The rapid pace at which mobile technologies evolve requires regular re-evaluation of a mobility program to ensure it is accomplishing its security, privacy, and workplace functionality. Built-in mobile protections may not be enough to fully mitigate the security challenges associated with mobile information systems. Usability, privacy, and regulatory requirements each influence which mobile security technologies and security controls are going to be well-suited to meet the needs of an organization’s mobility program.

The goal of the Mobile Device Security: Corporate-Owned Personally-Enabled (COPE) project is to provide an example solution demonstrating how organizations can use a standards-based approach and commercially available technologies to meet their security needs for using mobile devices to access enterprise resources.

The sample solution details tools for an enterprise mobility management (EMM) capability located on-premises, mobile threat defense (MTD), mobile threat intelligence (MTI), application vetting, secure boot/image authentication, and virtual private network (VPN) services.

This practice guide can help your organization:
- reduce adverse effects on the organization if a device is compromised
- reduce capital investment by embracing modern enterprise mobility models
- apply robust, standards-based technologies using industry best practices
- reduce privacy risks to users through privacy protections
- provide users with enhanced protection against loss of personal and business data when a device is stolen or misplaced
- deploy enterprise management technologies to improve the security of enterprise networks, devices, and applications
- reduce risk so that employees can access the necessary data from nearly any location, using a wide selection of mobile devices and networks
- enhance visibility for system administrators into mobile security events, quickly providing notification and identification of device and data compromise
- implement government standards for mobile security

This project is the first in a series of builds that will focus on Mobile Device Security for Enterprises. The second build, Mobile Device Security: Bring Your Own Device (BYOD), is in development.
**HIGH-LEVEL ARCHITECTURE**

The specific architecture of each build varies based on the necessary enterprise services and management technology in use. Each build will use network-based confidentiality protection mechanisms, such as a Virtual Private Network. Additionally, device-side security mechanisms will be utilized to identify known vulnerabilities and mobile malware. Enterprise Mobility Management (EMM) policy sets will be created, and then tailored to an individual user’s risk profile in accordance with established best practices. Each MDSE build will include the following:

- an example risk assessment using an established methodology (e.g., NIST SP 800-37, Cybersecurity Framework)
- installation and configuration instructions for a variety of mobile security technologies, such as an enterprise mobility management system, virtual mobile infrastructure, application vetting, or mobile threat defense
- a set of mobile security controls, mapped to a variety of industry and government standards (e.g., ISO, NIST, NIAP)

These processes and technologies will enable users to work inside and outside the corporate network, while mitigating threats posed from across the mobile ecosystem.

The technology vendors who are participating in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

- apthority
- kryptowire
- Lookout
- Mobileiron
- paloalto
- Qualcomm

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.

**DOWNLOAD THE PUBLISHED DRAFT**

For more information about this project, visit: https://nccoe.nist.gov/projects/building-blocks/mobile-device-security/corporate-owned-personally-enabled.

**HOW TO PARTICIPATE**

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this project, please email mobile-nccoe@nist.gov.