White Paper

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

ATARC Future of Secure Work Working Group

March 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*

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

Muddasar Ahmed, *MITRE*

Bob Bauman, *Trusted Systems*

John Cavanaugh, *Internet Infrastructure Services Corporation*

Brian Egenrieder, *SyncDog*

Michael Epley, *Red Hat*

Patricia Fisher, *Janus Associates*

Adam Flasch, *State of Maryland*

Michael Hudson, *Clearforce, Inc*

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

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

Nnake Nweke, *Dunu Tech*

Pat Pulliam, *Blackberry*

Michael Schellhammer, *Artemist Advisory* Group

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

Randy Siegel, *Center Circle Consultants*

Austin West, *IT Veterans*

Executive Summary

To remain relevant and effective, Secure Work must leverage, embrace and expand access to mobile communications.

In legislation and strategies from the national to department levels, the Federal government has articulated requirements for mobile technology to maximize workforce efficiency, flexibility, connectivity, and speed, protected by comprehensive security. Lessons from the Ukraine war also show that thoroughly secured mobile solutions are vital for forces to fight and survive on the modern battlefield.

Because security risk is inherent in all communications, the US Government (USG) developed security standards and procedures to address risk and enable operations. In response to government and consumer demand, Industry has matured mobile devices and supporting infrastructure to meet or exceed USG security requirements while enabling the workforce to access the same tremendous computing power available to all people and organizations outside the government.

> *"Office Life at the Pentagon is Disconcertingly Retrograde.... the military's hub may be soon be a threat to national security."* https://www.wired.com/story/opinion-office-life-at-the-pentagon-is-disconcertingly-retrograde/

Studies of risk, available technology, and architectures published by the Committee on National Security Systems (CNSS) and the National Institute of Science & Technology (NIST) outline procedures for expanding use of mobile devices for greater efficiency, including in secure spaces. Modern mobile devices and supporting infrastructure procured and managed to USG standards can mitigate security risk and improve existing practices.

This paper consolidates and highlights the national intent, potential security issues and methods to mitigate risks. It sets a vision for the future of secure work for enhanced security, decision-making, productivity, operational flexibility, and auditability.

Five use case situations present immediate opportunities to meet the improvements above and begin advancing the future of secure work: ***Operational Security; Classified Tablet and Devices; Workforce Enablement; Signature and Location Management; and Wearable Healthcare Technology.***

This paper establishes a foundation to analyze the five use cases in more detail and publish follow-on "how to" guides as annexes to this paper that explain how to implement the national intent.

Table of Contents

Introduction: The Stage is Set for the Secure Workforce to Make its 21st Century Debut

Secure workforces are ready for a revolution of productivity and security. Working together, we are evolving from industrial age policy to meet the needs and reality of the information age.

The modern work environment has moved beyond traditional office spaces with legacy wired communications. Today's workforce is comprised of digital natives who use mobility for rapid information management across multiple networks. Secure work environments can keep pace with such changes without sacrificing security.

> *"I consider my time spent in the Pentagon as being time spent in a communications black hole."*
> ***US Air Force Officer***

The vision for the Future of Secure Work features improved security with auditability, increased productivity, flexibility, and decision-making speed, with access to state-of-the-art technology. It will support an engaged and accountable workforce, blending the needs of leaders, employees and security managers. This vision will evolve secure work from industrial age policy to meet information age needs. The result will be an ecosystem that allows secure workplace flexibility that enables mission accomplishment to meet national security objectives.

Imagine secure working environments where EVERYONE can:

- Remain connected to increase productivity and decision-making speed.
- Access text messaging, calendars, and unclassified email continuously.
- Seamlessly use government-issued mobile devices both in and outside of secure areas.
- Securely conduct work on the go, free from the threat of device attacks, regardless of location.
- Connect for work in any location through approved WIFI and LIFI networks while masking their RF location signature.
- Access classified documents through approved mobile tablets, geo-fenced to designated areas and auditable by security managers and investigative personnel.
- Use wearable healthcare devices in secure workspaces, improving health, the available workforce, retention, safety and happiness.

Samsung Survey: The State of Enterprise Mobility

- Employees can't work effectively without a mobile phone
- Mobile devices are essential to business workflows
- Mobile devices are essentially mandatory
- Management expects employee availability after hours and remotely

- Work on classified information remotely or on the go as easily and thoroughly as in a secure workspace – reducing the need for expensive, vulnerable and antiquated SCIF construction.
- Operate on a modern battlefield without risking detection and destruction.

