

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 was done while at employer.*

July 2019

DRAFT

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



1 Executive Summary

- 2 ▪ Mobile devices provide access to workplace data and resources that are vital for organizations
3 to accomplish their mission while providing employees the flexibility to perform their daily
4 activities. Securing these devices is essential to the continuity of business operations.
- 5 ▪ While mobile devices can increase organizations' efficiency and employee productivity, they can
6 also leave sensitive data vulnerable. Addressing such vulnerabilities requires mobile device
7 management tools to help secure access to the network and resources. These tools are different
8 from those required to secure the typical computer workstation.
- 9 ▪ To address the challenge of securing mobile devices while managing risks, the National
10 Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and
11 Technology (NIST) built a laboratory environment to explore how various mobile security
12 technologies can be integrated within an enterprise's network.
- 13 ▪ This NIST Cybersecurity Practice Guide demonstrates how organizations can use standards-
14 based, commercially available products to help meet their mobile device security and privacy
15 needs.

16 CHALLENGE

17 Mobile devices are a staple within modern workplaces. As employees use these devices to perform
18 everyday enterprise tasks, organizations are challenged with ensuring that devices regularly process,
19 modify, and store sensitive data securely. These devices bring unique threats to the enterprise and
20 should be managed in a manner distinct from traditional desktop platforms. This includes securing
21 against different types of network-based attacks on mobile devices that have an always-on connection
22 to the internet.

23 Managing the security of workplace mobile devices and minimizing the risk posed can be challenging
24 because there are many mobile device security tools available. Proper implementation is difficult to
25 achieve for an end user because the method of implementation varies considerably from tool to tool. In
26 addition, unfamiliarity with the threats to mobile devices can further compound these implementation
27 difficulties.

28 SOLUTION

29 To address the challenge of securing mobile devices within an enterprise, NIST built an example solution
30 in a lab environment at the NCCoE to demonstrate mobile management tools that enterprises can use
31 to secure their networks. These technologies are configured to protect organizational assets and end-
32 user privacy, providing methodologies to enhance the security and privacy posture of the adopting
33 organization.

34 Both Apple iOS and Android devices are used in the example solution, which includes detailed device
35 configurations and enterprise mobility management policies provisioned to the devices. The foundation
36 of this architecture is based on federal U.S. guidance, including that from NIST 800 series publications,
37 National Information Assurance Partnership, U.S. Department of Homeland Security, and the Federal

38 Chief Information Officers Council. These standards, best practices, and certification programs help
39 ensure the confidentiality and integrity of enterprise data on mobile systems.

40 This guide provides:

- 41 ▪ a detailed example solution and capabilities that address risk and implementation of security
42 controls
- 43 ▪ a demonstration of the approach using commercially available products
- 44 ▪ how-to instructions for implementers and security engineers, with instructions on integrating
45 and configuring the example solution into their organization's enterprise in a manner that can
46 achieve security goals with minimum impact on operational processes

47 The NCCoE sought existing technologies that provided the following capabilities:

- 48 ▪ enhanced protection of data that resides on the mobile device
- 49 ▪ centralization of management systems to deploy policies and configurations to devices
- 50 ▪ ability to evaluate the security of mobile applications
- 51 ▪ inhibition of the eavesdropping of mobile device data when traversing a network
- 52 ▪ privacy settings that protect end-user data
- 53 ▪ protection from phishing attempts

54 Commercial, standards-based products such as the ones we used are readily available and interoperable
55 with existing information technology (IT) infrastructure and investments.

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

62 **BENEFITS**

63 The NCCoE's practice guide *Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)* can
64 help your organization:

- 65 ▪ reduce adverse effects on the organization if a device is compromised
- 66 ▪ reduce capital investment by embracing modern enterprise mobility models
- 67 ▪ apply robust, standards-based technologies using industry best practices
- 68 ▪ reduce privacy risks to users through privacy protections
- 69 ▪ provide users with enhanced protection against loss of personal and business data when a
70 device is stolen or misplaced
- 71 ▪ deploy enterprise management technologies to improve the security of enterprise networks,
72 devices, and applications

- 73 ▪ reduce risk so that employees can access the necessary data from nearly any location, using a
74 wide selection of mobile devices and networks
- 75 ▪ enhance visibility for system administrators into mobile security events, quickly providing
76 notification and identification of device and data compromise
- 77 ▪ implement government standards for mobile security

78 **SHARE YOUR FEEDBACK**

79 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/enterprise)
80 [device-security/enterprise](https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise). Help the NCCoE make this guide better by sharing your thoughts with us as
81 you read the guide. If you adopt this solution for your own organization, please share your experience
82 and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our
83 solution, so we encourage organizations to share lessons learned and best practices for transforming the
84 processes associated with implementing this guide.

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

87 **TECHNOLOGY PARTNERS/COLLABORATORS**

88 Organizations participating in this project submitted their capabilities in response to an open call in the
89 Federal Register for all sources of relevant security capabilities from academia and industry (vendors
90 and integrators). The following respondents with relevant capabilities or product components (identified
91 as “Technology Partners/Collaborators” herein) signed a Cooperative Research and Development
92 Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.



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

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses’ most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit <http://www.nccoe.nist.gov>
nccoe@nist.gov
301-975-0200