device Security: *Corporate-Owned Personally-Enabled (COPE)*

- Fully-managed organizationally owned device
- Android and Apple mobile phones
- Volumes A, B and C published and available in PDF and web versions
- Additional feedback can be shared via email at mobile-nccoe@nist.gov

apthority TRUST YOUR APPS

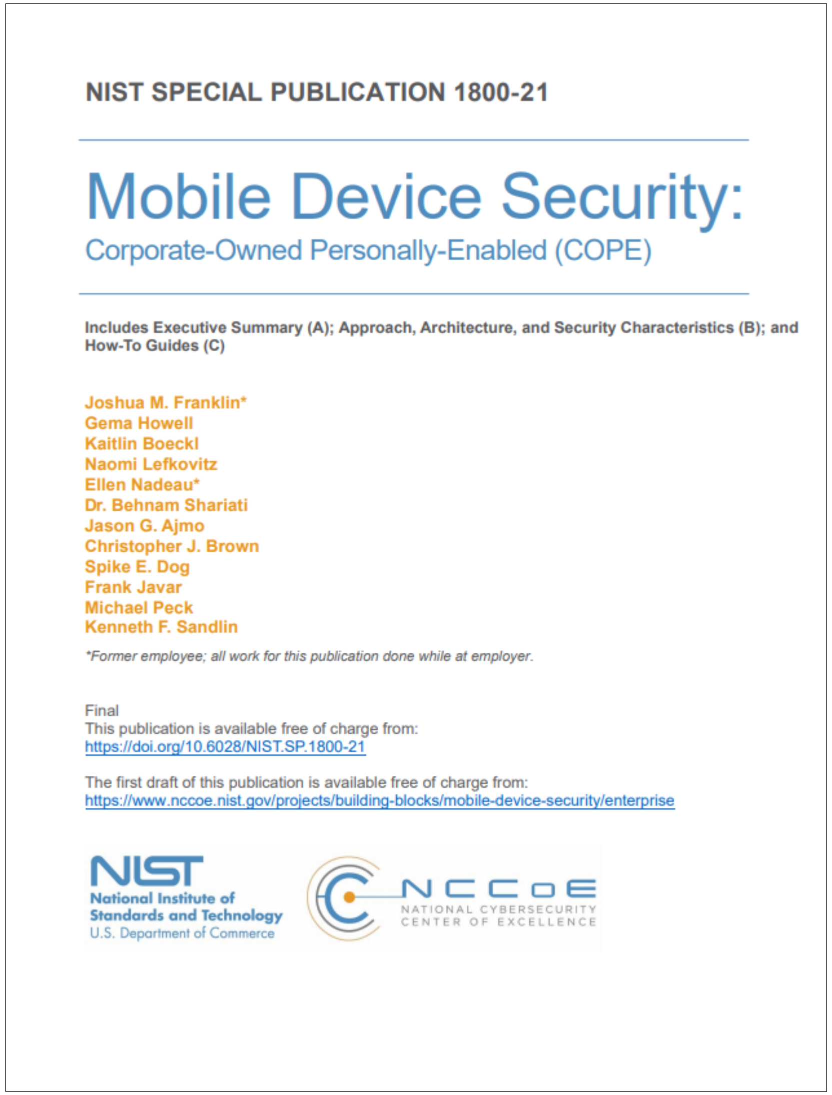
kryptowire

paloalto NETWORKS

Lookout

mobileiron

Qualcomm



NIST SPECIAL PUBLICATION 1800-21

Mobile Device Security:

Corporate-Owned Personally-Enabled (COPE)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Joshua M. Franklin*
Gema Howell
Kaitlin Boeckl
Naomi Lefkovitz
Ellen Nadeau*
Dr. Behnam Shariati
Jason G. Ajmo
Christopher J. Brown
Spike E. Dog
Frank Javar
Michael Peck
Kenneth F. Sandlin

*Former employee; all work for this publication done while at employer.

Final
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-21

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise

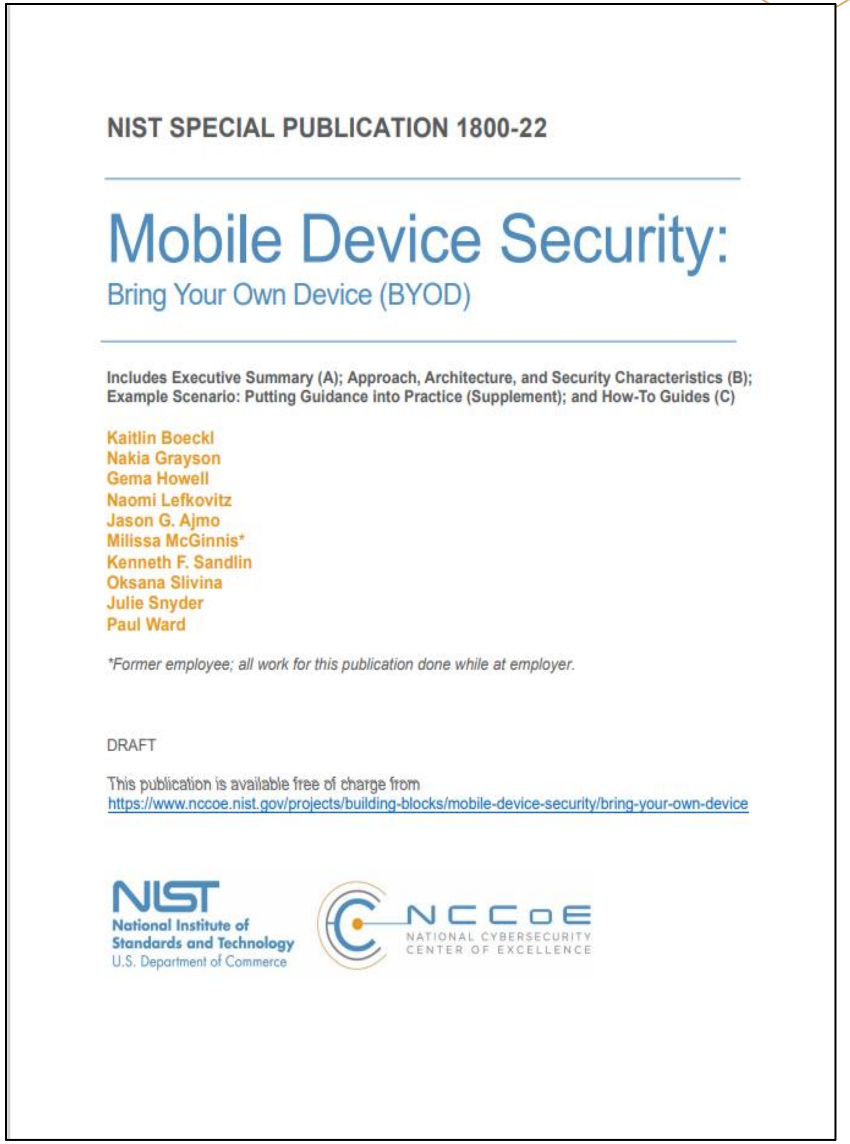
NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# MOBILE DEVICE SECURITY NIST SP 1800-22

## NIST SP 1800-22 *Mobile Device Security: Bring Your Own Device (BYOD)*

- Employee-owned device with security and privacy enhanced architecture
- Android and Apple mobile phones
- Comments on the published draft can be submitted to https://www.nccoe.nist.gov/webform/comments-draft-sp-1800-22-mobile-device-security-bring-your-own-device or mobile-nccoe@nist.gov by **Monday, May 17, 2021**



NIST SPECIAL PUBLICATION 1800-22

Mobile Device Security:

Bring Your Own Device (BYOD)

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); Example Scenario: Putting Guidance into Practice (Supplement); and How-To Guides (C)

Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz
Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward

*Former employee; all work for this publication done while at employer.

DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# QUESTION #3: AWARENESS OF NIST SP 1800-22?

- Who’s aware of NIST SP 1800-22, Mobile Device Security: BYOD?

- A: Aware of it, and have started reading it
- B: Aware of it, but haven’t started reading it
- C: Not aware of it before being invited to this webinar

# NIST SP 1800-22, MOBILE DEVICE SECURITY: BRING YOUR OWN DEVICE (BYOD)

## DOCUMENT STRUCTURE OVERVIEW AND AUDIENCE

### Volume A: Executive Summary

- Summary of the document
- Business decision makers, including chief security and technology officers

### Volume B: Approach, Architecture, and Security Characteristics

- What we built and why
- Technology or security program managers

### Volume C: How-To Guides

- Instructions for building the example solution
- IT Professionals

### Supplement: Example Scenario: Putting Guidance into Practice

- How a fictional exemplar organization deployed their BYOD solution
- Technology or security program managers and IT Professionals

# QUESTION #4: WHICH PARTS OF NIST SP 1800-22 WILL BE MOST USEFUL?

- Which parts of the publication will be most useful to you?

- A: Volume A, Executive Summary (to help achieve Stakeholder awareness)
- B: Volume B, Approach, Architecture and Security (and Privacy) Characteristics (to understand the architecture)
- C: Volume C How-To Guide (to have a ready to implement how-to set of instructions)
- D: The Supplement: Example Scenario: Putting Guidance into Practice
- E: All of the above

# SUPPLEMENT: OUR APPROACH TO TELLING THE STORY

## Scenario-based example:

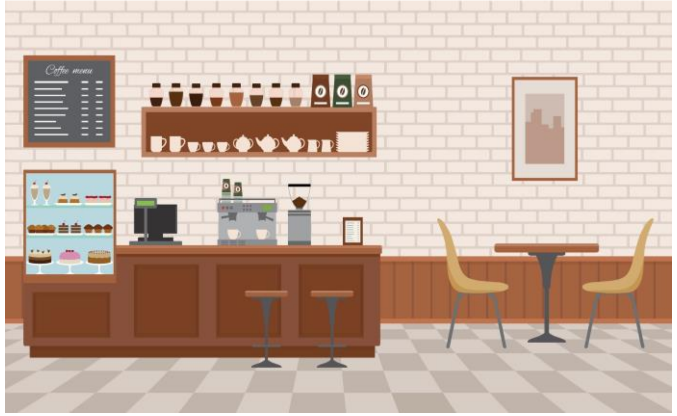
- Small-to-mid-sized (fictional) accounting services company

## Motivation for BYOD:

- Growing organization, now with remote work needs

## Goals:

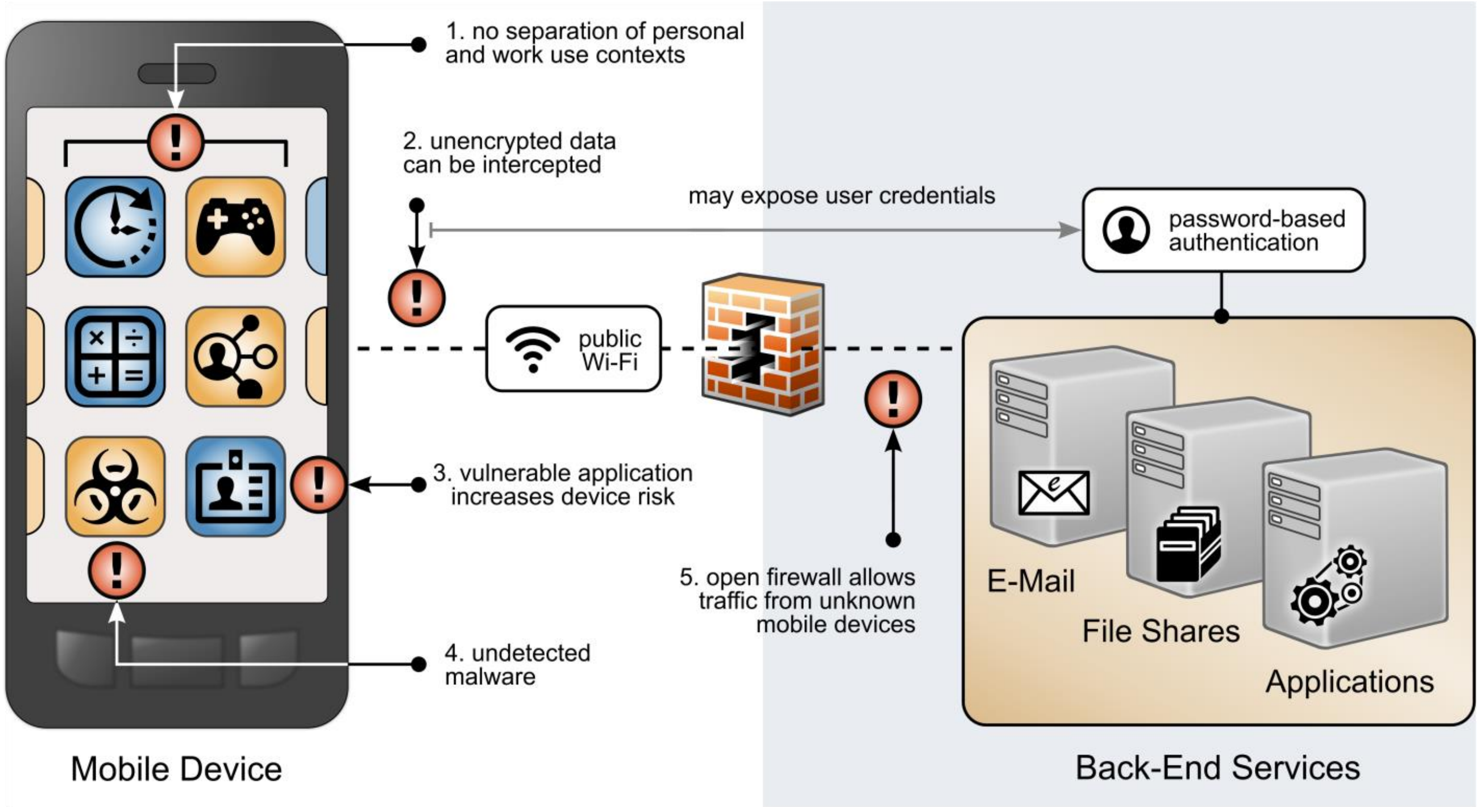
- Provide remote work capability
- Comply with organization’s policies
- Leverage security and privacy best practices and standards