And Security Managers can:

- Gain instantaneous awareness of unauthorized or risky behaviors inside their facilities.
- Instantly identify and remove unauthorized wireless devices within workspaces.
- Measure workforce compliance with secure mobility procedures.
- Extend physical security protections to remote environments quickly.
- Intervene early to prevent unauthorized activity.
- Gain flexibility to designate security profiles to remote workers.
- Maintain continuous contact with Security Staff in large facilities.

> "NNSA is committed to delivering and enabling modern technologies to our partners across the nuclear security enterprise. We face an ever-changing and fast-paced threat landscape, and modern mobile solutions will help support our workforce, protect our security and privacy, and meet mission needs."
> ***National Nuclear Security Administration***

And Leaders can:

- Benefit from a more engaged and efficient workforce!
- Command and control their forces in combat, without risk from detection and destruction.
- Remain in contact –no more, "Oops, I missed that critical meeting because I was inside a secure facility!"
- Reduce costs through use of government-issued mobile phones as primary unclassified computers and telephones.
- Increase inclusion of workforce requiring wearable health devices.

This synergy of intent, policy, computing power and security forms a foundation for secure work of the future. Agencies and organizations can now expand mobile communications capabilities across the spectrum of USG work, meeting national intent and keeping pace

The Requirement: Modern Work Environments Need Mobility

"Mobility has transformed how enterprises deliver information technology (IT) services and accomplish their missions."[1]

Embracing mobile communications to improve workforce efficiency is a decades-old concept. The White House featured mobility in its 2012 Digital Government Strategy, seeking "access to quality digital government information and services anywhere, anytime, on any device."[2] Other strategies and legislation have continued that vision:

- *2012:* DOD Mobile Device Strategy published a vision for "a highly mobile workforce equipped with secure access to information and computing power."[3]
- *2017:* CNSSD Directive 510 states the USG relies on mobile technologies for "increased productivity and mission flexibility." The directive provides requirements for use of mobile devices in secure spaces.[4]
- *2019:* DOD Digital Modernization Strategy objective, "increased availability and use of secure, mobile, wireless platforms across the Department."[5]
- *2022:* Department of State Bureau of Intelligence and Security Strategic Plan goal to, "devise a mobile strategy and develop mobile capabilities to improve support to diplomats worldwide."[6]
- *2023:* FY 2024 National Defense Authorization Act (NDAA) Sections 1552 directs DOD to implement recommendations from DODIG Report No. 2023–041, "Management Advisory: The DoD's Use of Mobile Applications," including to implement use standards for mobile devices.[7]

---

[1] National Institute of Science and Technology (NIST) Special Publication (SP) 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, (May 2023), 1: SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise | CSRC (nist.gov)

[2] Digital Government; Building a 21st Century Platform to Better Serve the American People, The White House, (May 23, 2012); 2; Digital Government: Building a 21st Century Platform to Better Serve the American People (archives.gov)

[3] Department of Defense Mobile Device Strategy, Version 2.0, Office of the DoD Chief Information Officer, (May 2012), 1; Department of Defense Mobile Device Strategy. Version 2.0 (dtic.mil)

[4] Committee on National Security Systems (CNSS) Directive (CNSSD) No. 510, Directive on the Use of Mobile Devices Within Secure Spaces, (November 20, 2017); 3; CNSS Directive No. 510, Directive on the Use of Mobile Devices Within Secure Spaces, dated 11-20-2017 — NNSA Directives (doe.gov)

[5] DOD Digital Modernization Strategy, (July 12, 2019); 14; DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF (defense.gov)

[6] Department of State Bureau of Intelligence and Security Strategic Plan; (2022); 5; INR_Phamplet_Spread.pdf (state.gov)

[7] FY 2024 National Defense Authorization Act (NDAA) Section 1552; Management by Department of Defense of mobile applications.

- *2024:* Intelligence Community Directive (ICD) 123 is projected to provide IC policy to allow wireless capabilities in secure spaces.

"From office productivity to tactical operations, the potential for mobile devices to strengthen the DoD workforce is manifold." DoD Mobile Device Strategy, 2012[8]

The USG legislation and guidance recognizes the benefits of enabling workforces through mobile communications. A sampling is shown in Figure 1.

