BUSINESS PAPER

Enabling Federal Mobility via NTSWG-approved Hardware-Based Security, Device Monitoring, and Device Management

How Fulcrum Secure Mobility Platform meets National Nuclear Security Administration requirements, enabling mobile device use in sensitive and secure spaces.

PRIVORO®

Background

Mobile devices pose significant risks to National Security Systems in limited and secure spaces, resulting in stringent security policies that have essentially banned their use. However, bans impact the operational and productivity benefits of mobile technology while also colliding with the always-connected expectation of a modern workforce.

Policy directives affecting Department of Energy labs within the National Nuclear Security Administration

- **Committee on National Security Systems**

  CNSS Directive No. 510: Directive on the Use of Mobile Devices Within Secure Spaces

- **National Nuclear Security Administration**

  NNSA SD 470.6: Supplemental Directive on the Use of Mobile Devices Within Secure Spaces

These directives include requirements to secure and monitor smartphone cameras and microphones to prevent adversarial surveillance, also known as Mobile Hardening.

Meeting Mobile Hardening Requirements

SafeCase is a smartphone-coupled security device that protects against illicit camera and microphone use, even if the smartphone has been hacked.

Audio Masking

Random noise is fed into each of the smartphone's microphones to protect the content of conversations, the identity of speakers, and that conversations are occurring in the vicinity of the mobile device.

Camera Blocking

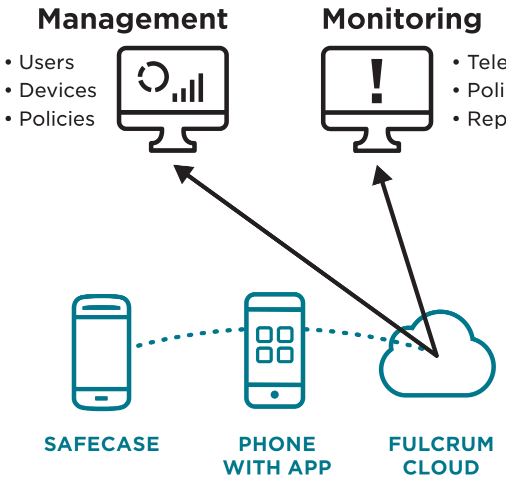
Physical barriers cover all smartphone cameras to prevent intruders from observing or recording visual data in the device's vicinity.

SafeCase, when paired with a consumer off-the-shelf mobile device, is the only NTSWG-approved solution enabling these devices in secure spaces.

Meeting Directive Requirements for Monitoring and Compliance

The Fulcrum Secure Mobility Platform ensures SafeCase-paired mobile devices are compliant with mobile hardening policy.

The Fulcrum Portal is how a system administrator interacts with the Fulcrum Cloud, allowing user, device and policy management. The SafeCase, through the paired phone's Fulcrum app, securely sends SafeCase telemetry to the Fulcrum Cloud, which is monitored and analyzed for compliance.



FULCRUM PLATFORM

Understanding the Fulcrum Portal and Required Functions for Directive Compliance

The Fulcrum Portal provides a suite of administrative features. Management and monitoring functions meet policy requirements.

MANAGEMENT

User management

- Manage users and groups of users

Device management

- Assign devices to users
- Create groups of devices
- Manage devices and groups of devices
- Remote firmware updates

Policy management

- Manage and configure policies
  - Set conditions for required SafeCase protection of mobile devices
- Assign policies to individual devices, users, or groups of devices or users

Customer Support

MONITORING

Secure collection and transmission of telemetry data

Monitor SafeCase telemetry data

- Phone connectivity status and type (e.g., if the protected phone is using a WiFi or cellular connection)
- Battery status
- Mic/camera protection status

View historical reports

For more information on Fulcrum Portal features and functions, contact your Privoro administrator.