# OUR APPROACH - TELLING THE STORY

## Scenario-based challenges to be solved:

- Managing employee-owned mobile devices
- Separating personal and work data
- Identifying and mitigating vulnerable mobile applications
- Detecting unusual activity or malware
- Encrypting data in transit
- Preventing unknown device traffic
- Protection from executed code with integrity issues
- Preserving the privacy of employee's personal data



1. no separation of personal and work use contexts
2. unencrypted data can be intercepted
may expose user credentials
password-based authentication
public Wi-Fi
3. vulnerable application increases device risk
5. open firewall allows traffic from unknown mobile devices
4. undetected malware
E-Mail
File Shares
Applications
Mobile Device
Back-End Services

## The supplement

- Provides a "walk through" of how a fictional organization implemented the example solution

# QUESTION #5: THOUGHTS ON THE EXAMPLE SUPPLEMENT?

- The Example Supplement is something new that we have included in NIST SP 1800-22 Mobile Device Security: BYOD. How helpful do you think the Example Scenario supplement will be in helping your organization implement the guide?

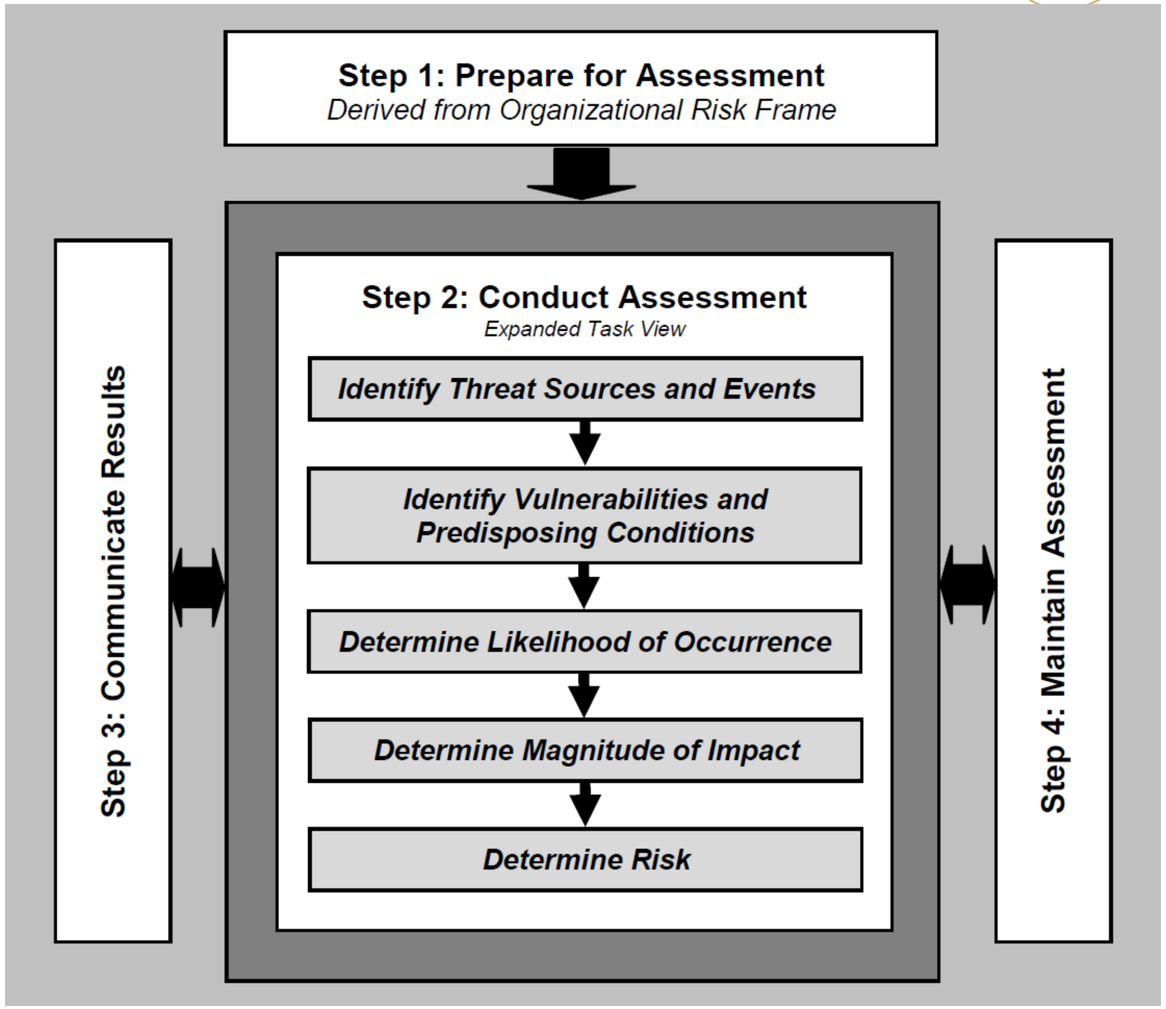
- A: Very helpful
- B: Somewhat helpful
- C: Not very helpful

# RISK ASSESSMENT

- Referenced NIST Cybersecurity Framework, Risk Management Framework, and Privacy Framework

- Identified Threats Events (TE) using the NIST Mobile Threat Catalogue (MTC)

