The Future of Secure Work:
How to Enable the Secure Workforce of the Future Through Secure Mobility

White Paper Annex 4
How to Enable the Workforce of the Future through Mobile Signature Management

ATARC Future of Secure Work Working Group

June 2024

ATARC

Advanced Technology Academic Research Center

ATARC would like to take this opportunity to recognize the following Future of Secure Work Working Group members for their contributions:

Mark Gorak, *U.S. Department of Defense*

Heather McMahon, *Privoro*

Jose Moreno, *U.S. Department of State*

Mike Burr, *Social Mobile*

Muddasar Ahmed, *MITRE*

Brian Egenrieder, *SyncDog*

Michael Epley, *Red Hat*

Lt. Col. Jamie J. Johnson, *U.S. Space Force*

Pat Pulliam, *Blackberry*

Michael Schellhammer, *Artemist Advisory* Group

Randy Siegel, *Center Circle Consultants*

Sabina Aguon, *U.S. Department of Defense*

Bob Bauman, *Trusted Systems*

John Cavanaugh, *Internet Infrastructure Services Corporation*

Patricia Fisher, *Janus Associates*

Adam Flasch, *State of Maryland*

Michael Hudson, *Clearforce, Inc*

Ethan Kwan, U.S. *Department of State*

Nnake Nweke, *Dunu Tech*

David Shultz, *U.S. Department of Defense*

Austin West, *IT Veterans*

***Disclaimer**: This document was prepared by the members of the ATARC Future of Secure Work Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with and shall not be used for advertisement or product endorsement purposes.*

Table of Contents

The Situation

Mobile devices are double-edged swords. Connectivity brings benefits but presents safety trade-offs. They undoubtedly provide connectivity, efficiency, information access, and speed decision making processes. Operated without proper security, they also present risk to users. Adversaries can exploit mobile radio frequency (RF) emissions and network connection identifiers to surreptitiously reveal user locations, identities, military organization affiliations, and movements.

The risks apply to Government Furnished Equipment (GFE) and privately-owned cell phones and tablets used for command and control, intelligence and logistics roles and in more sensitive government operations.

> *"There have been widespread reports in Western media since the beginning of the [Ukraine] war about both sides' abilities to intercept and geo-locate phone calls for targeting purposes."* ***Makiivka attack: Could mobile phones have revealed Russian location?*** *BBC News, January 4, 2023*

Tracking certainly presents general and anti-terrorism safety risks to US Government (USG) personnel traveling outside the United States and significant operational security risks to any USG operation including defense and intelligence. Adversaries have the capability to identify any radio signatures to include mobile device signatures while units marshal for deployment, in transit, and later locate units during missions. Conversely, adversaries can identify mobile device signatures during missions and track those device users back to their home stations. In foreign locations adversaries use local government-controlled service provider networks to identify USG personnel, regardless of mobile device make or model. Lessons from the Ukraine war show that all radios to include mobile devices are easily identified through electronic warfare and targeted with artillery or air attack. Prescribing mobile device restrictions for a recent exercise at the National Training Center to his staff, a US Army general officer said, "this device is going to get our soldiers killed."[1]

The largest risk is the association of the device's International Mobile Equipment Identifier (IMEI) with the user and the USG, and subsequently recognized operating outside the US. This often generates an automatic "flag" for additional action. This capability is widely available to nations around the world.

As a result of lessons from Ukraine and in training, the USG is considering changing where and how it uses mobile devices. And the US defense and intelligence communities have

[1] "What the Pentagon has learned from two years of war in Ukraine," The Washington Post, February 22, 2024.

*Mobile devices: Inclusive of mobile, end user, and PED devices

notably recognized the vulnerability to deployed personnel through mobile device monitoring and surveillance and seeks solutions for personnel safety.

Fortunately, USG personnel can significantly reduce the vulnerability of their signatures through the steps in this Annex to the Future of Secure Work Base Paper.

