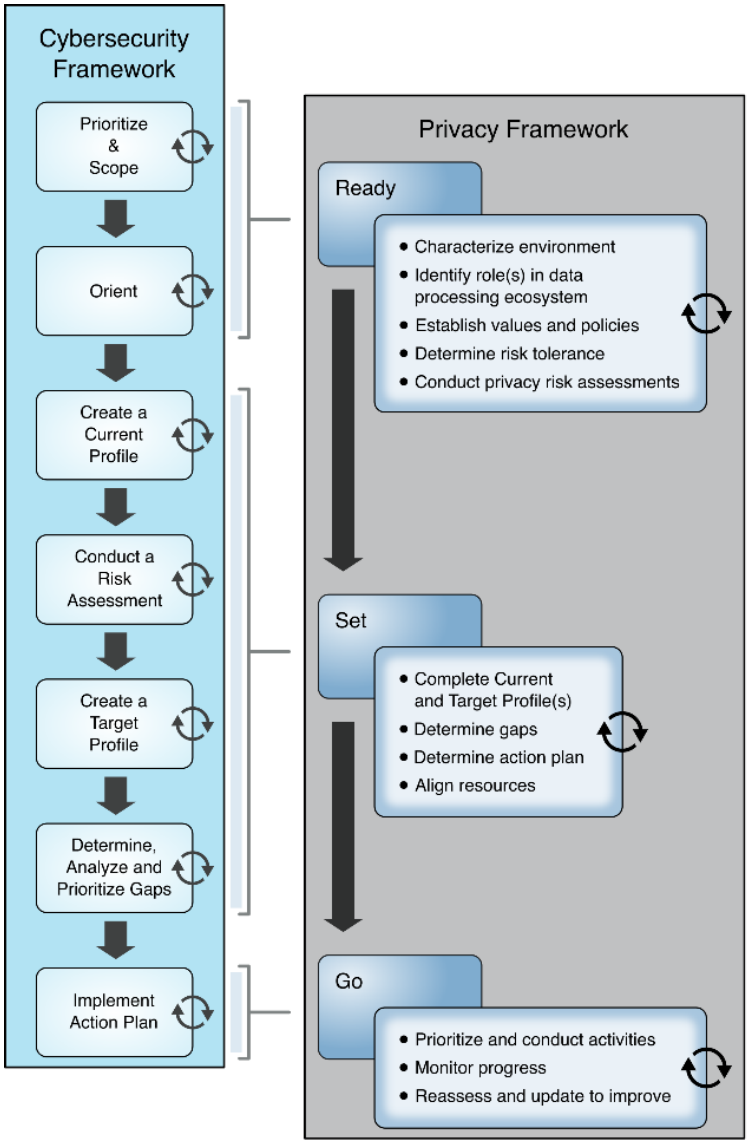
Mobile Device Security

Privacy: Bring Your Own Device (BYOD)

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is addressing the challenge of protecting an organization's information when accessed by Bring Your Own Device (BYOD) solutions. The NCCoE developed an example solution to help protect the security and privacy of employees through collaborative efforts with industry and the information technology community, including vendors of cybersecurity solutions.

Background

Many organizations now authorize employees to use their personal mobile devices to perform work-related activities. To help organizations address security and privacy risks when implementing these solutions, we published NIST Cybersecurity Practice Guide Special Publication 1800-22, *Mobile Device Security: Bring Your Own Device*.



Challenge

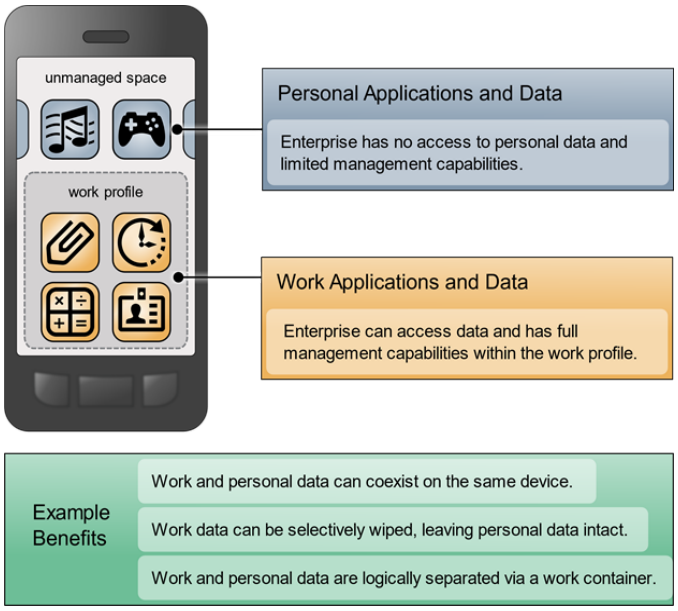
Some of the features that make personal mobile devices increasingly flexible and functional present unique privacy-related challenges for individuals. BYOD capabilities can introduce new privacy risks to employees by providing their employer a degree of access to their personal devices, opening the possibility of privacy challenges that would not otherwise exist.

The NCCoE examined three major privacy challenges:

- **Personal device resetting**. Devices can be wiped and reset to factory settings. When devices are wiped this can result in loss of personal data.
- **Personal device visibility**. The presence of BYOD capabilities on a personal device can provide a degree of visibility into those devices that employers would not otherwise have.
- **Personal data sharing**. Data about individuals and their devices can flow between various applications and analytical tools that may be part of the organization's BYOD solution. This may result in revealing device and personal information to employers and third parties.

Example Solution Goals

- **Personal data protection**. Ensure employee personal data is not deleted by having the organization only uninstall work applications and data, if necessary.
- **Data separation**. Separate organizational and personal information by restricting data flow between organizationally managed and unmanaged applications and prevent sensitive data from crossing between work and personal contexts.
- **Reduce information sharing**. Limit organizational and third party access to application and location information.



Benefits

To help organizations benefit from BYOD's flexibility while addressing critical privacy challenges from its implementation, this NIST Cybersecurity Practice Guide provides several types of information. These include Cybersecurity Framework and Privacy Framework mappings, as well as an example solution that can help protect the privacy of employees by:

- safeguarding access to personal photos, documents, and other data (including from the organization)
- separating work and personal data while simultaneously meeting an organization's objectives for business functions, usability, security, and employee privacy
- providing concise and understandable information about what data is collected and what actions are allowed and disallowed on personal devices.

The technology vendors who participated 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:

IBM Kryptowire Palo Alto Networks Qualcomm Zimperium

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.

HOW TO PARTICIPATE

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

DOWNLOAD THE DRAFT PRACTICE GUIDE

For more information about this project and to download the NIST Cybersecurity Practice Guide Special Publication 1800-22, *Mobile Device Security: Bring Your Own Device* practice guide, visit: https://www.nccoe.nist.gov/projects/building-blocks/mobile-device-security/bring-your-own-device.