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

White Paper Annex 1
How to Implement Secure Mobile Operational Security

ATARC The Future of Secure Work Working Group

August 2024

ATARC

Advanced Technology Academic Research Center

Table of Contents

INTRODUCTION 1

ANNEX 1: HOW TO IMPLEMENT SECURE MOBILE OPERATIONAL SECURITY 3

THE SITUATION 3

GOAL 4

RESOURCES 4

RISKS TO MOBILE DEVICES 5

MITIGATING THE RISKS 6

TIPS FOR EMPLOYING MOBILITY WHILE MITIGATING THE RISKS 6

TIP 1 6

TIP 2 6

TIP 3 7

TIP 4 8

TIP 5 10

TIP 6 12

CONCLUSIONS 12

FREQUENTLY ASKED QUESTIONS 12

MOBILE COMMUNICATIONS STANDARDS / REFERENCES 14

ATARC would like to give special thanks to The Future of Secure Work Working Group members Mark Gorak (Department of Defense), Jose Moreno (Department of State), Heather McMahon (Privoro), Michael Schellhammer (Artemist Advisory Group), Lt. Col. Jamie Johnson (United States Space Force) John Cavanaugh (IIS Corp), Michael Epley (Red Hat), Pat Pulliam (Blackberry), Randy Siegel (Center Circle Consultants), and James Stanger (CompTIA), for their insights on this paper.

Annex 1: How to Implement Secure Mobile Operational Security

For the purposes of this paper, consider a workforce required to be in constant contact 24/7 in every setting from fixed sites or offices to various field and office locations, at home and on-the-road. Employees using mobile devices without thorough security mitigations are vulnerable to targeting by adversaries, advertisers or criminal actors who will steal information via the device cameras, microphones, or network connections. This paper outlines actions users can take to mitigate risks.

The Situation: Mobile devices are essential to modern life. Today, US Government (USG) agencies and organizations issue over a million mobile devices to enable connectivity in any operational location. This is in addition to the millions of employees conducting government business on personal devices. In the workplace, mobile devices provide essential efficiency, information access, and speed decision making processes in ways that were previously only imaginable. The post-COVID-19 office environment is also more mobile and flexible than in previous years. Unfortunately, evolving mobile technology and their expanded use has also changed how adversaries target mobile devices. Agencies and organizations are developing measures for constant operational security awareness to counter such risks.

> "... cell site simulators pose a major growing threat to national security, personal privacy, and crime prevention. It must be taken at least as seriously as Chinese technology theft and Russian hacking."
>
> Are the Chinese and Russians listening to your phone calls? The Hill, December 24, 2018

However, many current risk mitigations are often not uniformly implemented across agencies. This results in employees using mobile devices that present security risk because of ineffective or incomplete security measures.

Security measure? Or an adversarial collection opportunity?

What risks are out there?
Devices are vulnerable to adversary eavesdropping, malware insertions, and surreptitious microphone or camera activation, risking access to the mobile device itself and information in its vicinity. Without proper mitigation and tradecraft, adversaries may also exploit a mobile device's high-powered radios for location tracking and combine that information to develop intelligence information on users. In foreign locations adversaries use local government-controlled service provider networks to identify USG personnel, regardless of mobile device make or model. Risks to mobile devices also exist within the United States as spyware knows no borders.

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

> In February 2024, a random security check revealed traces of spyware on devices belonging to two European Union Parliament members and an adviser working on the Subcommittee on Security and Defense, highlighting the vulnerability of employees to attempted hacks or infections.

Agencies, organizations and employees increasingly must operate in any environment and any time of day. All expect that their mobile devices are protected from communications monitoring, intelligence collection, device geolocation, and data exposure or manipulation. This includes VIPs, Senior Leaders, Executives, First Responders, Law enforcement field office agents, Emergency Operations and Managers. It also includes the population of government employees who are growing more and more dependent on mobile devices for effectiveness. That could arguably be everyone in government, if not today, soon. Recognizing such imperatives, the mobile communications industry has recognized the need for Zero Trust strategies for mobile devices and has developed new capabilities to meet the need for risk mitigation in hardware and software. The USG community is now postured to combine Zero Trust concepts with improved mobile device endpoint security to enable 24/7 OPSEC.

