

NIST SPECIAL PUBLICATION 1800-22A

Mobile Device Security: Bring Your Own Device (BYOD)

**Volume A:
Executive Summary**

**Kaitlin Boeckl
Nakia Grayson
Gema Howell
Naomi Lefkovitz**

Applied Cybersecurity Division
Information Technology Laboratory

**Jason G. Ajmo
Milissa McGinnis*
Kenneth F. Sandlin
Oksana Slivina
Julie Snyder
Paul Ward**

The MITRE Corporation
McLean, VA

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

March 2021

DRAFT

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



1 Executive Summary

2 Many organizations now provide employees the flexibility to use their personal mobile devices to
3 perform work-related activities. An ineffectively secured personal mobile device could expose an
4 organization or employee to data loss or a privacy compromise. Ensuring that an organization's data is
5 protected when it is accessed from personal devices poses unique challenges and threats.

6 Allowing employees to use their personal mobile devices for work-related activities is commonly known
7 as a bring your own device (BYOD) deployment. A BYOD deployment offers a convenient way to
8 remotely access organizational resources, while avoiding the alternative of carrying both a work phone
9 and personal phone. This NIST Cybersecurity Practice Guide demonstrates how organizations can use
10 standards-based, commercially available products to help meet their BYOD security and privacy needs.

11 CHALLENGE

12 BYOD devices can be used interchangeably for
13 work and personal purposes throughout the day.
14 While flexible and convenient, BYOD can introduce
15 challenges to an enterprise. These challenges can
16 include additional responsibilities and complexity
17 for information technology (IT) departments

18 caused by supporting many types of personal mobile devices used by the employees, enterprise security
19 threats arising from unprotected personal devices, as well as challenges protecting the privacy of
20 employees and their personal data stored on their mobile devices.

An ineffectively secured personal mobile device could expose an organization or employee to data loss or a privacy compromise






21 SOLUTION

22 The National Cybersecurity Center of Excellence (NCCoE) collaborated with the mobile device
23 community and cybersecurity technology providers to build a simulated BYOD environment. Using
24 commercially available products, the example solution's technologies and methodologies can enhance
25 the security posture of the adopting organization and help protect employee privacy and organizational
26 information assets.

This practice guide can help your organization:

- **protect data** from being accessed by unauthorized persons when a device is stolen or misplaced
- **reduce risk to employees** through enhanced privacy protections
- **improve the security of mobile devices and applications** by deploying mobile device technologies
- **reduce risks to organizational data** by separating personal and work-related information from each other
- **enhance visibility** into mobile device health to facilitate identification of device and data compromise, and permit efficient user notification
- **leverage industry best practices** to enhance mobile device security and privacy

27 The example solution uses technologies and security capabilities (shown below) from our project
28 collaborators. The technologies used in the solution support security and privacy standards and
29 guidelines including the NIST Cybersecurity Framework and NIST Privacy Framework, among others.
30 Both iOS and Android devices are supported by this guide’s example solution.

Collaborator	Security Capability or Component
	Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance
	Application Vetting to determine if an application demonstrates behaviors that could pose a security or privacy risk
	Firewall and Virtual Private Network that controls network traffic and provides encrypted communication channels between mobile devices and other hosts
	Trusted Execution Environment that helps protect mobile devices from computer code with integrity issues
	Mobile Threat Defense detects unwanted activity and informs the device owner and BYOD administrators to prevent or limit harm that an attacker could cause

31 While the NCCoE used a suite of commercial products to address this challenge, this guide does not
32 endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your
33 organization's information security experts should identify the products that will best integrate with
34 your existing tools and IT system infrastructure. Your organization can adopt this solution or one that
35 adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and
36 implementing parts of a solution.

37 HOW TO USE THIS GUIDE

38 Depending on your role in your organization, you might use this guide in different ways:

39 **Business decision makers, including chief information security and technology officers** can use this
40 part of the guide, *NIST SP 1800-22a: Executive Summary*, to understand the impetus for the guide, the
41 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could
42 benefit your organization.

43 **Technology, security, and privacy program managers** who are concerned with how to identify,
44 understand, assess, and mitigate risk can use the following:

- 45 • *NIST SP 1800-22b: Approach, Architecture, and Security Characteristics*, which describes what
46 we built and why, the risk analysis performed, and the security/privacy control mappings.

- 47 • *NIST SP 1800-22 Supplement: Example Scenario: Putting Guidance into Practice*, which provides
48 an example of a fictional company using this practice guide and other NIST guidance to
49 implement a BYOD deployment with their security and privacy requirements.

50 **IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-22c: How-*
51 *To Guides*, which provides specific product installation, configuration, and integration instructions for
52 building the example implementation, allowing you to replicate all or parts of this project.

53 **SHARE YOUR FEEDBACK**

54 You can view or download the guide at [https://www.nccoe.nist.gov/projects/building-blocks/mobile-](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device)
55 [device-security/bring-your-own-device](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device). Help the NCCoE make this guide better by sharing your thoughts
56 with us. If you adopt this solution for your own organization, please share your experience and advice
57 with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so
58 we encourage organizations to share lessons learned and best practices for transforming the processes
59 associated with implementing this guide.

60 To provide comments or to learn more by arranging a demonstration of this example implementation,
61 contact the NCCoE at mobile-nccoe@nist.gov.

62

63 **COLLABORATORS**

64 Collaborators participating in this project submitted their capabilities in response to an open call in the
65 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
66 and integrators). Those respondents with relevant capabilities or product components signed a
67 Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to
68 build this example solution.

69 Certain commercial entities, equipment, products, or materials may be identified by name or company
70 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
71 experimental procedure or concept adequately. Such identification is not intended to imply special
72 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
73 intended to imply that the entities, equipment, products, or materials are necessarily the best available
74 for the purpose.