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

White Paper Annex 3
How to Enable Secure Mobility for Fixed Location Workplaces

ATARC Future of Secure Work Working Group

May 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*

Table of Contents

The Situation

The Future of Secure Work Base Paper outlines how the US Government (USG) has acknowledged the utility of mobile devices across environments. However, agencies that use sensitive or classified information often deal with mobile devices in two ways: either banning them from secure work environments or using commercial devices that lack thorough security protection. Banning mobile devices from secure workspaces is increasingly inefficient. Personnel lose access to decision-making, communications, critical information, files, calendars and more. This impedes productivity and mission success. Such an environment also challenges organizations to attract, retain and engage mobile natives and others used to working – and living - on their mobile devices. As the Future of Secure Work Base Paper outlined, a synergy of national intent, policy, computing power, and security forms a foundation for how agencies and organizations can expand mobile communications and address such issues through:

- Leveraging policies that allow approved mobile devices in secure spaces
- Controlled architecture connections
- Devices that mask ambient audio, disable radios, cameras and microphones

Goal

Enable workforce increased efficiency, productivity and satisfaction through intelligently designed, comprehensive security for mobile devices and architectures that will allow employees to use government-managed mobile devices in secure spaces.

Resources

- Access to government-procured and managed mobile devices. Note that the mobile devices must meet the shielding, anti-surveillance and anti-activation requirements contained in Committee on National Security Systems (CNSS) Directive No. 510, Directive on the Use of Mobile Devices Within Secure Spaces
- Access to a secure and monitored network environment (Federal Risk and Authorization Management Program (FedRAMP) authorized cloud service provider / Security Information and Event Management (SIEM) system /VPN/trusted WiFi or LiFi) combined with Zero Trust concepts
- Wireless Intrusion Devices (WIDS) at the primary office location
- Access to:
    - DOD Mobility Access Portal: https://public.cyber.mil/mobility/

    - DOD Mobility Service Portal: https://disa.deps.mil/ext/cop/dod_mobility (CAC enabled)
- References:
    - CNSS Directive No. 510, Directive on the Use of Mobile Devices Within Secure Spaces
    - CNSS Policy 11: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products
    - NIST Special Publication (SP) 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise
    - NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
    - NIST SP 800-30, Guide for Conducting Risk Assessments
    - NIST SP 1800-22C: Mobile Device Security: Bring Your Own Device, Volume C: How to Guides
    - DODI 8420.01: Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies
- ATARC White Paper: The Future of Secure Work: How to Enable the Secure Workforce of the Future Through Secure Mobility

Step-by-Step Instructions:

Step 1: Review applicable organization policies. Is there policy that:

- Contains procedures to request allowing mobile devices in secure spaces (Example: See CNSSD Directive 510 or Deputy Secretary of Defense Memorandum, SUBJECT: Mobile Device Restrictions in the Pentagon, 22 May 2018).
- Addresses Mobile Device Management (MDM), User Endpoint Management (UEM).

Step 2: 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. What leaders, units, systems or management changes need to be considered to implement secure mobility? 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.
  - Identify legacy information technology capabilities that would become unnecessary with the introduction of a trusted mobile capability, such as unclassified desktop phones.
- 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.
  - Work with your resource manager to identify budget efficiencies that will sustain a mobile capability as it grows and replaces legacy, wired, information technology.
- 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.
  - Continue to identify legacy capability that will be replaced by a transition to an enterprise, trusted, mobile capability for budgeting.

The journey from the conceptual framework to the tangible implementation of secure mobility within secure spaces necessitates a collaborative, phased, and iterative approach. By integrating these steps, we pave the way for a secure workforce that is not only more flexible and connected but also equipped to meet the challenges of tomorrow with increased productivity and efficiency. Embracing change management techniques, focusing on the human element of transformation, and maintaining a steadfast commitment to continuous improvement are essential for navigating the transition from industrial-age to information-age security protocols.

Step 3: Obtain the necessary components for a mobility pilot program

- Mobile devices approved by the National Telecommunications Security Working Group (NTSWG) and meeting requirements in CNSS Directive No. 510, with physical controls over microphones and cameras. The shielded mobile devices should:
  - Mask ambient audio and block ambient visual data.
  - Enables users to "check into" a secure space, whereby anti-surveillance protections are engaged and prevented from being turned off.
  - Pass status information – including anti-surveillance protection mode, check-in status and battery level – to an organization's secure and monitored network.
- Consider a phased wireless broadband capability. Mobility pilots may leverage commercial broadband wireless networks for evaluation and testing. As a pilot program transitions into broader adoption organizations should consider a trusted wireless network system with device whitelisting for approved mobile devices and the ability to capture and report device addresses.
- Consider a phased deployment of Wireless Intrusion Detection System (WIDS) with the appropriate governance process.
- Consider a phased integration into your existing security information and event management.
- Figure 1 shows an example architecture for a pilot program.