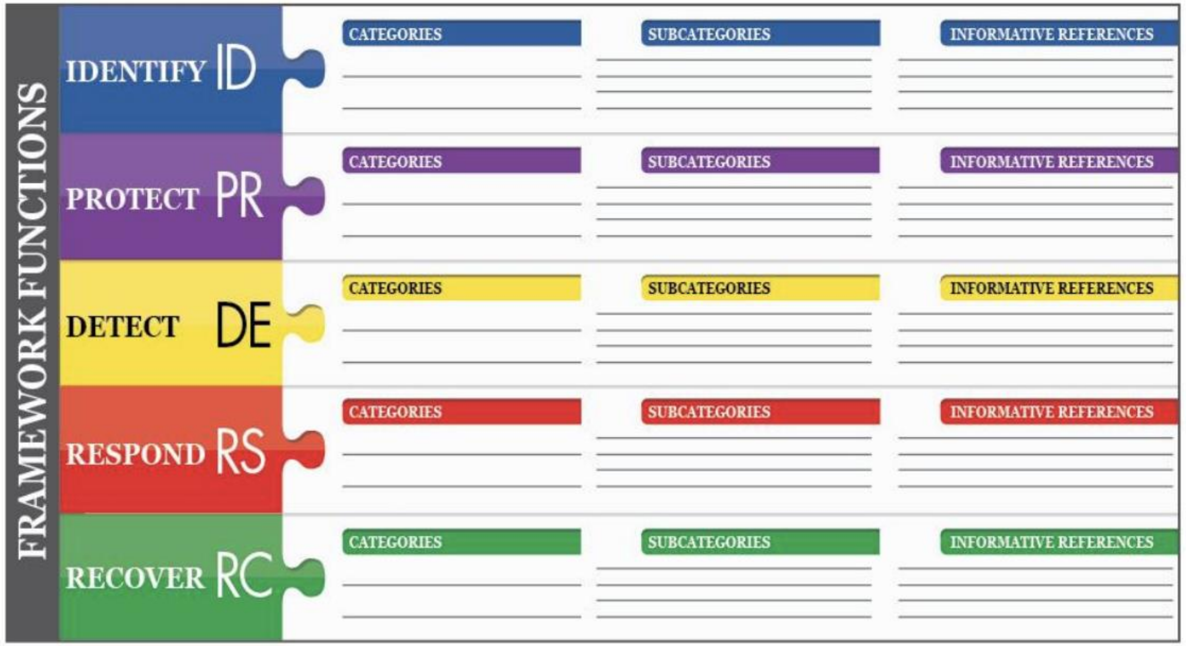
  - Selected **12 threats events** of high likelihood and high adverse impact


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

# THREAT EVENTS FROM NIST SP 1800-22

- TE-1: Privacy-intrusive application
- TE-2: Account credential theft through phishing
- TE-3: Malicious applications
- TE-4: Outdated phones
- TE-5: Camera and microphone remote access
- TE-6: Sensitive data transmissions
- TE-7: Brute force attacks to unlock a phone
- TE-8: Weak password practices protection
- TE-9: Unmanaged device protection
- TE-10: Lost or stolen data protection
- TE-11: Protecting data from being inadvertently backed up to a cloud service
- TE-12: PIN or password sharing protection

# CYBERSECURITY FRAMEWORK PROFILE



FRAMEWORK FUNCTIONS

IDENTIFY ID — CATEGORIES — SUBCATEGORIES — INFORMATIVE REFERENCES

PROTECT PR — CATEGORIES — SUBCATEGORIES — INFORMATIVE REFERENCES

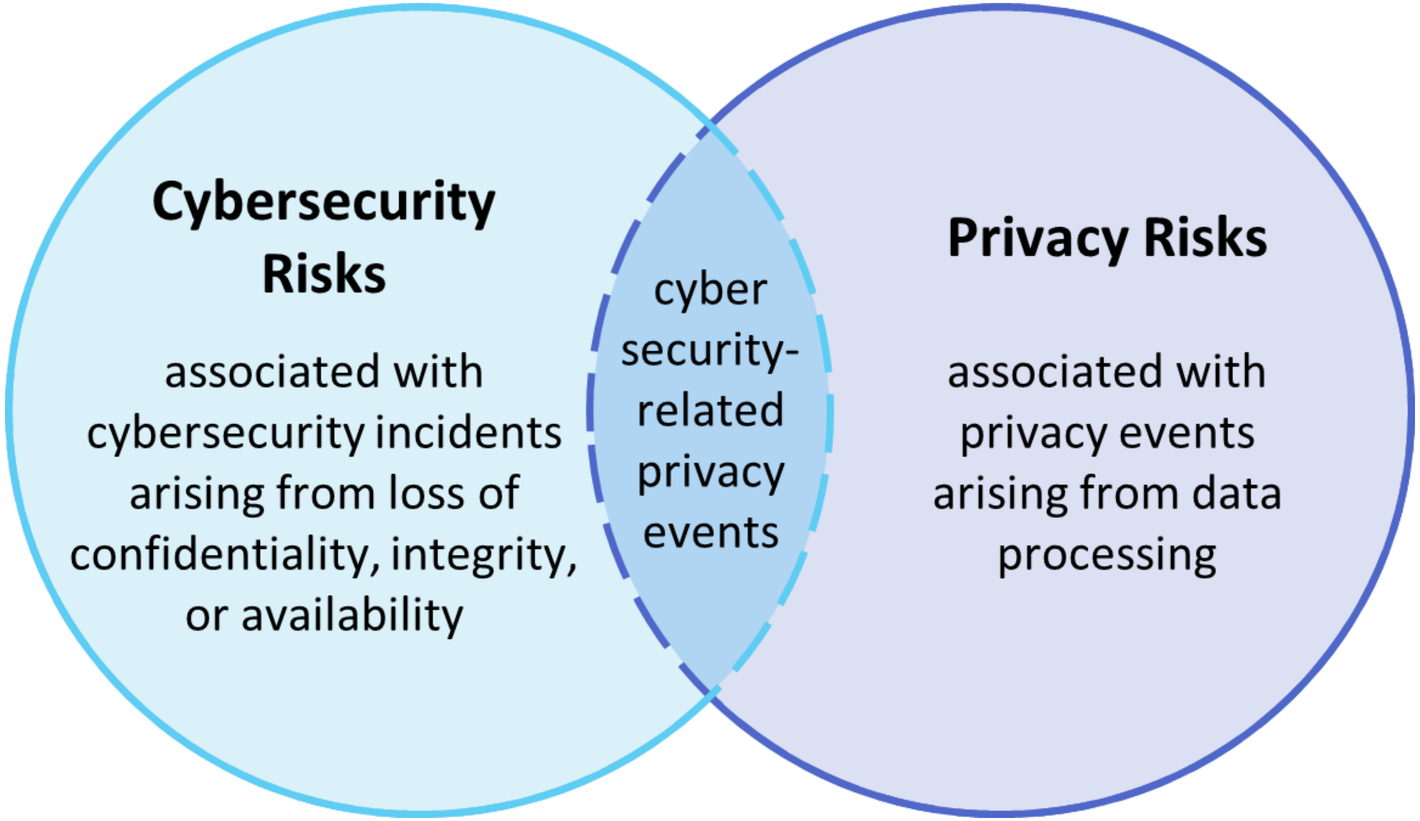
DETECT DE — CATEGORIES — SUBCATEGORIES — INFORMATIVE REFERENCES

RESPOND RS — CATEGORIES — SUBCATEGORIES — INFORMATIVE REFERENCES

RECOVER RC — CATEGORIES — SUBCATEGORIES — INFORMATIVE REFERENCES

- Identified the NIST’s Cybersecurity Framework as a useful tool :
  - To highlight and communicate high priority security expectations
  - To perform a self-assessment comparison of current risk management practices and target risk management goals