Goal:

Help employees and their organizations be aware of the risks of using mobile devices, and help organizations improve operational security and establish Tailored Trustworthy Spaces (TTS) with risk mitigations, allowing them to operate mobile devices with security and confidence.

Resources:

- Smartphones and tablets managed by user-based security policies
    - Unified Endpoint Management (UEM) policies for all deployed devices
    - Containerization for mobile applications, as required
    - Encrypted calling / messaging/file sharing capability, as required
    - Additional hardware-based protections, as required, for highly-sensitive data and/or use in secure spaces
    - Mobile Threat Defense
- Adopt evolving connectivity architectures (VPN, MFA, Zero Trust, End Point Protection, and Secure LiFi or Wifi)
- Wireless Intrusion Detection System (WIDS)/Wireless Intrusion Prevention System (WIPS)[1]

[1]https://media.defense.gov/2022/Nov/14/2003113710/-1/-1/0/WIDS-WIPS%20ANNEX%20V1.0%20800-53%20CONTROL%20MAPPING.PDF

- Access to NIST SP 800-124 r2; Guidelines for Managing the Security of Mobile Devices in the Enterprise.
- Agency user policy and training when navigating from public, CUI and Classified data applications. For more information see Annex 2, Classified Tablet and Device use.
- User awareness of both physical surroundings and logical data protection can be thought of as a "Tailored Trustworthy Space" (TTS). Users cannot always be in a secure facility, and industry vendors currently produce some level of secure communications capability, regardless of user location.

Risks to Mobile Devices

A modern mobile phone commonly operates as many as 10 communication systems. The nature of wireless connectivity makes all the sensors subject to access, activation, manipulation or location by adversaries or criminal actors. Table 1 shows common risks of using mobile devices outside of secure networks:

Type of Risk	Risk to employee or organization
Physical Security	• Devices outside of secure spaces are subject to loss or theft, which compromises information. • Security Managers have no way of locating or disabling devices if lost or stolen
Cyber Security	• Device as an attack vector into the network • Connecting to a network is vulnerable to adversary eavesdropping, malware, device activation.
Human Risk	• Device activation, information theft by malicious insiders • Lack of WIDS or SIEM to detect unauthorized use • Situational awareness of surroundings (See Annex 2, Classified Tablet and Devise Use, for more information)
RF Signature Risk	• Adversarial use of user's geolocation
Supply Chain Risk	• Adversary malicious hardware or software insertion; can allow remote activation
Efficiency Risk	• Loss of access to files, calendars, constant switching between networks
Environmental Risk	• Consider the electronics inherent in the environment that you must operate in, including any second, personally owned device.

Table 1: Common mobile device risks

Mitigating the Risks

In recent years USG policies established requirements for securely using mobile devices inside and outside of secure workspaces. Most significantly, the "Guidelines for Managing the Security of Mobile Devices in the Enterprise," published by NIST in May 2023, contains recommendations for how organizations may mitigate security risks and select, implement and manage devices.[2]

Concurrently with the USG emphasis on mobility, the mobile device and mitigation industry has improved device security and capabilities to the point they now address many security concerns.

This paper summarizes some of the most significant aspects, provisions and considerations for safely using mobile devices outside of secure spaces. We present a series of "Pro-Tips" that combine best practices with hardware and software solutions to address most common risks and enhance mobile security.

Tips for Employing Mobility while Mitigating the Risks

Tip 1: Review the organization policy on use of mobile devices. Look for if your organization has policies that support employees that are multi-tasking from one application data level to another.

Does your organization have policies that address:

- Provisions for mobile connections through a secure network, such as a VPN, MFA, Zero Trust, End Point Protection, and Secure LiFi or Wifi?
- Procure devices that meet organizational security standards, or standards published by the General Services Administration (GSA) CIO-IT Security-12-67, Securing Mobile Devices and Applications?
- Allows use of mobile devices on official travel or deployment, including recommended or required best security practices?
- Clear instructions for employees to apply OPSEC measures outside of the office environment?

If policies do not exist, see NIST SP 800-124r2 for guidelines on developing mobile device policies.