- Increased productivity, innovation, creativity
- Availability of increased computing power in all environments
- Higher probability of retention of people in the secure workforce
- Attracting and empowering technology-native generations
- Increased security through application and device control
- Lower probability of burnout
- Increased collaboration with geographically separated teammates
- Lower barriers to sharing and reduction of inefficient stovepipes
- Increase ability to use modern technology and software in classified environments
- Increased flexibility and mobility for the workforce

Figure 1: Benefits of Increasing Mobility in Secure Work

Improvements in platform computing power and security contribute to the popularity and utility of mobile devices. Common mobile phones have more Random Access Memory (RAM) than high-end laptop computers.[9] Modern IOS and Android phones feature enhanced security such as protected key storage. Technology for secure PKI-enabled SIPRNet connectivity through remote workstations or approved secure tablets also exists and is in wide use.

However, adoption of mobility is inconsistent across agencies. Mobile devices remain banned from most secure workspaces. Employees lack secure mobile devices to conduct their work while traveling or deployed, personnel use undesignated personal mobile devices for official work, and cannot move seamlessly in and out of workspaces.

Banning mobile devices from secure workspaces is particularly inefficient. People lose access to communications, critical information, files and calendars. This impedes productivity and mission success. Separating employees from their physician-prescribed wearable medical devices presents health risks, undesirable work conditions, and even legal liability. Such an environment also challenges organizations to attract, retain and engage mobile natives and

[8] DOD Mobile Device Strategy, 2012, 1.
[9] TechFow, Are Phones More Powerful Than Computers (Detailed Response!) (October 18, 2022); https://www.techfow.com/are-phones-more-powerful-than-computers-detailed-response/?expand_article=1

others used to working – and living - on their mobile devices. The desk-centric model that is most common in secure workspaces is an antiquated antithesis of the workplace of the future.

One significant reason that mobile communication is not fully implemented in the USG is that the nature of mobility inherently incurs some level of security risk. Our community must understand the current risks in order to mitigate them and unlock the potential of the secure workforce.

The Risks: Identifying and Mitigating the Risks Mobile Devices Present to Secure Work

A modern mobile phone commonly operates as many as 10 communication systems. A report in the *Cipher Brief* from 2023 summarizes security concerns; "Devices that photograph and connect to an outside signal are therefore highly problematic. In fact, any electronic devices that can be used to snap images or take audio recordings are explicitly banned.[10]

If uncontrolled or not disabled, the mobile device communications capabilities can certainly present security risk. Devices that connect from within a secure space are vulnerable to adversary eavesdropping, malware insertions, microphone or camera activation. 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. Malicious or careless insiders may intentionally or inadvertently capture and depart the secure area with sensitive information. The Ukraine war also shows the deadly impact of using unsecured cell phones on the modern battlefield. There, the signatures of unshielded cell phones have proven detectable, and targetable. "Russian artillery has rendered maneuver difficult and command posts unsurvivable," is how one US division commander describes the effect of unsecured mobility.[11]

> *"I think our addiction to cellphones is equally as threatening," Taylor said. "This is the new cigarette in the foxhole."* MG Curtis Taylor, quoted in the Washington Post

Comprehensively mitigating such risks and allowing widespread use of mobility has historically been challenging for the USG. Now, our community has the policies and procedures to address the concerns and enable secure work of the future.

[10] Cipher Brief; Leak Questions Begin To Center Around A Cell Phone,(April 12, 2023); Leak Questions Begin To Center Around A Cell Phone (thecipherbrief.com)

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

Mitigating the Risks

"The ubiquity and diversity of mobile applications, and the typical use of the devices outside the agency's traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstations."[12]

In recent years USG policies established requirements for using mobile devices in secure spaces to mitigate security risks (See Appendix 1, Policies on Mobility). 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.[13] The DOD CISO also approved the CNSS "Directive on the Use of Mobile Devices in Secure Spaces," intended to improve workforce efficiency. The directive outlines the security requirements that mobile device must meet to permit their use within secure workspaces and has other agency approvals from across the government.[14]

Concurrently with the USG emphasis on mobility, the mobile device industry has improved device security and capabilities to the point they now address most security concerns. For example, Apple has conducted Federal Information Processing (FIPS) validations on each new model since 2012. Figure 2 shows the capabilities and security mitigation functions on modern mobile devices and associated architecture tools:

New Mobile Device Security Capability	**Provides Security Function:**
Camera and microphone disabling	Prevents adversary or use activation, and capture/transmitting secure activities
Device radio complete disabling	Adversary location monitoring, activation, eavesdropping, or loading malware
Wireless Intrusions Devices (WIDS)	Alerts Security Managers to presence of a non-approved device in the secure workspace; notifies of camera, radio, network connection
Faraday case storage	Prevents adversary geo-location, eavesdropping, malware loading outside of the secure workspace (i.e. travel, home use)

[12] Department of Homeland Security, Study on Mobile Device Security, (April, 2017); i; DHS Study on Mobile Device Security - April 2017-FINAL.pdf

[13] 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)

[14] CNSS Directive on the Use of Mobile Devices in Secure Spaces; CNSSD 510 dtd 20 Nov 2017.pdf (doe.gov)

Ambient audio masking	Prevents adversary eavesdropping outside of secure workspace
Notification and Alerts for Improper Use	MDM can alert Security Managers to user policy violations, creating audit record to measure compliance
Secure WiFi	For all workspaces, authorized secure WiFi access, allows greater protection, auditability, and option to turn off high power cell radios while connecting to authorized unclassified applications (Outlook, calendar, text, etc)
Secure LiFi	For sensitive workspaces, enable connectivity while adhering to restrictions necessitation lower-power transmitters.
Wearable Health Devices	Deploy capabilities limiting the features of smart devices to only those functions explicitly authorized (e.g., enable BlueTooth, but disable phone, microphone, camera, WiFi, cellular, etc.
COTS software solutions	iOS® and Android™ devices allow secure phone calls and exchange secure messages,
Remote work options	Compartmented, shielded workstations allow PKI-enabled SIRNet connectivity at remote or home workspaces

Figure 2: Security capabilities available with modern mobile device deployments

The combination of device maturity and the research and solutions contained in the USG guidance presents mitigation capabilities for each risk. (See Figure 3)

Risk	**Mitigation**
Physical Security Devices in secure spaces violate many physical security policies. Lack of Wireless Intrusion Devices (WIDS) precludes Security Managers from knowing if unauthorized mobile devices are in secure spaces	● Update policies to be consistent with NDAA 2024, ICD 123, NIST and CNSS guidelines ● WIDS, MDM monitoring
Cyber Security	● Security-focused device selection ● OS, application isolation; application vetting

Connecting to a network is vulnerable to adversary eavesdropping, malware, device activation. Device as an attack vector into the network	• 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 Unified Endpoint Management (UEM) • Mobile Threat Defense • FIPS Encryption for mobile applications • Application-specific security policies • Compliance policies
Human Risk Device activation, information theft by malicious insiders Lack of WIDS to detect use	• UEM technologies • Mobile device security policies • User education • WIDS, MDM monitoring and disabling of device radios • Devices that mask ambient audio, fully disable radio, camera and microphone • Secure storage containers for operational travel
RF Signature Risk Geolocation of user, destruction in combat	• Devices with RF signature masking
Supply Chain Risk Adversary malicious hardware insertion; allows remote activation	• User education • Security-focused device selection
Efficiency Risk Loss of access to files, calendars, constant switching between networks	• Mobile device use IAW policy permits access and proper security
MEDPEDS Risk	• WIDS for unauthorized BLE/MEDPED detection and location

Unauthorized use of smart devices while in the secure area Bluetooth Low Energy (BLE) radio enabled in secure area	• User education on proper use

Figure 3: Mitigations for Risks[15]

With the intent for mobility documented, and security guidelines specified, agencies and organizations are armed with the tools to expand mobility. Senior leaders may proliferate mobility within USG security guidelines, and not incur risk to their information. This will enable secure workforces to maintain access to their information when working in hybrid environments, moving from unclassified to secure offices, and on the go.

Commercial, independent platforms that meet USG security standards offer readily available hardware and software for organizations to implement published guidance. (See Appendix 2: Existing Solutions for Mobility with Manageable Risk)

As important as these technical solutions are, adopting mobility is a significant cultural change from decades of secure work in traditional spaces. Embracing secure mobility must begin at the senior level and permeate through organizations to succeed. Leaders should follow models for technical and cultural change management, including setting goals, building implementation teams, developing strategies, overcoming resistance, and continual improvement. The change management lifecycle will enable the success of secure mobility.

Implementing the Vision for Secure Work of the Future

This synergy of documented USG intent, legislation, policy, research, device computing power and security guidance forms a foundation that enables us to envision the secure work of the future. Agencies and organizations can now expand mobile communications capabilities across the spectrum of USG work, meeting national intent and keeping pace with commercial technologies.

