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

White Paper Annex 2
How to Enable the Secure Workforce of the Future by Implementing Classified Tablets and Phones

ATARC The Future of Secure Work Working Group

September 2024

ATARC

Advanced Technology Academic Research Center

Table of Contents

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), Samuel Moser (US Department of Commerce, NTIA) and James Stanger (CompTIA), for their insights on this paper.

Annex 2: How to Enable the Secure Workforce of the Future by implementing Classified Tablets and Phones

The Situation: The US Government (USG) is facing an amazing time of improved connectivity and efficiency. Thanks to advances in mobile device hardware, software and architectures, USG personnel can now access information up to the Top Secret level in a variety of environments from secure fixed facilities and on operational missions, with increased security measures in place.

This advancement is the product of decades of work. As far back as 2012, a DOD Mobile Device Strategy advised embracing across all classification levels to improve productivity. The Defense Information Systems Agency (DISA) continued that concept in 2017 with the Defense Mobility Classified Capability-Secret (DMCC-S) with tablets and phones for key leaders to access classified information on the move. Popularity of the program contributed to its expansion for information at the Top Secret level. The DOD offers the DMCC-S and DMCC-TS capabilities to all US Government (USG) agencies.

While currently operating on a limited scale, these programs offer tremendous capabilities. Consistent physical risk mitigation and training can help expand the programs and possibly even replace the need for fixed classified facilities.

DMCC-S Security Features

- Phone calls securely placed through Cellcrypt for Classified

- Embedded Federal Information Processing Standards (FIPS) IP Security (IPSec) Virtual Private Network (VPN) accessible through native Samsung VPN client

- Pre-loaded items managed through Quark Security Shield for streamlined, user-friendly interface

- Data-in-transit protection

- Remote device wipe capability

***Source:** DISA Fact Sheet*

Classified work has historically been conducted within government fixed facilities with strict rules limiting exposure to uncleared personnel and uncontrolled electronics that may act as espionage devices – actively listening and watching.

For example, smartphones are banned from fixed facility classified workspaces because of the risk they may record classified matter via the camera or microphone. Physically banning those devices from entering the facility is the mitigation.

Similar security concerns exist when an organization introduces classified mobile devices. Organizations inform employees to be aware of uncleared listeners, but physical bans on unclassified or personal smartphones near the classified device are not reasonable. This is a challenging risk to mitigate. Now, new technologies that physically control risks of exposing the camera and microphone and controlling the radios on an unclassified government issued or personal smartphone are becoming available.

Embracing these new technologies that physically control the active espionage risk, and thorough training can enable employees to use the classified devices with proper security

practices that fully protect the information. Uniform security practices across agencies will close gaps that adversaries would otherwise exploit. Both will enable employees and organizations to expand classified tablets and devices with confidence, contributing to secure mission accomplishment.

This paper presents a series of recommendations and considerations as "Pro Tips" to successfully implement secure tablet and phone programs.

Goal: Enable your workforce to leverage secure tablets and phones in remote work environments while mitigating security risks, while increasing compliance and auditing, and adhering to applicable policy and risk-mitigation strategies. Recognizing the breadth of USG missions, this can include the entirety of the workforce across all agencies, units and environments.

Who Benefits from Classified Connectivity?

- Senior leaders
- Official travelers
- Multi-tasked professionals
- Field operators
- Remote workers
- Ship and aircraft crews and supporters
- And more . . .

Resources:

- A fleet of DISA-provided Next Generation Device (NGD), such as the DMCC-S, DMCC-TS or other approved devices
- Associated government-issued hotspots to connect them to the network (VPN/Wi-Fi/Li-Fi)
- Properly-cleared workforce with active classified network accounts
- Wireless Intrusion Devices (WIDS)
- DISA DoD Mobility Classified Capability – Secret Public Facing site: https://storefront.disa.mil/kinetic/disa/service-catalog#/forms/dod-mobility-classified-capability---secret
- DOD Mobility Service Portal: (account enabled)

References:

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

Tips for Implementing Secure Tablet or Phone Programs

Tip 1: Establish a program that embraces the mission enhancements of modern classified mobile computing capabilities

Using classified devices outside of secure spaces can be a substantial departure from ingrained practices for many employees and organizations. Employees may fear the consequences of security mistakes or simple human error. However, consider that national level organizations have been using classified tablets inside and outside of designated secure spaces for years.