Tip 2: Conduct a risk assessment of mobile connectivity. Risk assessments help organizations determine the range of risks to operations, personnel and information and prioritize mitigations.

[2] NIST SP 800-124 r2; Guidelines for Managing the Security of Mobile Devices in the Enterprise; SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise | CSRC (nist.gov)

- Consider threat capabilities for signature targeting from home station, during transit, and in the operational area.
- Consider how your workforce actually behaves and operates.
- Identify if your mission has a level of acceptable risk.

Update your risk assessment periodically to keep pace with evolving threats and inform security audits. Many risk assessment methodologies exist, and an organization can choose the applicable method that suits its mission or tailor their approach. Use NIST Cybersecurity, Privacy and Risk Management Frameworks and 1800-22 series. Specially, apply the Risk Model in NIST 800-30 to identify organizational risk, as shown in Figure 1:

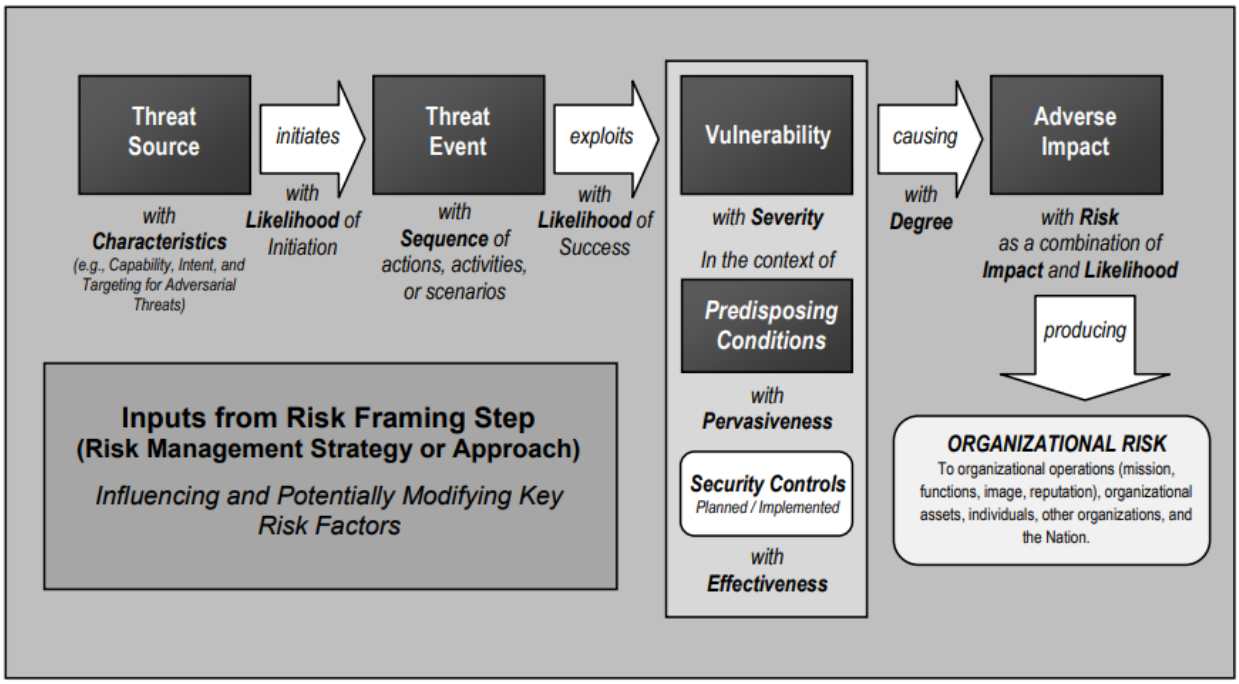

Figure 4: NIST risk model with key risk factors[3]

Tip 3: Consider Organizational Change Management.

Implementing secure mobility can bring significant change to organizational culture. 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 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

[3] NIST SP 800-30, Guide for Conducting Risk Assessments, Revision 1, September 2012, p. 12. https://csrc.nist.gov/pubs/sp/800/30/r1/final

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.

