**Committee on National Security Systems**

**CNSS Directive No. 510**
**20 November 2017**


# DIRECTIVE ON THE USE OF MOBILE DEVICES WITHIN SECURE SPACES

THIS DOCUMENT PROVIDES MINIMUM STANDARDS FOR NATIONAL SECURITY SYSTEMS. IT ALSO MAY OFFER GUIDELINES FOR THOSE PERFORMING THE SAME FUNCTIONS FOR NON-NATIONAL SECURITY SYSTEMS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENATATION.

# CHAIR

## FOREWORD

1. Committee on National Security Systems (CNSS) Directive (CNSSD) No. 510, *Directive on the Use of Mobile Devices Within Secure Spaces*, specifies instructions to control the introduction and use of mobile devices in secure spaces, both domestic and overseas, as defined herein.

2. Implementation of this Directive does not preclude the application of more stringent requirements and, independently, may not satisfy the requirements of other security programs, such as TEMPEST, Communications Security, Operations Security, or Overseas Security Policy Board (OSPB) Standards.

3. CNSSD No. 510 is effective upon signature.

4. Copies of this Directive are available from the Secretariat, as noted below, or the CNSS Web site: www.cnss.gov.

/s/

Essye B. Miller

**CNSS Secretariat. National Security Agency. 9800 Savage Road, STE 6165. Ft Meade, MD 20755-6716**
**Office: (410) 854-6805**
**cnss@nsa.gov**

**DIRECTIVE ON THE USE OF MOBILE DEVICES WITHIN SECURE SPACES**

# Table of Contents

## SECTION I – PURPOSE

1. The U.S. Government (USG) relies on mobile technologies to provide USG Departments and Agencies (D/As) increased productivity and mission flexibility. The introduction of mobile devices into secure spaces may pose risks to National Security Systems (NSS) and the information contained therein. D/As will take physical and technical security measures to mitigate these risks.

2. This Directive provides a minimum set of requirements for the introduction and use of mobile devices in secure spaces. D/As may develop internal policies and procedures to supplement the requirements of this Directive to ensure the introduction of mobile devices into secure spaces does not adversely impact the security of NSS.

## SECTION II – AUTHORITY

3. This Directive derives its authority from National Security Directive 42, which outlines the roles and responsibilities for securing national security systems (Reference a), consistent with applicable law, E.O. 12333, as amended, and other Presidential directives.

4. Nothing in this Directive should be interpreted as altering or superseding the authorities of the Director of National Intelligence.

## SECTION III – SCOPE

5. This Directive applies to all D/As employees, contractors, agents, and visitors who have access to secure spaces where NSS are employed.

6. This Directive applies to the introduction and use of mobile devices (regardless of ownership) in secure spaces where NSS are employed.

7. This Directive does not apply to Sensitive Compartmented Information Facilities (SCIFs) or Special Access Program Facilities (SAPF).

## SECTION IV – POLICY

8. For secure spaces under their purview, D/As will:

a. Establish and document procedures in accordance with this Directive to govern the introduction and use of USG managed mobile devices in secure spaces.

NOTE: The use of the phrase “mobile device(s)” in this directive means “USG managed mobile device(s)” as defined in Section VI of this Directive, unless otherwise stated.

b. Document a justification based on mission need prior to approval and introduction and/or use of a mobile device in a secure space. Examples of mission need include: command, control, and communication, counterintelligence, cover, testing, training, research, and development activities.

c. Designate a Cognizant Security Authority (CSA), or designee, at each D/A to serve as the approval authority for the introduction and use of mobile devices in secure spaces.

d. The CSA will complete the following actions prior to approving the introduction and/or use of a mobile device in a secure space:

i. Consult with the Authorizing Official(s) (AO) of the mobile device and NSS, and with the servicing technical surveillance counter measures (TSCM) organization.

ii. Obtain risk input and TEMPEST countermeasures guidance from the Certified TEMPEST Technical Authority (CTTA) and TSCM servicing organization, and accept any residual risk of compromise in writing, if any additional countermeasures are not implemented.

