CAPACITY ENHANCEMENT GUIDE

Mobile Device Cybersecurity Checklist for Organizations

November 2021

OVERVIEW

CISA has created this Enterprise Mobility Management (EMM) system checklist to assist your organization in mitigating vulnerabilities and increasing enterprise protection. Enterprise-managed mobile devices face threats from a wide variety of sources. Implementing the following best practices will enable your organization to provide your employees with secure mobile access to enterprise resources.

Audience and Scope

The measures described in this guidance focus on various easy-to-implement steps organizations can take to improve the cybersecurity of their enterprise-managed mobile devices. **Note:** for additional guidance tailored for—but not limited to—federal enterprise-managed mobile devices, see the National Security Agency publication Mobile Device Best Practices.

SECURITY-FOCUSED DEVICE MANAGEMENT

- ☐ **Select devices.** Select devices that meet enterprise requirements with a careful eye on supply chain risks.
- ☐ **Update platforms.** Enable your Mobile Device Management (MDM) system's automatic update feature to ensure the latest updates are applied as soon as they are available.
  - Operating system (OS) updates include new/updated features that help protect privacy, enhance security, and fix flaws that leave devices vulnerable to attack by malicious actors.
- ☐ **Require devices to be trusted.** Trusted devices have the following characteristics:
  - Updated to the latest platform patch level.
  - Properly configured by EMM to enterprise standards.
  - Not jailbroken or rooted.
  - Continuously monitored through the EMM system.

  If *any* of these conditions are not met, the device is "untrusted" and should not have access to enterprise resources.
- ☐ **Deny access to untrusted devices.** Devices should be considered untrusted and denied access to enterprise resources unless they meet all of the above criteria.

USE STRONG AUTHENTICATION

- ☐ **Enable device authentication.** Enforce strong login passwords/PINs for the device; PINs should be at least six digits. For maximum protection, enable the use of biometric authentication (face or fingerprint).
- ☐ **Enable two-factor authentication.** Enable two-factor authentication (2FA) for access to enterprise networks. 2FA options pair a password or PIN with another form of authentication, such as a rotating passcode, SMS message, or biometric input.

PRACTICE GOOD APP SECURITY

- ☐ **Use curated app stores**. Disable third-party app stores, which are common vectors for the spread of malware.
- ☐ **Isolate enterprise apps.** Use security container technology to isolate enterprise data. Your organization's EMM should be configured to prevent data exfiltration between enterprise apps and personal apps.
- ☐ **Minimize PII in all apps.** Limit the amount of personally identifiable information (PII) in apps. If an app does not store or have access to PII, it is much more difficult for malicious actors to leak or steal the data.
- ☐ **Restrict permissions.** Disable any sensitive permissions (such as camera, location) by default when installing apps.
- ☐ **Ensure app vetting strategy for enterprise-developed applications.**
- ☐ **Restrict OS/app synchronization.** Prevent data leakage of sensitive enterprise information by restricting the backing up of enterprise data by OS/app-synchronization.

PROTECT NETWORK COMMUNICATIONS

- ☐ **Disable unneeded network radios (BT, NFC, Wi-Fi, GPS).** Every network connection to a device is a potential point of entry that can be exploited to exfiltrate data, attack a device, or even surreptitiously gain control over the device.
    - Disabling Bluetooth, Wi-Fi, and NFC when they are not in use can reduce the opportunity for malicious actors to attack a device.
    - Disabling the GPS radio and related location services protects the user's privacy regarding location.
- ☐ **Disable user certificates.** User certificates not issued by the organization should be considered untrusted because malicious actors can craft malformed or malicious certificates to facilitate attacks on devices, such as intercepting communications.
- ☐ **Use secure communication apps and protocols.** Many network-based attacks allow the attacker to intercept and/or modify data in transit—resulting in leaks of PII, theft of credentials, tracking of a user's location and activities, and more. Configure the EMM to use VPNs between the device and the enterprise network.

PROTECT THE DEVICE

- ☐ **Utilize a Mobile Threat Defense (MTD) system.** An MTD can protect a device from a variety of malicious software that can compromise apps and operating systems, and can extract sensitive data. Additionally, an MTD can detect improper configurations.
- ☐ **Charge device with trusted chargers and cables.** A malicious charger or PC can introduce malware, enabling an attacker to circumvent protections and take control of the device.
    - Issue trusted chargers and cables to employees and instruct them to only use those items to charge their devices.
    - Configure organization-provided devices to use USB restricted mode, which disables data transfer between the phones and USB devices.
- ☐ **Enable lost device function.** Configure settings to automatically wipe the device's data after a certain number of incorrect login attempts (e.g., 10), and enable the option to remotely wipe the device.

PROTECT ENTERPRISE SYSTEMS FROM THE DEVICE

- ☐ **Do not allow mobile devices to connect to critical systems.** Infected mobile devices can introduce malware to business-critical ancillary systems such as enterprise PCs, servers, or operational technology systems.
    - Instruct users to never connect mobile devices to critical systems via USB or wireless. Also, configure the EMM to disable these capabilities.