> "This solution will allow critical work to continue securely and seamlessly outside of traditional secure-processing areas,. . ."
> *MG Mitchell Kilgo, CG, Aberdeen Proving Ground*

A secure work environment of the future must consider the capabilities of modern and emerging communications as well as how our adversaries develop and move information. Considering these factors, Figure 4 shows a vision for secure work in the future :

[15] Partial source: NIST SP 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, Table 1, May 2023

	Enabled by Mobility Function	Resulting In
Productive	• Constant connectivity, access to information through managed devices • Work in any environment through secure devices	Workforce leverages computing power and conducts missions in any environment, in any classification
Secure	• Signatures, conversations, locations, movement masked • Radios, cameras, mics disabled • WIDS detect unauthorized activity • Security-focused device, app selection • Anti-surveillance protection • Ambient audio masked • Security manager alerts, access audits • Employees educated on proper device use • Data management and encryption	Workforce access information across environments without incurring security risk to information, operations or people
Flexible	• Managed and shielded devices allow movement in/out of secure space • Classified tablets allow work from all locations • Continual connectivity, information access	Workforce moves seamlessly across environments without loss of connectivity; enables complete Continuity of Operations
Efficient	• Continual connectivity • Regular updates to EDM-managed devices • Access to information, calendars	Leveraging and managing all required mission information at speeds faster than adversaries
Modernized	• All of the above • Reduces reliance on paper in the office	Enables recruitment and retention of technology-savvy employees who desire a flexible, modern, efficient and effective work environment

		Enables communication and information access with the speed, availability and efficiency expected in the modern world

Figure 4: A vision for secure work in the future

We envision five use cases where applying mobility can bring immediate improvements, and begin creating the secure work force of the future:

Use Case 1: Operational Security: Users need access to classified and unclassified information, in any operational location, without security risk, including protection from communications monitoring, intelligence collection, geolocation. Agencies can address this through:

- Shielded devices and storage containers for operational travel
- Disabled device radios, cameras and microphones
- Controlled architecture connections

Use Case 2: Classified Tablets and Devices: Leaders and operators use authorized classified tablets in many environments: US Government, public and private locations, Research & Development (R&D), others. This includes using the devices inside and outside of secure spaces. The community needs policy and best practices for proper use and to mitigate security risk. Agencies can address this through:

- Risk analysis for designated device use
- Clear requirements for security protections, monitoring, compliance and response

Use Case 3: Workforce Enablement: Workforces in secure facilities struggle to remain connected to an increasingly mobile world and lose efficiency when unconnected. Secure work of the future must reduce the risk of authorized unclassified mobile devices in secure spaces. Agencies can address this through:

- Leverage policies that allow approved mobile devices in secure spaces
- Controlled architecture connections
- Devices that mask ambient audio, disable radios, cameras and microphones
- Develop policy recommendations for proper use

Use Case 4: Signature and Location Management: Government-furnished or personally owned cell phones do not mask transmissions or location data. Adversaries can exploit most devices for information collection, eavesdropping, and geo-location of users. This presents personal and operational security risk, and destruction in combat operations. Agencies can address this through:

- Leverage policies that allow approved mobile devices in secure spaces
- Use devices that mask ambient audio, disable radios, cameras and microphones
- Use secure storage containers for operational travel

- Develop policy recommendations for expanded use

Use Case 5: Wearable Healthcare Technology: Wearable healthcare technology (commonly called "MEDPEDS") such as hearing aids, glucose monitors, heart monitors, and other biosensors are increasing in the health care industry, and vital to employees in every sector. Current policies limit workforce MEDPEDS in secure spaces.

- Assess current and true risk from common MEDPEDS. Use independent testing.
- Recommend policy updates for risk and mitigation approach to allowing MEDPEDS in secure spaces

In the Use Case Annexes that follow, the working group will offer implementation steps for each use case.

Final Thoughts

Every new defense technology has presented both opportunity and risk; the steam engine, railroad, telegraph, radio, radar, the internet. Thoughtful risk management, not risk aversion, has enabled the US to maintain its technological and information advantage.