iii. Document a risk determination associated with a given mobile device and its capabilities. A risk determination may apply to a specific mobile solution (e.g., the Department of Defense Mobile Unclassified Capability) or to an entire class of mobile devices (e.g., wearable fitness devices). When making risk determinations, the CSA will consider the:

1. Vulnerabilities associated with the mobile device, any NSS it may interact with, and any network(s) or Information System(s) it may connect to within the secure space or any adjacent space at the same or higher classification level;

2. Known and potential threats to NSS and/or information stored, processed, discussed, or transmitted within secure spaces;

3. Sensitivity and classification level of the information contained within the secure space, network, IS, mobile device, and the impact of its compromise or disclosure;

4. Adjacent spaces not under their control, and coordinate with their CSA to make an appropriate risk determination; and

5. Potential impact to facility’s vulnerability to technical attack.

Note: This Directive is intended to give the CSA flexibility in making risk determinations. The CSA may disallow the introduction and use of a mobile device in one secure space but allow the introduction and use of the same mobile device in another secure space, based on the CSA's risk determination and the considerations above. For example, an increased adversarial threat in a secure space at an overseas location or the presence of highly sensitive

information in a secure space may lead the CSA to prohibit mobile devices based on their risk determination. In cases where information regarding the considerations above is not readily available, the CSA is encouraged to consult the resources located in Annex B for guidance when making risk determinations.

iv. Ensure the mobile device is certified against the requirements of the National Information Assurance Partnership Program in accordance with CNSS Policy (CNSSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enable Technology Products," dated June 2013 (reference e).

e. Include the following requirements in the documented procedures:

i. Use and control of the mobile device is specified in the D/A's policies and standard operating procedures.

ii. The user of the mobile device will safeguard the device in accordance with requirements for configuration, control, and as specified in training for the use of the device regardless of location.

iii. The mobile device will be made available periodically and on demand to D/A authorities for configuration verification, security updates, search and/or seizure;

iv. The mobile device will be continuously monitored for unauthorized activity such as microphone use, camera functions, malicious applications, and unauthorized connections to the internet, other devices, or systems;

v. Aforementioned device capabilities which introduce risk to classified spaces will be disabled when not in use; and

vi. Wireless systems and networks employed within secure spaces comply with the requirements in CNSSP No. 17, *Policy on Wireless Systems* (Reference d).

f. Document and implement physical, technical, supply chain, and counterintelligence mitigations to reduce risk to an acceptable level. The process to evaluate devices will be reviewed, at minimum, annually to ensure all associated risks are adequately mitigated. Mobile devices, and their capabilities, will be reviewed on a continuous basis to ensure all associated risks are adequately mitigated.

g. Document specific procedures for mobile devices which are approved to connect to a government NSS in secure spaces to include, at a minimum, the following:

i. The mobile device is authorized by the AO for the Information System (IS) and the user consents to continuous monitoring;

ii. Proper use and control of mobile devices is specified in the D/A's System Security Plan for the NSS to which the mobile device is connected;

iii. If connecting to a classified NSS or used to store, transmit, or process National Security Information (NSI), the mobile device will meet one of the following requirements:

1. Compliance with a Commercial Solutions for Classified (CSfC) Capability Package as described in CNSS Policy No. 7, *Policy on the Use of Commercial Solution to Protect National Security Systems* (Reference f);

2. Approval by the National Manager as a tailored solution; or

3. Certification as a National Security Agency (NSA)-certified product.

h. Ensure that mobile devices only connect to information systems at the same classification level and are never connected across security domains (e.g., unclassified IS to a classified IS).

i. Develop and implement procedures to ensure mobile devices removed from a secure space, or disconnected from an NSS, are continuously monitored for compromise, suspicious activity, and not used to exfiltrate sensitive or classified information.