Goal

Increase the safety and operational effectiveness of personnel by enabling workforces to reliably manage device signatures and location management for GFE and personally owned mobile devices. This is achievable through a series of complementary and reinforcing security measures (see below).

Resources

- Access to government-procured and managed mobile devices.
- Access to a broadband, or high bandwidth, obfuscated re-transmission device.
- A government furnished, approved mobile device sleeve with anti-surveillance features.
- An effective government furnished Faraday case.
- ATARC White Paper: The Future of Secure Work: How to Enable the Secure Workforce of the Future Through Secure Mobility

Part 1: Considerations for Mobile Signature Management

Consider Organizational Change Management

Discussing the mobile solution and gaining the support of key leaders, stakeholders, security managers, and the workforce is critical for success. In navigating the complexities of organizational change management to foster secure mobility, a strategic and comprehensive approach is essential. This transformation, pivotal for enabling the Government's classified workforce, aims to bridge the gap between traditional security protocols and the demands of the information age. Success hinges on meticulous planning, stakeholder engagement, and a deep commitment to change management, as detailed in the OPM Guidance for Change Management in the Federal Workforce.

Key steps include:

- Strategic Alignment and Planning:

    - Develop strategic objectives that align with future human capital requirements.
    - Conduct a detailed workforce analysis to identify competency gaps and training needs.
- Stakeholder Engagement and Support:
    - Secure the endorsement and active support of leaders, stakeholders, security managers, and the workforce through transparent communication and shared vision.
    - Utilize scenario planning to evaluate potential impacts and select the best path forward.
- Implementation and Training:
    - Identify specific training programs to equip the workforce with the necessary skills for leveraging approved mobile devices in secure areas.
    - Implement structural and cultural changes to facilitate the adoption of new protocols and technologies.
- Evaluation and Adaptation:
    - Manage transformation through ongoing evaluation, leveraging human capital strategies to ensure continuous adaptation and alignment with objectives.
    - Employ evidence-based strategies for workforce reshaping, including restructuring, resizing, reskilling, and recruitment.

Prior to Mission or Travel:

- Conduct risk analysis. Use organizational processes to understand the types and levels of risk you or your unit will face during travel/mission. Consider threat capabilities for signature targeting from home station, during transit, and in the operational area.
- Identify if your mission has a level of acceptable risk.
- Compare risk to capabilities of mobile devices. Upgrade devices to mitigate risk.
- Develop success criteria to measure effectiveness. For example, units in training or on exercises should experience fewer operational security incidents.

Part 2: Reinforcing Security Measures and Guidelines

Organizations can manage the signatures of mobile devices through two security measures:

- **Measure 1a** - Fully disabling the primary mobile device cellular radio in hardware and leveraging secondary broadband, or high-bandwidth, transmission through an alternative, obfuscated path, or:

    - Measure 1b: Leveraging secondary retransmission designed for low probability of intercept or detection (LPI/LPD). This is usually a lower bandwidth option that focused on critical information only.
- **Measure 2** - transporting mobile devices during operations in an approved Faraday case.

Using both measures provides the most thorough solution for mobile device security. Paired with a monitoring capability, they enhance organization security through auditability and the ability lock phones in case of loss or adversary theft.

Measure 1a: Physically control the mobile device radios and sensors

The simplest way to eliminate mobile device signatures is to disable the device radio. However merely switching-off a mobile device radio through software, commonly referred to as airplane mode, leaves the cellular radio in operation and provides false security.