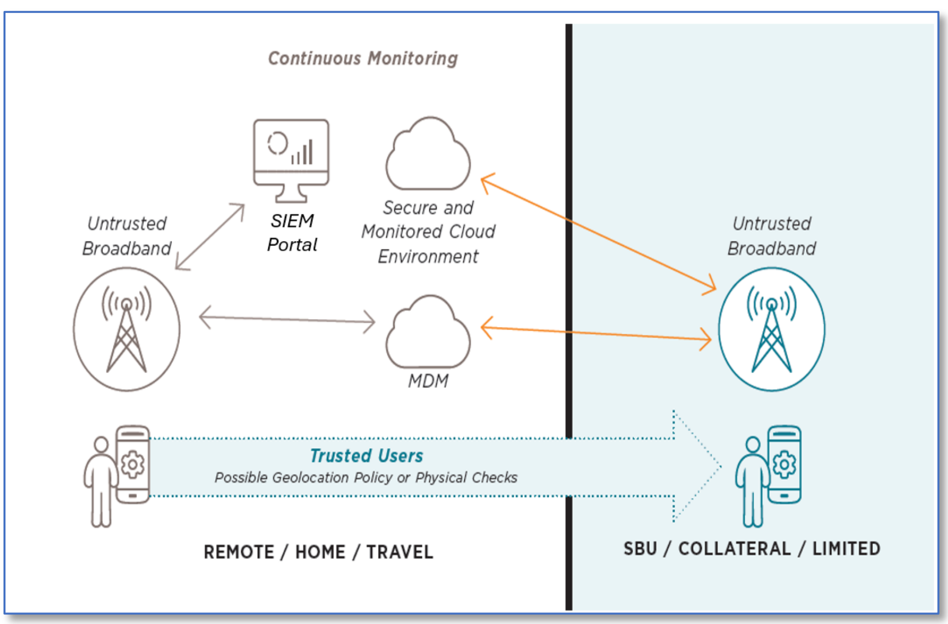

Figure 1: Example pilot program architecture

Step 4: Establish a Secure Spaces Pilot/Test/Trial

An organization may test/trial/pilot a limited number of shielded devices for use in specified areas.

- Designate a project leader for the Pilot Program, with the authority to direct members of the information technology and security teams to support the pilot.
- The project leader may designate selected employees to participate in the pilot and give feedback.
- Consider a phased approach to introducing mobile capability.

For example, provide your trusted mobile capability to a small number of trusted users with access to collateral secret spaces, with possible expansion after evaluation.

- Use an existing cellular connectivity in lieu of deploying a trusted wireless system.
- Maintain change management procedures and collect lessons learned.
- Educate pilot program participants on rules of use of the designated mobile device and procedures for entering and exiting the secure space.
- Develop and publish to your stakeholders the success criteria for the pilot program. Examples are: operational security improvements, effective facility security in accordance with agency policies, improved productivity, improved workforce access to information, successful monitoring, workforce operational agility or flexibility for secure work at multiple locations, workforce satisfaction, and others determined by the organization.
- Standards and criteria will probably differ by agency or organization.
- Training and education. Allocated resources for training on trusted mobile device use and explain the success criteria monitoring plan.
- During the pilot: employees use designated mobile devices as instructed. The organization collects data for the secure network on daily operational connectivity and security alerts.
- Monitor participants for proper device use continuously. Treat trusted mobile capability as a 24/7 operational security improvement by having the participants carry the devices in all environments.
- Plan for enhanced compliance requirements and monitoring when participants enter secure work facilities.

> ***Remote Wipe and Lock:*** *Maintain the ability to remotely wipe or lock devices in case they are lost, stolen, or compromised. This helps prevent unauthorized access to organizational data and mitigates the risk of potential data breaches.*

> ***Privacy Considerations****: Clearly define what data the organization will access and obtain consent from employees. Establish procedures for handling and protecting employee personal information in compliance with privacy regulations.*

   - Trusted mobile device users “check into” the organization secure facilities or spaces, acknowledging that by entering the classified space the anti-surveillance protections are engaged and can only be deliberately disengaged by the user where appropriate.