# CYBERSECURITY & PRIVACY INTERSECTION



Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cybersecurity-related privacy events
Privacy Risks
associated with privacy events arising from data processing

**Source:** *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, January 16, 2020.*
https://www.nist.gov/privacy-framework

# INTEGRATING PRIVACY INTO NCCOE SOLUTIONS

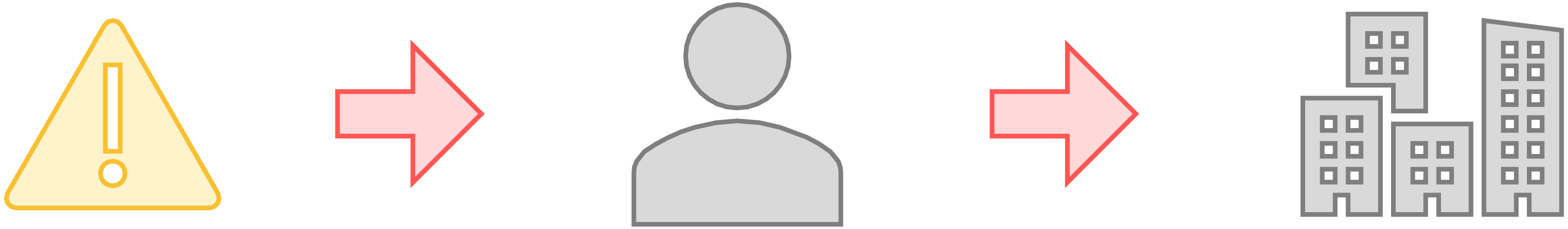
## Objectives

- Highlight the importance of privacy in this context
- Identify areas where the solution addresses privacy risk

## Applying NIST privacy guidance:

- Privacy Risk Assessment Methodology (PRAM)
- Catalog of Problematic Data Actions
- NIST Privacy Framework

# PRIVACY RISK AND ORGANIZATIONAL RISK



**Problem**

arises from data processing

**Individual**

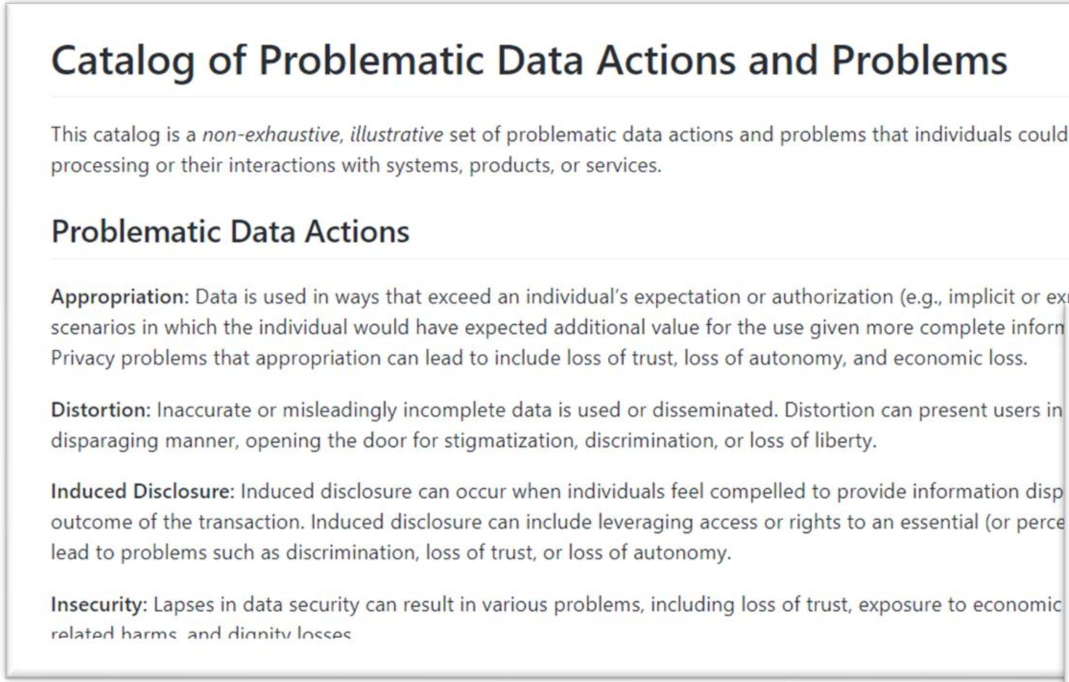
experiences direct impact
(e.g., embarrassment, discrimination, economic loss)

**Organization**

resulting impact
(e.g., customer abandonment, noncompliance costs, harm to reputation or internal culture)

**Reference:** *NIST Privacy Framework Webinar: Ready. Set. Adopt Version 1.0, January 29, 2020*

# NIST PRAM



## Catalog of Problematic Data Actions and Problems

This catalog is a *non-exhaustive, illustrative* set of problematic data actions and problems that individuals could experience as the result of data processing or their interactions with systems, products, or services.

### Problematic Data Actions

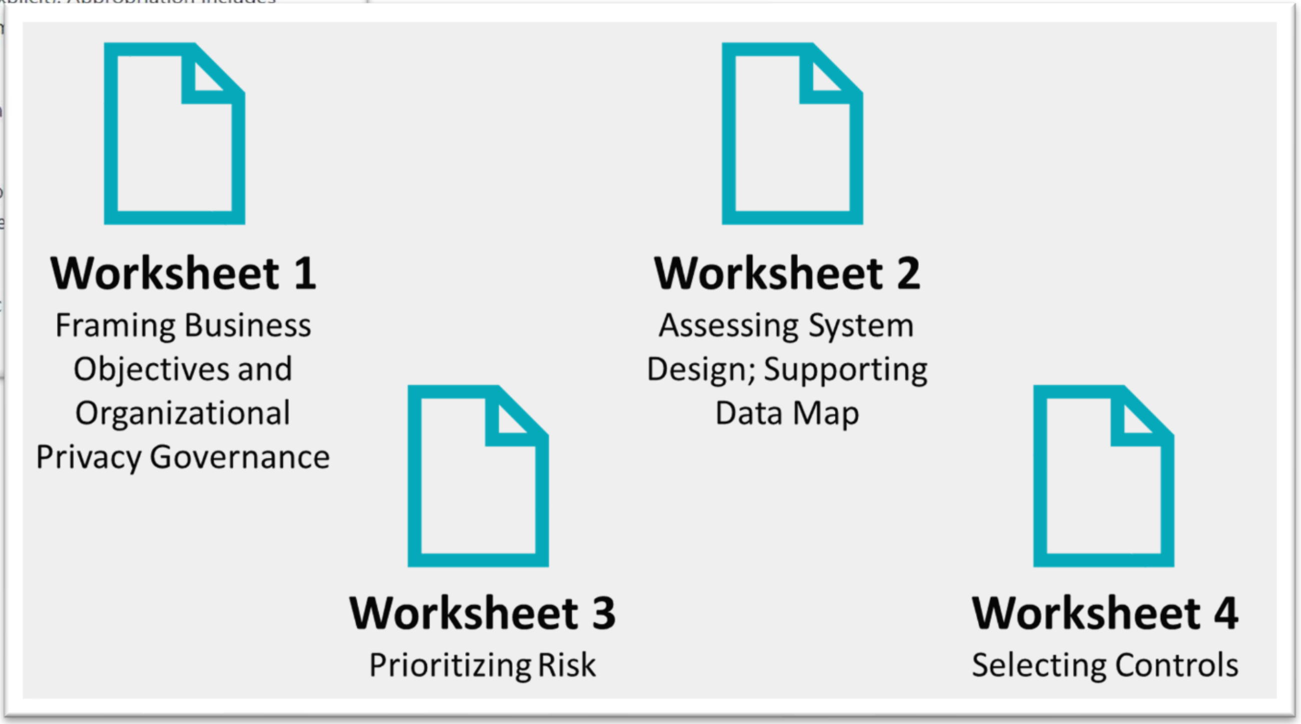
**Appropriation:** Data is used in ways that exceed an individual's expectation or authorization (e.g., implicit or explicit). Appropriation includes scenarios in which the individual would have expected additional value for the use given more complete inform
Privacy problems that appropriation can lead to include loss of trust, loss of autonomy, and economic loss.