Tip 4: Consider these Best Practices for Mobile Device Security while outside of Secure Workspaces

a. **Use shielded mobile devices**. Organizations can manage the vulnerabilities of mobile devices (both Government Furnished Equipment (GFE) or Bring Your Own Devices (BYOD)) to adversarial remote activation, eavesdropping or manipulation through commercial shielding. Commercial shielding can provide three security measures that protect mobile devices:

- **Measure 1** - Fully disabling the primary mobile device cellular radio in hardware and leveraging secondary broadband, or high-bandwidth, transmission through an alternative, obfuscated path.
- **Measure 2** - transporting mobile devices during operations in an approved Faraday case.
- **Measure 3** – shield devices from eavesdropping. A properly configured shield, paired to the mobile device, can mask ambient audio and block the mobile device's cameras. This will render meaningless any adversary-captured audio and video data.

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

Refer to Annex 4 for a detailed outline of how to protect mobile devices against geo-location.

b. Combine shielded devices with monitoring via Cloud environment

Shielding employee mobile devices gains security on the device itself. To achieve complete OPSEC 24x7, combine the shielded mobile device with continuous monitoring via a cloud environment with a Security Incident Event Management (SIEM) system. Use of the SIEM allows security managers to continually monitor mobile devices for unauthorized activity such as microphone use, camera functions, malicious applications, and unauthorized connections to the internet, other devices, or systems.

Table 2 shows how combining shielded devices with cloud SIEM monitoring mitigates mobile device vulnerabilities.

Table 2:

Type of Risk	Risk to employee or organization	Mitigation
Physical Security	• Devices outside of secure spaces are subject to loss or theft, which compromises information. • Security Managers have no way of locating or disabling devices if lost or stolen	• SIEM allows remote wiping of mobile device, reducing information loss. • Continuous monitoring through SIEM allows locating devices. • Supports other security efforts such as Technical Surveillance Countermeasures (TSCM)
Cyber Security	• Device as an attack vector into the network • Connecting to an unsecured network is vulnerable adversary eavesdropping, malware, device activation • Potential for offensive hacking.	• Continuous monitoring alerts to external attacks • Shielding in hardware prevents adversary eavesdropping; • Use of authorized networks reduces risk of malware insertion

Human Risk	• Device activation, information theft by malicious insiders • Lack of WIDS or SIEM to detect unauthorized use	• Shielding prevents unauthorized device activation • SIEM prevents unauthorized use and creates a record of activity for audit
RF Signature Risk	• Adversarial geolocation of user	• Shielding with radio deactivation capability and prudent use of faraday case prevents geolocation • There are currently solutions from Industry that can physically disconnect the baseband radio
Supply Chain Risk	• Adversary malicious hardware or software insertion can allow remote activation of endpoint microphones and cameras	• SIEM alerts on malicious software insertion • Shielding in hardware mitigates risk of remote activation • Both measures protect from effects of remote activation
Efficiency Risk	• Loss of access to files, calendars, constant switching between networks	• Shielding in hardware combined with SIEM enables constant secure connectivity to networks with risk mitigation

Mitigating mobile device risks.