j. Establish requirements for (re)introducing mobile devices into secure spaces after they have been taken outside of the United States. D/As will specify the appropriate device configuration prior to travel, an incident reporting process, procedures for reconfiguration, procedures for complete or partial wipe, and other approved mitigations prior to its (re)introduction into the secure space.

k. Comply with all applicable laws and presidential directives when making a determination on the introduction of medical devices (e.g., Bluetooth®-enabled hearing aids) into a secure space. Nothing in this Directive alters or supersedes D/As' legal or policy requirements regarding accommodation of employees' medical needs. D/As will have procedures for determining whether such technologies may be permitted into their secure space.

l. Ensure official job-related mobile devices carried by emergency personnel (e.g., fire, medical, police) responding to a crisis within a secure space will be admitted into the secure space without regard to the security status of the mobile devices, provided such devices are required for official job-related communication. Emergency personnel carrying such mobile devices should be escorted to the degree practical. Where possible, D/As will debrief such emergency personnel, and/or examine their mobile devices to ensure that they do not contain classified information.

m. Provide annual training in accordance with Reference d and any local D/A requirements.

9. For secure spaces in overseas locations, executive branch D/As and their employees under Chief of Missions (COM) authority (except for employees under the command of a

United States area military commander) will conform to the Overseas Security Policy Board (OSPB) Standards and Policies (Reference g).

10. When two or more D/A's agree to allow each other's mobile devices within shared or adjacent secure spaces, they will document such agreement via a written Memorandum of Agreement, as appropriate.

11. Non-USG managed mobile devices are prohibited in secure spaces. Heads of D/As may grant waivers on behalf of their D/A on a case by case basis. Waivers will document the mission need and any provisions in Section IV of this Directive which are not satisfied. The use of waivers must be compliant with applicable Executive Orders, statutes, and regulations. The continuing need for any such waiver will be reviewed, at a minimum, annually or whenever relevant changes occur to the non-USG managed mobile devices' capabilities and/or the D/A's threat environment.

## SECTION V - RESPONSIBILITIES

12. Heads of D/As will:

a. Develop, implement, and manage programs necessary to ensure that the requirements of this Directive are implemented and adequately resourced, and the plans, programs, and CNSS issuances that implement this Directive are fully supported;

b. Ensure that AOs, CSAs, CTTAs, and TSCM practitioners are appropriately trained and authorized to make appropriate risk determinations; that they have access to threat, vulnerability, and technical information required to conduct the risk assessment; and that they are held accountable for their determinations;

c. Assess the risks associated with introducing various mobile technologies and their capabilities into secure spaces using applicable risk guidance documentation;

d. Enforce any decision made by the appropriate CSA to prohibit mobile devices in secure spaces under their purview;

e. Incorporate the proper introduction and use of mobile devices into secure spaces as a point of interest in the D/A oversight, inspection, and review process;

f. Review and revise annually their programs to reflect the advancements in technology and the emerging security threats and risks associated with the use of mobile devices in secure spaces; and

g. Incorporate the content of this Directive into applicable user and administrator education, annual training, and awareness programs.

## SECTION VI – DEFINITIONS

13. The following definition is provided to clarify the use of a specific term or phrase contained in this Directive. All other terms used in this Directive are defined in CNSSI No. 4009, *Committee on National Security Systems (CNSS) Glossary* (Reference k).

a. Secure Space: A secure space is defined as a building, facility, or controlled area (whether permanent, temporary, or mobile) that meets all of the following criteria:

i. Contains NSS;

ii. Is operated by a USG D/A, U.S. or Allied Military Command, an appropriately cleared contractor, or a State, Local or Tribal government;

iii. Is protected at a level commensurate with the classification or sensitivity of the information that is processed, stored, used, or discussed therein;

iv. Falls under the responsibility of a Cognizant Security Authority (CSA) or Senior Agency Official responsible for ensuring the physical and technical security of the space; and

v. Is not an accredited SCIF or SAPF.