Leaders should overcome such legitimate issues by establishing the program as one that is important for mission accomplishment. Embrace technologies that provide physical controls over the active espionage risk from other unclassified mobile devise, provide training on properly mitigating the risk of uncleared people near classified mobile, and encourage savvy use and emphasize that self-reported security mistakes do not incur punitive measures against employees, within applicable regulations. The DMCC-S and TS are designed to minimize security risk. Establish the program to trust and maximize the built-in security capabilities.

Tip 2: Apply change management that embraces new technologies that reduce the risk of active espionage while embracing classified mobility

Consider applying change management theory to help establish the program, recognizing Tip 1. At the national level, organizations already used change management principles to successfully manage classified tablets moving in and out of secure spaces – with no security degradation.

To expand that concept, what leaders, units, systems or management changes need to be considered to implement a classified tablet or device program? Discussing mobile solutions 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.

The journey from the conceptual framework to the tangible implementation of secure mobility 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.

Tip 3: Conduct a Risk Assessment

Security risk is inherent in all communications. Conducting a thorough risk assessment is the USG-approved process for identifying the true risk to organizational activities and mitigating those risks through focused security measures, tailored for each organization and employee.

Start the process by engaging the organization's supporting counterintelligence (CI) and security personnel. Outline the environments where employees will use the classified tablets and phones. Identify with them the known or suspected adversarial threats. For example, certain areas or travel locations may present particular vulnerabilities to adversary cyber collection, eavesdropping, or criminal theft. Develop mitigations for each risk and communicate recommendations to employees.

Review, create or update the system security plan for use of the classified tablets or devices.

- If a system security plan does not exist, create one using Risk Management Framework and guidelines in NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems.
- Include a Risk Assessment at the Information Systems level. The Risk Assessment should consider organization-specific security requirements, threat information, or special circumstances.
- If the Risk Assessment does not exist or address the factors above, consider creating one using procedures in NIST SP 800-30, Guide for Conducting Risk Assessments.
- As stated in Chapter 2 of NIST SP 800-30, organizations may conduct a targeted risk assessment, where the scope is narrowly defined, to produce answers to specific questions. Figure 1 shows the NIST Risk Assessment process:

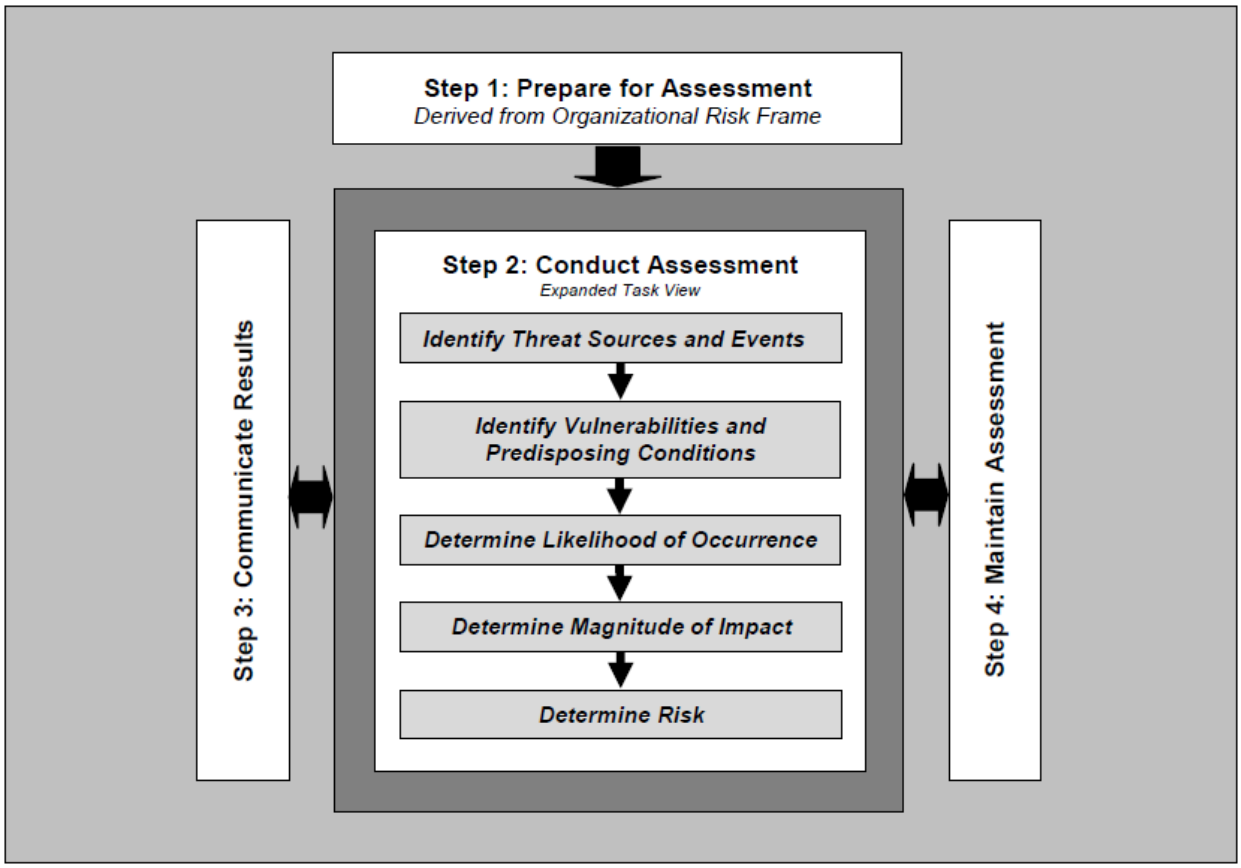

Figure 1: The Risk Assessment Process (see NIST SP 800-30)

Tip 4: Employee education and technology risk mitigation programs

It is crucial that employees fully understand risks associated with system use and know their mitigations. Review Tips 1-3 above and develop mitigation measures that the organization or users can reasonably apply. The table below shows an example of risks and mitigations:

Environment	Risk	Risk Tolerance	Mitigations
Residence	Unauthorized network connection	Low	Use only program-issued hot spot to connect to authorized network Use endpoint authentication technologies for monitoring of the mobile devices connecting
	Device RF collection	Low	Use hardware-shielded devices that physically control or monitor the radios of the classified and unclassified or personal devices that may be present
	Overheard classified conversations	Medium	Use headphones for audible conversations and hardware shielded technologies that block microphones for unclassified and personal mobile devices that may be present
	Observed classified work	Medium	Shield device screen from view Close room doors/blinds/curtains during classified work Use hardware shielded devices that block cameras on unclassified and personal mobile devices that may be present
Travel	Adversary eavesdropping or device manipulation	Low	Consult with supporting CI office on known or suspected adversary risk
Office	Unauthorized mobile devices mixing with approved devices	Low	Use wireless intrusion detection (WIDS) and endpoint authentication technologies for monitoring of the mobile devices in the facility
	Camera or microphone activation	Medium	Use hardware shielded devices that disable mic and camera with monitoring to confirm appropriate use

Table: Examples of risks, tolerance and mitigations

- **Create Employee Training Program**. Educate employees on 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. Leader examples and solid program establishment as discussed in Tips 1 and 2 will be crucial for successful education.