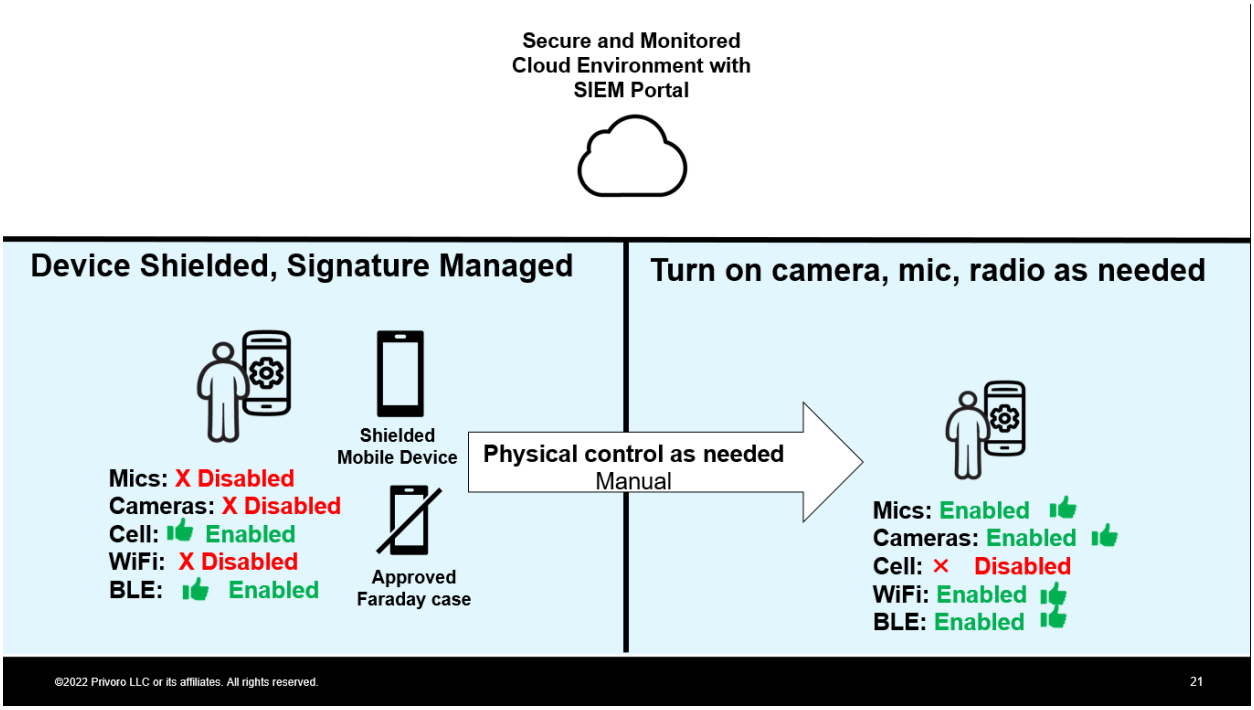

Figure 3: Mobile industry leading practice for architecture and protections for shielded devices with cloud monitoring

Tip 5: Use True End-to-End Encryption.

In addition to the functional security requirements demanded by NIAP protection profiles:

- Session keys for voice and IM are protected end-to-end using S/MIME encrypted and signed containers.
- Related static and ephemeral key pairs are only accessible by the SecuSUITE application on the device, and all cryptographic operations related to private keys are executed within the key-store engine.
- Key material is extracted from secure storage only when needed for a cryptographic operation and is removed from RAM afterwards.
- **Secure authentication** of call participants based on S/MIME user certificates exchanged during key agreement.
- **Protected registration and authentication** of clients using Secure Remote Password Protocol (SRP) which provides authentication of the communication partners as well as encryption. In addition to the SRP encryption, the connection between clients and the backend server is secured by TLS v1.2.

- **User Certificate Handling Service** stores the public certificate of every client on the SecuSUITE server to enable other clients to establish secure communication from the start.
- **Secure Session Initiation** using Session Initiation Protocol (SIP) to exchange SIP messages with the server through a TLS v1.2 connection, providing encryption and mutual authentication with the backend infrastructure. The SIP stack on the mobile client side is an integral part of the client application.

Tip 6: 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.

Conclusions

Mobile communications are a permanent part of business and life. Their increased utility and use in government activities is inevitable, as is their targeting by adversaries, advertisers and criminals. Thankfully, the mobile device industry, improved network connections, and government security practices now create a synergy that allows expanded mobile device use with robust security measures. Thoughtful, forward-thinking organizations can now empower their employees to operate with maximum efficiency and flexibility while enabling security managers to assess and manage adversarial risk. By applying mobile device OPSEC measures, USG employees can improve their efficiency worldwide, in all environments, and outpace adversaries at the same time. The US government is the most powerful force for good in the world. Government leaders and employees are ready for their mobile security to enable them to reach the goals of America.

Frequently Asked Questions:

Question: Are there methods to allow secure classified connections with OPSEC?
Answer: 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 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 4 shows a sample architecture in this solution.