Mobile communications now present a similar situation. Secure work organizations from the federal level, state and local government, industry and educational institutions all exist in an increasing mobile world where information moves at the speed of 5G networks and human ingenuity. Mobile devices will inevitably become the primary and preferred platforms for communications and work. Restricting secure workforces from mobility denies them the tools they need to remain competitive against adversaries that present existential risks. With adversaries already leveraging technology to its fullest advantage, adopting mobility for the US secure workforce offers more opportunity to catch up than it does risk. Lessons from the Ukraine war prove the physical danger from using unsecured mobile devices. Further, adoption of secure mobility as described above can provide security managers, leaders and investigators with more tools to measure workforce compliance and to take corrective action where necessary. This will support a more productive, flexible and resilient workforce.

The USG encourages mobility for workforce efficiency, satisfaction, safety and operations. Modern and powerful mobile technology, compatible with security standards, is available. Security procedures are documented and ready for implementation. This combination puts the US on the precipice to widely adopt mobility, exponentially boost efficiency, and design a future secure work environment that meets the vision of national intent.

Our adversaries already operate in the future. It's time for the US to catch up.

Enclosures:
Appendix 1: Policies on Mobility
Appendix 2: Existing Solutions for Mobility with Manageable Risk

To be published Spring 2024
Annex 1: Operational Security
Annex 2: Classified Tablet and Devices
Annex 3: Workforce Enablement
Annex 4: Signature and Location Management
Annex 5: Wearable Healthcare Technology

Appendix 1: Policies on Mobility

Policy	Mobile Use Requirements and/or Standards
CNSS Directive 510: Directive on the Use of Mobile Devices Within Secure Spaces*	Section V: standards for continuously monitoring for unauthorized activity, microphone use, camera functions, malicious applications, and unauthorized connections to the internet, other devices, or systems
NNSA Supplemental Directive 470.6: Technical Security Program	Attachment 6, Section T: standards for rendering device camera and microphone secure; radio identification numbers; EMM/MDM for prevention of manipulation
DOD Instruction 8420.01: Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies	Section 3.6: standards for device with RF transmitter separation from classified processing equipment and TSCM requirements
NIST SP 800-124r2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, May 2023	Comprehensive guide to mobility requirements, issues, risks, and strategies for risk mitigation
NIST SP 800-37: Risk Management Framework for Information Systems and Organizations	Lists steps in applying Risk Management to mobile uses
NIST SP 1800-22: Mobile Device Security: Bring Your Own Device (BYOD)	Overall guidance on implementing BYOD solutions
NIST SP 1800-22C: Mobile Device Security: Bring Your Own Device, How To Guides	Procedures for implementing BYOD solutions
CNSS Policy 11: National Policy Governing the Acquisition of IA and IA-Enabled IT Products; June 2013	Recommends use of COTS products for solutions when they meet organization security requirements
CNSS Policy 17: Policy on Wireless Systems, January, 2014	Section V: Requirements for WIDS
NSA Mobile Device Best Practices; October 2020	Recommends smartphone users utilize a protective case with audio masking and camera blocking

* The Committee on National Security Systems (CNSS) is resident in the Secretariat of the NSA, is chaired by the DOD CISO, and includes 24 agencies and departments across the USG: About CNSS
HYPERLINK https://www.cnss.gov/CNSS/about/about.cfm

Appendix 2: Existing Solutions for Mobility with Manageable Risk

The following is a short list of commercial off the shelf management and technical solutions for applying mobility when integrated under national guidance and policy (listing does not constitute endorsement):

COTS	Application
IBM	Mobile Device Management policy
Kryptowire	Application Vetting
Trusted Systems	Tempest proof safes for SIPRNet with access control; integrated into office suites for home or office. In use by DOD.
Samsung	Samsung smartphones paired with Privoro anti-surveillance technology allow for mitigation of smartphone radios
PaloAlto	Firewall and Virtual Private Network, encrypted channels between mobile devices and other hosts
Qualcomm	Trusted Execution Environment to protect mobile devices from computer code with integrity issues
Zimperium	Mobile Threat Defense detects unauthorized activity
Privoro	Anti-surveillance devices for mobility; mobile signature management and hardware based radio control, secure comms
Bastille Networks WIDS	Detects cellular, WiFi, and BlueTooth using 100% passive software defined radios
iOS and Android platforms	Protected storage, hardware-backed security to store certificates and keys, and detect device compromise; protects verified boot process and prevents jailbreaks and rooting.
BlackBerry	Unified Endpoint Management, secure containerization and data/voice encryption

Partial source: NIST SP 800-22, Mobile Device Security, Bring Your Own Device (BYOD), Volume A, November 2022, 2.