**Distortion:** Inaccurate or misleadingly incomplete data is used or disseminated. Distortion can present users in
disparaging manner, opening the door for stigmatization, discrimination, or loss of liberty.

**Induced Disclosure:** Induced disclosure can occur when individuals feel compelled to provide information disp
outcome of the transaction. Induced disclosure can include leveraging access or rights to an essential (or perce
lead to problems such as discrimination, loss of trust, or loss of autonomy.

**Insecurity:** Lapses in data security can result in various problems, including loss of trust, exposure to economic
related harms, and dignity losses

Catalog of Problematic Data Actions and Problems Available at:
https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md



**Worksheet 1**
Framing Business Objectives and Organizational Privacy Governance

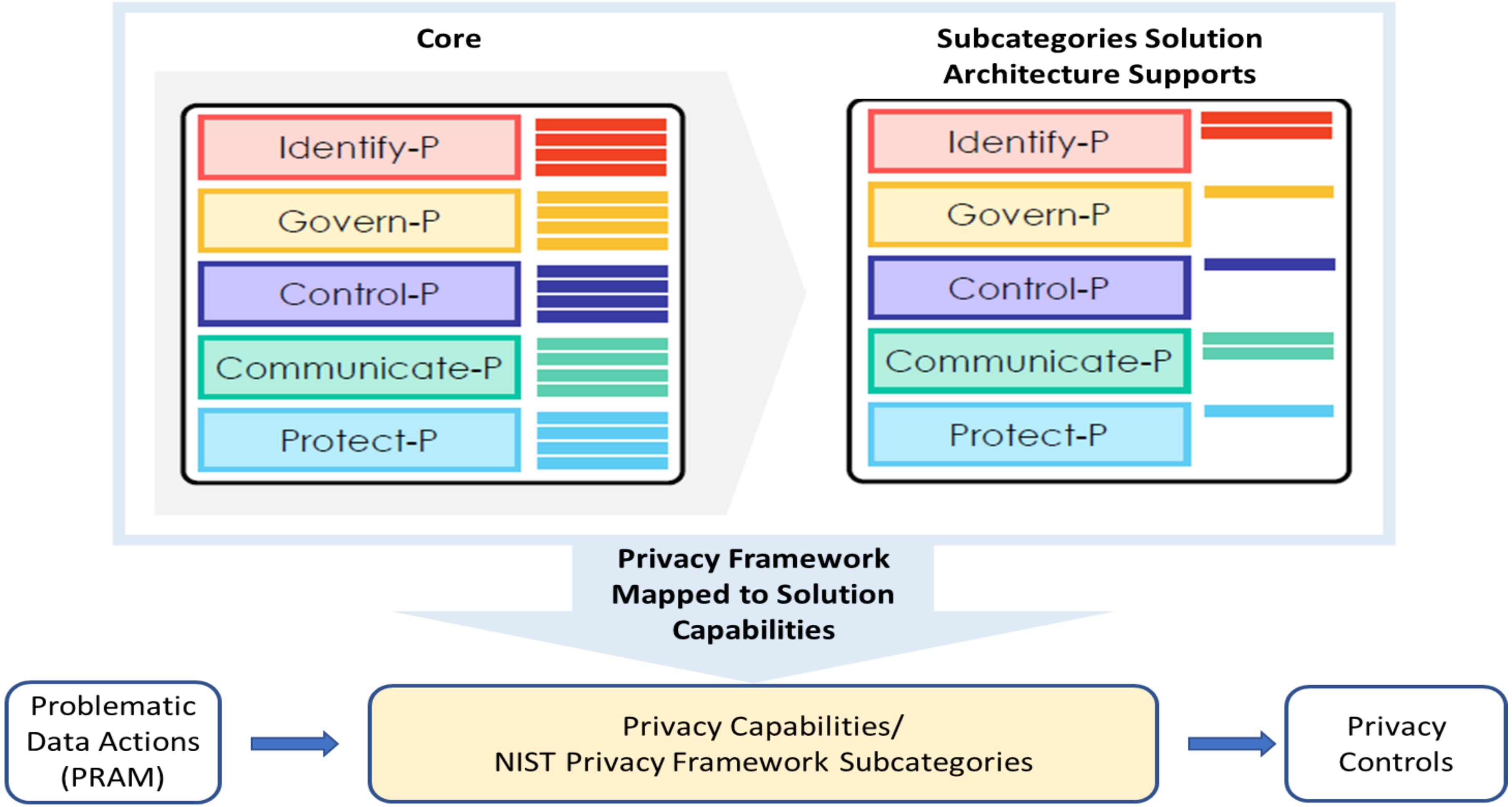
**Worksheet 2**
Assessing System Design; Supporting Data Map

**Worksheet 3**
Prioritizing Risk

**Worksheet 4**
Selecting Controls

PRAM Worksheets Available at: https://github.com/usnistgov/PrivacyEngCollabSpace/tree/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM

# 1800-22 PRIVACY APPROACH



Core

Identify-P

Govern-P

Control-P

Communicate-P

Protect-P

Subcategories Solution Architecture Supports

Identify-P

Govern-P

Control-P

Communicate-P

Protect-P

Privacy Framework Mapped to Solution Capabilities

Problematic Data Actions (PRAM)