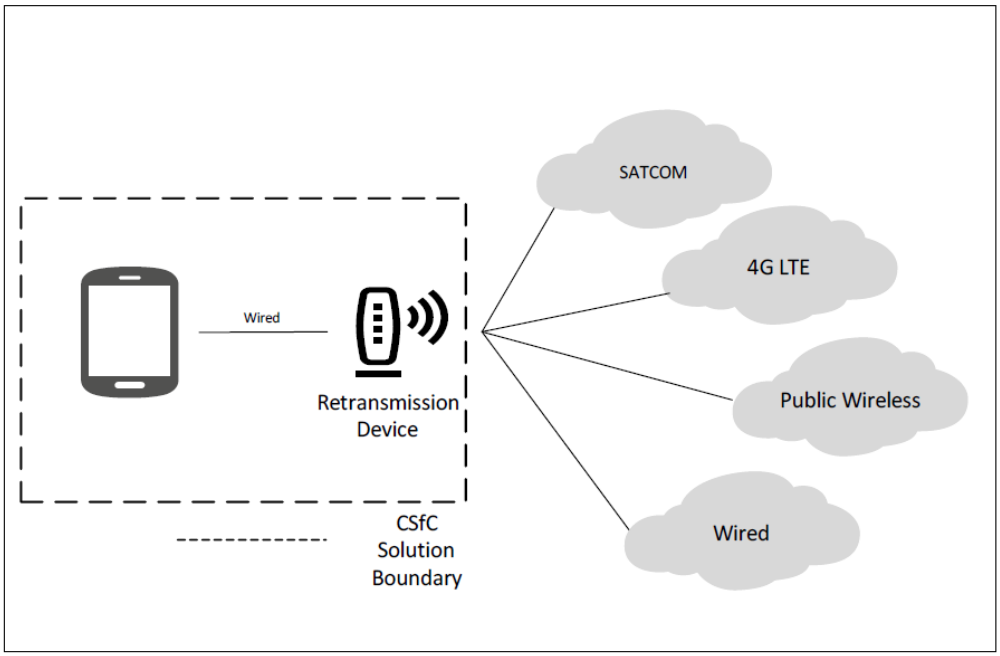

Figure 4: Retransmission Device Connectivity

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

Question: Are there USG guidelines on what mobile devices best support security?

Answer: Yes, and new guidelines are being conceived and updated frequently. See the "NSA/CSS CSfC Components List," below. The GSA has determined that all devices (iOS and Android) must have MaaS360 AND Lookout mobile security to satisfy security requirements. As such, all devices are monitored to ensure once installed, they remain active and updated to provide an increased level of security for all mobile smartphones and tablets. See more in GSA CIO-IT Security-12-67, Revision 5, Securing Mobile Devices and Applications, June 16, 2022.

Question: What are some of the situations where secure mobility and a TTS apply?

Answer: Operational travel or deployment presents multiple situations that present security risk and require solutions. For example, an employee may be in an unclassified meeting and need to address a classified task. This requires a supporting policy and devices to establish a TTS. Or an example in the opposite sense, a user is performing a classified task and must address a personal priority, the user policy and procedure may require the user to exit the

classified domain or prevent the unclassified task from observing classified data. User awareness of different application security levels (Public, Controlled Unclassified Information, Secret and Top Secret) use different networks to access high levels of data classification. To allow secure access in these situations, an organization requires policy, architecture and devices to continuously monitors the TTS device WID/WIP status, network routing device and communication. User training and acceptance of TTS rules such as call or access termination if a TTS policy is detected (for example a unknown person presence is sensed by WID sensors which could disconnect a call or terminate data access).

Question: If I need additional security when deployed, are there options for secure workspaces?

Answer: Yes. There are now multiple commercial options for containerized secure workspaces, including the TS/SCI information levels. ATARC can direct inquiries to available solutions.

Mobile Communications Standards / References

- NSA/CSS CSfC Components List: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Components-List/
    - MDM
    - TLS Protected Servers
    - Enterprise Session Controller
    - VoIP Applications
    - TLS Software Applications
    - End User Device/Mobile Platform
    - WIDS/WIPS
- Common Criteria Protection Profiles: https://www.commoncriteriaportal.org/pps/index.cfm
    - Mobile Device Management
        - Protection Profile for Mobile Device Fundamentals
        - Protection Profile for Mobile Device Management
    - Backend mobile communications servers
        - Collaborative Protection Profile for Network Devices
        - PP-Module for Enterprise Session Controller (ESC)
    - Mobile communications apps
        - PP-Module for Voice and Video over IP (VoIP)
        - Functional Package for TLS
        - Protection Profile for Application Software