Note: Secure spaces may include Special Access Program Facilities, as well as facilities that contain nuclear command and control materials or related information, that are not SCIFs. Secure spaces may also contain NSI commensurate to the level of the accreditation of the secure space. For policy applicable in SCIFs, see Appendix B, Resources 1. a.

The definition of secure spaces does not apply to unclassified lab environments where mobile devices may be introduced exclusively for official research, analysis, or testing purposes. D/As will ensure that the introduction of mobile devices into lab environments does not subject sensitive information (e.g., personally identifiable information) used or stored within the space to potential compromise.

b. USG Managed Mobile Device: A mobile device under the control and management of a USG enterprise system (i.e., Mobile Device Management, Enterprise Mobility Management, Active Directory, etc.) capable of enforcing and monitoring security controls, configuration settings, and compliance in accordance with D/A minimum standards.

c. Non-USG Managed Mobile Device: Does not meet the definition of a USG Managed Mobile Device.

## SECTION VII – REFERENCES

14. References applicable to this Directive are contained in Annex A.

# ANNEX A

## REFERENCES

a. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 5, 1990.

b. Executive Order 12333, *United States Intelligence Activities*, as amended, dated July 30, 2008.

c. CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, June 2013.

d. CNSS Policy No. 17, *Policy on Wireless Systems*, January 2014.

e. CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014.

f. CNSS Policy No. 7, *Policy on the Use of Commercial Solutions to Protect National Security Systems*, December 9, 2015.

g. The Overseas Security Policy Board Standards and Policy 12 FAH-6.

h. CNSS Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015.

# ANNEX B

## RESOURCES

1. This Annex identifies resources available to CSAs when making risk determinations in accordance with this Directive. The documents listed below provide general guidance that may be helpful, but are not intended to apply to all risk decisions.

    a. ICD 705 Technical Specifications, Chapter 10: This document contains the Intelligence Community's guidelines for making risk determinations applicable to SCIFs. Generally, restrictions for SCIFs should be more stringent than secure spaces, but the guidelines in Chapter 10 may serve as a resource for CSAs when making risk determinations for secure spaces.

    b. CSfC Capability Packages (CPs) and Risk Assessments: NSA's CSfC program allows D/As to implement NSA-approved Commercial-Off-The-Shelf solutions to protect NSS. CSfC solutions are configured according to guidance in the applicable CP. NSA provides a classified Risk Assessment of each type of CSfC solution, providing AOs with information on the residual risk associated with the solution (see Reference f for more information). The CSA is encouraged to consult these documents when determining a risk associated with introducing mobile devices that are part of a CSfC solution into the secure space.

    c. Intelligence Community Wireless Steering Committee: Intelligence Community (IC) Wireless Steering Committee (WSC) is the primary advisory body to the Director of National Intelligence (DNI) for the introduction of wireless technology, wireless-enabled devices, and their associated infrastructure with the IC. The WSC comprehensively addresses wireless technology and the risk mitigation approach surrounding its use within SCIFs or connected to IC networks.

    d. CNSSP No. 17, Annex B: This Annex contains references to general standards and best practices documents, including relevant National Institute of Standards and Technology publications. Although these documents are not specific to introducing mobile devices within secure spaces, they may be a source of information for CSAs.

# ANNEX C

## ACRONYMS

| | |
|---|---|
| AO | Authorizing Official |
| CNSS | Committee on National Security Systems |
| CNSSD | Committee on National Security Systems Directive |
| CNSSI | Committee on National Security Systems Instruction |
| CNSSP | Committee on National Security Systems Policy |
| CP | Capability Package |
| CSA | Cognizant Security Authority |
| CSfC | Commercial Solutions for Classified |
| CTTA | Certified TEMPEST Technical Authority |
| D/A | Departments and Agencies |
| ICD | Intelligence Community Directive |
| IS | Information System |
| NSA | National Security Agency |
| NSI | National Security Information |
| NSS | National Security Systems |
| OSPB | Overseas Security Policy Board |
| SCIF | Sensitive Compartmented Information Facility |
| USG | U.S. Government |
| WSC | Wireless Steering Committee |