Privacy Capabilities/
NIST Privacy Framework Subcategories

Privacy Controls

# PROBLEMATIC DATA ACTIONS FROM 1800-22

**Identified 3 problematic data actions in the solution that could result in privacy risk to individuals**

- Blocking access and wiping devices
- Employee monitoring
- Data sharing across parties

# EMPLOYEE MONITORING EXAMPLE

| Risk | Data Action | Problematic Data Actions and Example Privacy Events | How the Example Solution Architecture Helps Mitigate the PDA |
|---|---|---|---|
| Employees may feel as though they are being surveilled | The BYOD infrastructure comprehensively monitors device interactions related to enterprise connectivity and data processing. | **Problematic Data Action:** Surveillance<br>**Potential Problems for Individuals:** Monitoring BYOD resources on personal devices pro-vides a degree of visibility into personal devices that employers would not otherwise have, which in turn can result in the employer creating an incomplete narrative about employees that could lead to issues such as discrimination or employee loss of trust in the employer if the employee discovers unanticipated monitoring. Additionally, employees who connect their personal mobile device to the organization’s network may not be aware of the degree of visibility into their personal activities and data and may not want this to occur. For example, employers may be able to collect location information or application data that provides insights into employee health. | Restricts staff access to system capabilities that permit reviewing data about employees and their devices.<br>Limits or disables collection of specific data elements (e.g., location data). |

# QUESTION #6: YOUR THOUGHTS ON THE PRIVACY MATERIAL?

- Which aspects of the privacy content included in the guide will be most helpful to you?

- A: Mapping to the privacy controls in NIST SP 800-53
- B: Mapping to the Subcategories in the Privacy Framework
- C: Identification of Problematic Data Actions
- D: Discussion of privacy guidelines materials

# QUESTION #7: YOUR THOUGHTS ON THE PRIVACY MATERIAL?

- Which aspects of the PRAM will be most useful for evaluating risks for your solutions?

- A: Terms for describing privacy risk (Catalog of Problematic Data Actions and Problems)
- B: Step-wise process for identifying and evaluating risk and then selecting controls (PRAM worksheets)
- C: Inclusion of contextual considerations (e.g., business environment, privacy values and promises)

# SECURITY TECHNOLOGIES USED IN 1800-22

**Enterprise Mobility Management**

- Enforce policies and perform compliance actions

**Trusted Execution Environment**

- Verify the integrity of the device and ensure the confidentiality of data stored on persistent memory

**Virtual Private Network**

- Secure the connection between the mobile device and the enterprise network

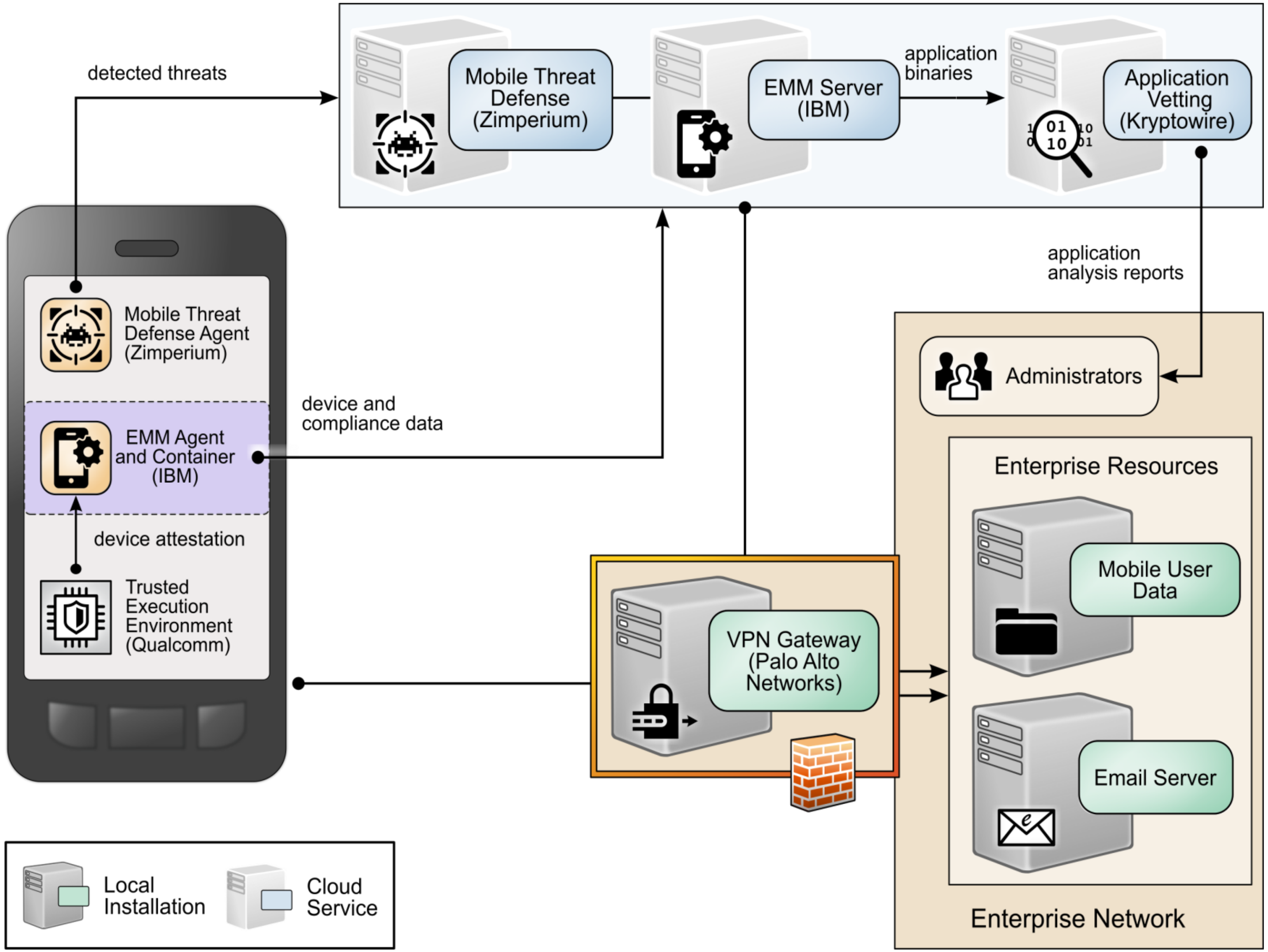
**Mobile Application Vetting Service**

- Determine if an application demonstrates any behaviors that pose a security or privacy risk

**Mobile Threat Defense**

- Analyze and inform the user of device-based threats, application-based threats, and network-based threats