- Use an organization-approved case or sleeve that pairs with the mobile device featuring chip-level control that enables user to physically control the risks on the on the mobile device. This includes physically controlling the camera and microphones, and the ability to disable mobile device radios to include cellular/GPS, with the options to include WiFi, and Bluetooth.
    - While the largest risk is for the cellular radio IMEI being identified with the USG and targeted for exploitation, the other mobile device radios represent a risk that may require management.
    - Physical control of the USG mobile device sensors will significantly reduce or eliminate the device signature, deny adversary tracking capabilities, and deny access to microphones and cameras even if a USG device is exploited.
- Use an organization-approved travel Faraday case. Whereas turning off mobile devices shows threat observers a network-disconnection and draws attention, an approved Faraday travel case will pause cellular connection to show only a lost signal to threat observers, not a network disconnect. Operational personnel will still be able to use mobile devices for situational awareness during missions and then effectively barricade them from the cellular network and other untrusted wireless equipment at other times when stored inside the Faraday case.
- Consider monitoring of the USG devices, to include Mobile Device Management (MDM) and User Endpoint Management (UEM) policies.

Measure 1b: Use retransmission connection

- To stay connected while managing your USG RF signature, leverage an alternative, obfuscated network path to required USG networks. Use a secondary retransmission designed for low probability of intercept or detection (LPI/LPD). This is usually a lower bandwidth option that focused on critical information only.

Measure 2: Transport mobile devices during operations in an approved Faraday case designed for modern mobile devices

A practical Faraday case prevents wireless signals from reaching the mobile device, in effect turning the device off in a reliable way. This allows mobile device users to leave commercial (and adversary observed) networks without drawing unwanted attention from network observers.

- Like with disabling device RF signatures, deploying personnel need a way to "go dark" with their devices, and surreptitiously leave cellular networks.
- Powering-off a mobile device can be a signal that can garner escalated attention from network observers. In the event of device compromise, it can be impossible to verify that the mobile device and its cellular radio are truly off.
- Network observers will only see a lost or dropped signal, not a network disconnect, even if the phone is compromised and powered on.
- Perform a user functions test. Based on the threat environment, consider the potentiality of electronic eavesdropping on any conversations held near the Faraday case. Use a case with sound jamming features.

How to test your Faraday case selection:

Many commercial off the shelf Faraday case options are designed for users who may not have the same risk profile as USG personnel. These, usually more affordable, options are made from cloth and come with both a risk of improper use, and natural decline in protection as they age. Consider proper testing to align to your risk profile. An example of a user functions test follows:

Signal to test	Smartphone settings	Action	Expected result
Cellular	Cellular is turned on, WiFi is turned off and the ringer is set to maximum.	Call the smartphone.	Your smartphone will not ring.

GPS	Location services are turned on and WiFi and Bluetooth are turned off.	Use a locator service (Like iPhone's Find My or Android's Find My Device) to locate the smartphone.	Your smartphone's current location will be unavailable.
WiFi	WiFi is turned on, cellular is turned off and the ringer is set to maximum.	Call the smartphone.	Your smartphone will not ring.
Bluetooth	Bluetooth and Bluetooth sharing are turned on.	From a compatible device, use the Bluetooth sharing feature (like iPhone's AirDrop or Android's Nearby Share) to send the smartphone a photo.	Your smartphone will not be discoverable.

Table: Examples for how to conduct a user function for a practical Faraday case

Guideline and Consideration: Educate employees on proper system use

This should include:

- Creating Employee Rules of Behavior. Work with security, counterintelligence (CI) and information technology sections to develop viable guidelines for proper use of the security-enabled devices and procedures.
- Create Employee Training Program. Inform employees of proper use of the system, including Rules of Behavior and recommended mitigation measures. If a training program does not exist, create one in coordination with security and CI personnel. The training should include procedures for contacting security or CI personnel in the event of a security issue. Ensure employees have access to security guidance and reporting procedures.

Guideline and Consideration: Expand the program for full operational capability

When the pilot program is successful, an organization can increase the number of security enabled devices, based on lessons learned and with continual monitoring for compliance.

