

Approved: 07-15-19

Expiration: 07-15-20

**SUBJECT: USE OF MOBILE DEVICES WITHIN NATIONAL NUCLEAR
SECURITY ADMINISTRATION SECURE SPACES**

PURPOSE: This Advance Change Directive (ACD) provides guidance on the implementation of Committee on National Security Systems (CNSS) Directive (CNS SD) 510, *Directive on the Use of Mobile Devices Within Secure Spaces*, and specifies the minimum set of requirements to control the introduction and use of mobile devices in National Nuclear Security Administration (NNSA) secure spaces.

URGENCY: CNSSD 510, binding on all federal departments and agencies, became effective November 20, 2017. The capabilities of mobile devices, their prevalence, and their usage in unprotected environments pose significant risk to NNSA secure spaces and information systems and require a vigilant security approach.

APPLICABILITY: This ACD applies to all NNSA employees, contractors, and visitors who have access to secure spaces within which a national security system (NSS), as defined by CNSS Instruction 4009, is physically present.¹ For the purposes of this ACD, mobile devices do not include laptop computers. This ACD does not apply to Sensitive Compartmented Information Facilities.

SUMMARY

1. The Chief, Defense Nuclear Security (CDNS) is the Cognizant Security Authority (CSA) for NNSA and serves as the approval authority for the introduction and use of mobile devices in secure spaces. This authority has been delegated to Field Office Managers, NA-15, NA-30, and NA-84. Through this delegation, Field Office Managers may delegate this authority to their respective Assistant Managers for Safeguards and Security.
2. These instructions must ensure that, prior to approving the introduction or use of a mobile device in a secure space, the approval authority:
 - a. Documents a justification based on mission need,
 - b. Documents a risk determination, in accordance with the criteria outlined in CNS SD 510, associated with a given mobile device or class of mobile devices,

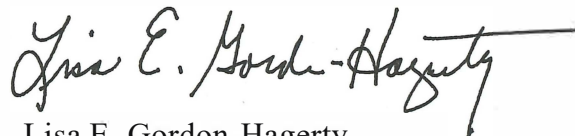
¹In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified in 50 U.S. Code sections 2406 and 2511, and to ensure consistency throughout the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

- c. Obtains risk input and countermeasures guidance from the Authorizing Official, Certified TEMPEST Technical Authority, local Technical Surveillance Countermeasures (TSCM) team, and the CSA of any adjacent security area.
 - d. Accepts residual risk of compromise in writing for any recommended countermeasure not implemented, and
 - e. Implements physical, technical, and supply-chain mitigations required by CONS, NNSA, Department of Energy (DOE), and national policy.
- 3. The CDNS will establish detailed instructions regarding these requirements for the approval, introduction, and use of mobile devices in secure spaces to establish a security baseline for the enterprise within 60 days of publication of this ACD.
 - 4. NNSA secure spaces include all Material Access Areas, Protected Areas, Vault-Type Rooms, special designated areas, and areas requiring recurring TSCM services. NNSA secure spaces also include Limited Areas, or any portion thereof, to include an individual room, within which, any NSS is physically present. Sufficient electromagnetic and acoustical isolation can be used to segregate secure spaces within larger Limited Areas.
 - 5. Mobile devices are prohibited within areas requiring recurring TSCM services, as defined in DOE Order 470.6, *Technical Security Program*.
 - 6. All camera functions must be disabled and all microphone functions must be restricted to only the native telephone application while in secure spaces. Exceptions can be approved only by the CDNS when supported by a critical mission need.
 - 7. The NNSA Chief Information Officer (CIO) will document procedures for mobile devices approved to connect to an NSS in secure spaces. The CIO will ensure processes and procedures are in place to provide continuous monitoring of mobile devices for unauthorized connection to the internet or NSS; microphone and camera usage; and exfiltration of sensitive or classified information. Additionally, the CIO will ensure authorized mobile devices are certified against the requirements of the National Information Assurance Partnership Program in accordance with CNSS Policy (CNS SP) 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Technology Products*.
 - 8. Secure spaces operating for longer than 30 days, not restricted to ad-hoc classified discussions by the Officially Designated Federal Security Authority (ODFSA), and authorized for mobile devices, must be equipped to continuously monitor the facility for unauthorized mobile devices. This monitoring must ensure the identification, enumeration, logging, and locating of all authorized and unauthorized mobile devices. Any discovery of an unauthorized device will be forwarded to the local TSCM element to determine the appropriate response. **Note:** Ad-hoc classified discussions must be unscheduled, irregular, infrequent, and not audible for longer than 9 hours in any one calendar month.

9. Secure spaces, within which the only authorized mobile devices are those assigned to protective forces and internal emergency services personnel (e.g., fire, medical, nuclear) whose primary responsibility requires the tactical response to emergencies within the secure space, and who have no other secondary means of communication, are exempt from this continuous facility monitoring requirement. Mobile devices assigned to emergency personnel must remain powered off until required as a secondary means of communication.
10. This ACD prohibits the introduction into secure spaces of personally owned and contractor-owned mobile devices on which the hardware, operating system, and applications are not fully managed by a DOE/NNSA enterprise mobility management system.
11. Approved mobile devices that have traveled outside of the United States or into foreign embassies and consulates may be reintroduced into secure spaces only after cyber security and TSCM evaluations have ruled out the possibility of compromise.
12. The CDNS or ODFSA, along with the CIO, may terminate mobile device approvals in response to an emergency, security breach, or receipt of threat information.
13. Nothing in this ACD alters or supersedes legal or policy requirements regarding accommodation of employees' medical needs. The CDNS will separately document procedures for determining whether such technologies may be permitted into secure spaces.

For questions or comments concerning this ACD, please contact the Office of Defense Nuclear Security at (202) 586-8900.

BY ORDER OF THE ADMINISTRATOR:

A handwritten signature in black ink, reading "Lisa E. Gordon-Hagerty". The signature is fluid and cursive, with a long horizontal stroke extending from the end.

Lisa E. Gordon-Hagerty
Administrator