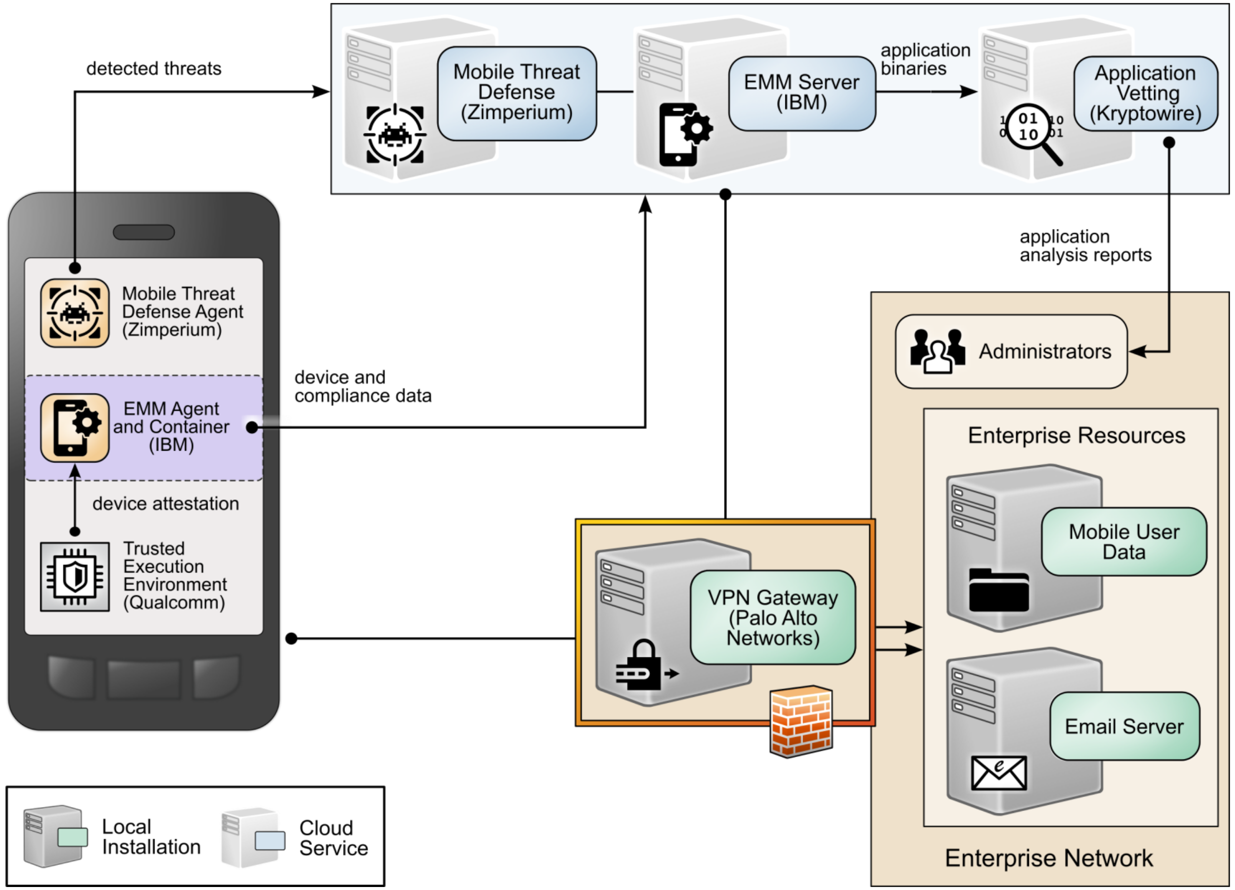
# NIST SP 1800-22, MOBILE DEVICE SECURITY: BRING YOUR OWN DEVICE EXAMPLE ARCHITECTURE


detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
01
10
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Enterprise Network
Local Installation
Cloud Service

# SOLVING THE CHALLENGE: EXAMPLE SOLUTION ARCHITECTURE

## The example solution uses technology available today*:

- **IBM** MaaS360 Mobile Device Management
- **Kryptowire** Application Vetting
- **Palo Alto Networks** Firewall and Virtual Private Network
- **Qualcomm** Trusted Execution Environment
- **Zimperium** Mobile Threat Defense



detected threats
Mobile Threat Defense (Zimperium)
EMM Server (IBM)
application binaries
Application Vetting (Kryptowire)
application analysis reports
Mobile Threat Defense Agent (Zimperium)
EMM Agent and Container (IBM)
device and compliance data
device attestation
Trusted Execution Environment (Qualcomm)
Administrators
Enterprise Resources
Mobile User Data
VPN Gateway (Palo Alto Networks)
Email Server
Enterprise Network
Local Installation
Cloud Service

*Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

# NIST SP 1800-22, MOBILE DEVICE SECURITY: BRING YOUR OWN DEVICE (BYOD)'S EXAMPLE SOLUTION ARCHITECTURE BENEFITS

- **Reduces security and privacy risk.** Organizations can increase the security & privacy across their mobile enterprise systems by using risk mitigation technologies and applying privacy protections to help reduce mobile device security risks.

- **Demonstrates enterprise-wide application.** Shows how organizations can deploy a variety of mobile enterprise management technologies to networks, devices, and applications.

- **Applies cybersecurity standards and best practices.** Provides an illustration of how the NIST Risk Management Framework, the Cybersecurity Framework, and the Privacy Framework can be applied to strengthen an enterprise's mobility.

# QUESTION #8: HOW USEFUL WILL 1800-22 BE FOR YOU?

- Having heard about the NIST SP 1800-22, Mobile Device Security: Bring Your Own Device (BYOD) publication today, do you think the publication would be helpful to improve your mobile device infrastructure?

- A Yes, we can use most of the guide
- B Yes, we can use parts of it
- C No

# Your Feedback!

# QUESTION #9: FUTURE TOPICS YOU WOULD LIKE ADDRESSED

- What other topic(s) would be helpful to include in future guides?

- A: Thin client / Virtual Mobile Infrastructure
- B: Unified Endpoint Management - desktop / laptop Management
- C: Wearable internet of things security and privacy guidance for use in the enterprise
- D: Telework guidance
- E: Other (type into the chat window)

# MOVING FORWARD IN 2021

## Potential Build 3 Topics

- Virtual Mobile Infrastructure *(as a supplement to BYOD guide - not as a build)*

## Potential Webinar Topics

- **Share current mobile device security work and discuss future topic areas**
- Privacy-focused discussion about mobile device deployment implementations
- Vendor Panel – Discussing the current mobile landscape and the capabilities available to address threats to mobile devices
- Threat specific discussions:
  - Preventing phishing attacks and spyware installations on BYOD devices
  - Identifying compromised organizational or personal mobile devices
  - Protecting employee health information while helping companies manage future health risks in the workplace
- Other topics?

Email us your ideas at mobile-nccoe@nist.gov

# GET INVOLVED

Share a Project Idea

Discuss Challenges

Contribute to Publications

Participate in a Project

Join a Community of Interest

# Mobile Device Security Project Team

mobile-nccoe@nist.gov

nccoe.nist.gov

@NISTcyber