Tip 5: Continually measure compliance

Adjust and revise security practices based on lessons learned. Figure 2 below shows the entire step-by-step process.

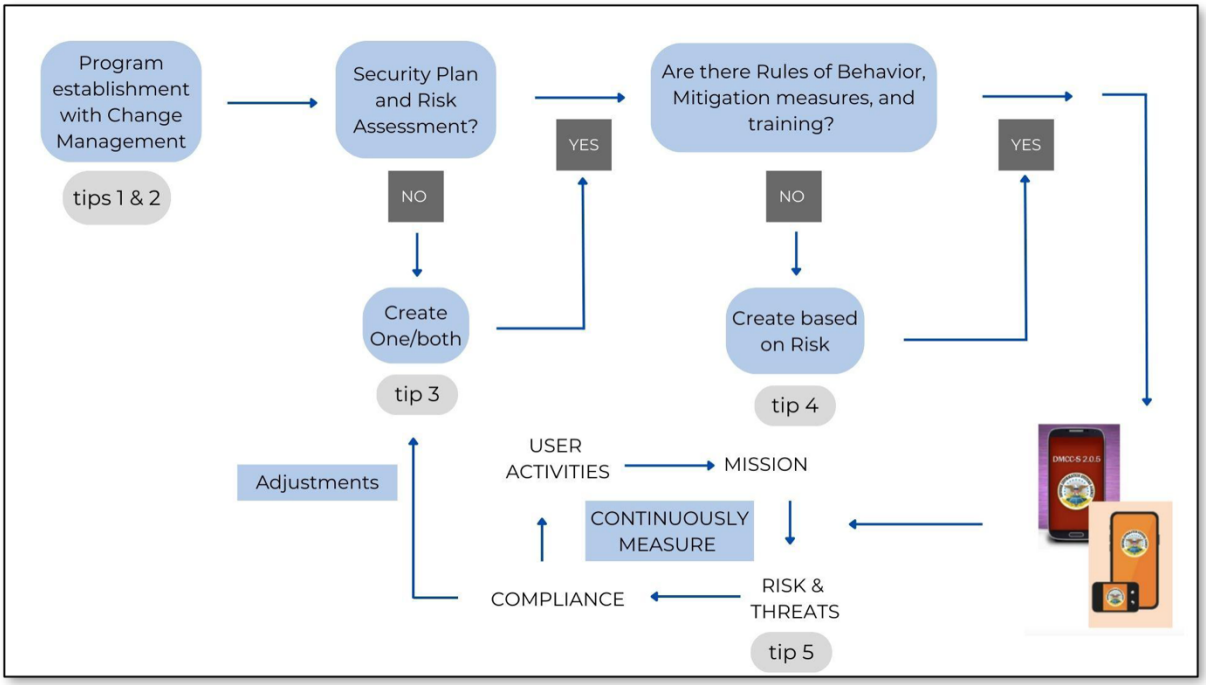

Figure 2: The step-by-step process for implementing secure tablets or phones with security guidance

Conclusions

Published USG strategies, requirements, and lessons from Ukraine battlefields all point to the need and utility of secure mobile communications. Now, government-designed secure mobile tablets and devices combine connectivity, efficiency and security. They are enabling the USG to meet its own published vision. All that is needed now to capitalize on these innovative devices and fully attain the USG intent is broad implementation across agencies and environments.

While small today, these programs offer tremendous capabilities. They can be even more effective and truly empower workforces with consistent physical risk mitigation and training, enabling these classified mobile capabilities to continue to grow and possibly even replace the need for today's fixed classified facilities

The steps and tips in this paper can help implementation with thorough security and enable organizations to maximize communications to accomplish their respective missions.
In the next conflict, our adversaries will move information quickly and across classifications. The USG needs to fully leverage classified mobility to defeat them. Adoption of secure mobility now will defend US national security in the future.