- Monitor for compliance.
- After the pilot, leverage your success criteria (see examples above) to support continuing the program.

Step 5: Build towards an initial operating capability (IOC)

Once the pilot program is successfully completed, an organization may increase the number of trusted mobile users under the pilot conditions and develop an IOC solution architecture for broader adoption.

IOC solution architectures may include the introduction of a trusted organizational wireless capability, and enhanced monitoring.

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.

Step 6: Enterprise, trusted mobile full operating capability (FOC)

For an enterprise mobile capability, organizations should consider user monitoring via a secure cloud environment.

Some FOC features may include:
- User compliance automatically tracked by a Security Incident Event Management (SIEM) system.
- Trusted mobile devices may be automatically connected to the organizational wireless system when arriving at a secure facility.
- Reduced mobile device accessibility while inside a secure space.
- Figure 2 shows an example FOC architecture.
- The Table shows mobile device mitigation measures at FOC.

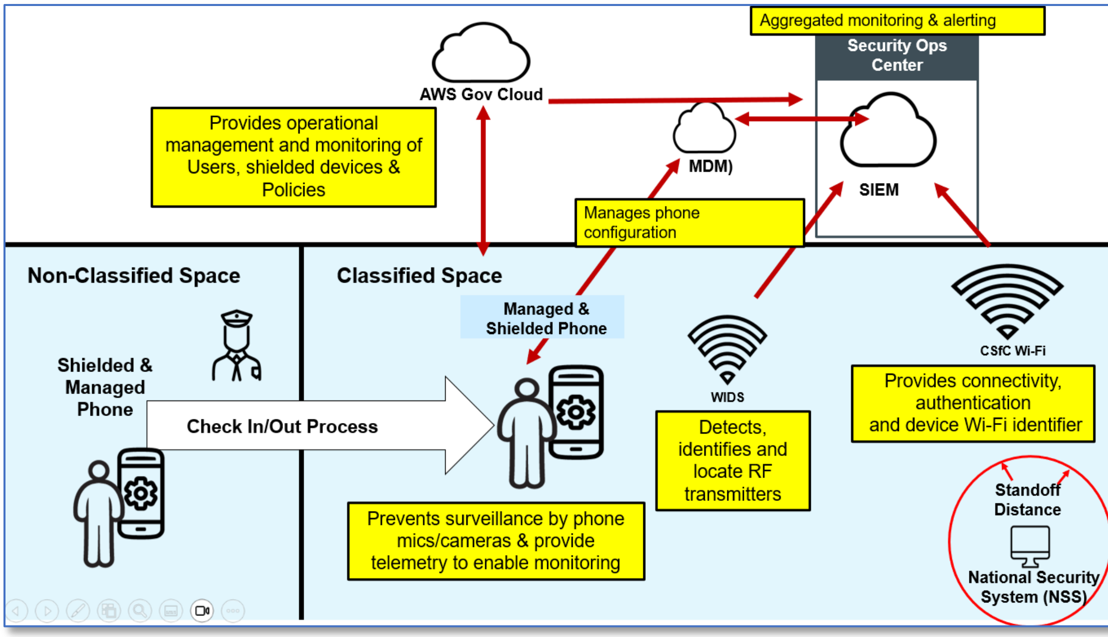

Figure 2: Completed FOC Secure Mobility Architecture

Risk	Mitigation
Physical Security	• Update policies to be consistent with NDAA 2024, ICD 123, NIST and CNSS guidelines
Cyber Security	• Security-focused device selection • OS, application isolation; application vetting • Anti-surveillance protections which can't be turned off by either attackers or users in secure spaces • WIDS, MDM monitoring and disabling of device radios • User education • Use devices that mask ambient audio, fully disable radio, camera and microphone • Implement secured data-in-transit with VPNs, on-device proxy settings, TLS 1.3, implement certificates for access to sites, WIFI and VPN • Mandate use of DNS or HTTPS/TLS via EMM
Human Risk	• EMM technologies • Mobile device security policies • Develop an Acceptable Use Policy and associated user education • WIDS, MDM monitoring and disabling of device radios • Use devices that mask ambient audio, fully disable radio, camera and microphone • Use secure storage containers for operational travel

RF Signature Risk	• Use devices with RF signature masking
Supply Chain Risk	• User education • Security-focused device selection
Efficiency Risk	• Mobile device use IAW policy permits access and proper security

Table: Examples of mobile device mitigation measures (see NIST SP 800-30)

Step 7: 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.