- Leverage your success criteria to support continuing the program.
- Continue to work with the information technology, security and resource management stakeholders throughout the growth of your trusted mobile enterprise capability. Future resourcing, prioritization of funding, and program management will be critical factors.
- Continue to analyze and address risk: Lower risk may allow changes in organizational travel procedures. However, risk factors and adversary methods will change as organizations scale.
- Consider Key Management and RF Signature Management: RF signatures may be influenced by the types and usage of encryption of data transmitted over radios. Key delivery/exchange and establishment of the symmetric keys may vary wildly and impact RF signature characterization. Evaluate the intersection of both for thorough RF signature reduction.

Guideline and Consideration: Continually measure compliance

Adjust and revise security practices based on lessons learned. Throughout the life of the program, continue regular security updates to mobile devices and maintain awareness of adversarial threats and risk. Update procedures as necessary. Consider enabling an organization incident response program for mobile security.

A Brighter Future with a Signatures Management Lens

Thorough signature management has profound impact in today's dangerous electronic warfare environment. Adversaries actively exploit mobile devices to target people and activities, and they constantly improve their targeting capabilities. Signature management defeats adversaries by:

- Lowering the risk of targeting people in transit or on missions, increases their physical safety, and enables mission accomplishment.
- Enabling security managers to thoroughly know how well their personnel are complying with security measures, and support assessments of adversarial risk, and enables fact-based changes to operational procedures.

- Forms a foundation for additional anti-detection techniques such as International Mobile Subscriber Identity (IMSI) or International Mobile Equipment Identity (IMEI) swapping.

The US has a significant advantage over our adversaries by caring for the welfare and safety of our people. Another advantage is how we apply innovation and technology to overcome brute force. Signature management combines these qualities. That's how the US maintains dominance in competition and wins at war.

Frequently Asked Questions:

What is the signature management solution for classified devices?

The NSA developed and proliferated the CSfC Mobile Access (MA) Capability Package (CP) Version 2.5 as a commercial strategy suitable for protecting classified information and National Security Systems (NSS), provided the customer's implementation of the solution is configured, maintained, and monitored as required by the CP (see CSfC Capability Package v2.5, 4 August 2021).

The NSA classified solution emphasizes broadband obfuscation via special operating systems on the mobile devices to eliminate the exploitation of the mobile devices sensors and physically connected retransmission.

In general, follow procedures in CSfC Capability Package v2.5 to implement this solution. Figure 2 shows a sample architecture in this solution.

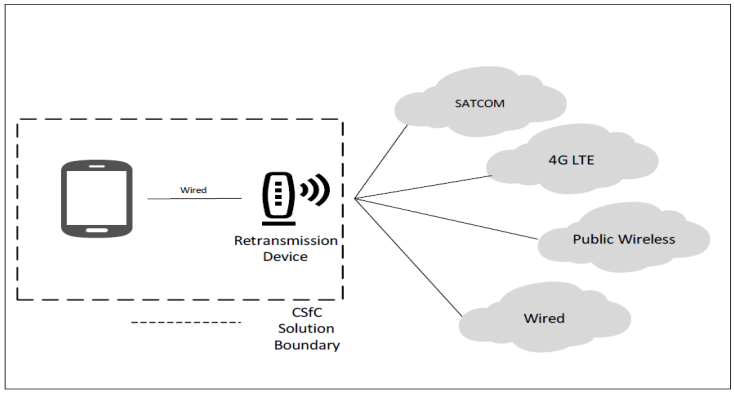

Figure 2: Retransmission Device Connectivity[2]

[2] Source: https://www.nsa.gov/Portals/75/documents/resources/everyone/csfc/capability-packages/(U)%20Mobile%20Access%20Capability%20Package%20v2.5.pdf?ver=vYeSxWuQRORbc2aEVTy0ug%3D%3D

We use mobile devices to operate Unmanned Aerial Vehicles. Is there a way to manage signatures for this mission?

Yes, there are also security measures, similar to what is in this annex, that can significantly reduce the signatures of UAV operations. We will publish the solution in Annex 2 to the Base Paper. Watch for it!