Sandia National Laboratories

Advanced Change Directive (ACD) 470.6

Frequently Asked Questions

Updated 02/04/2021

What is ACD 470.6?

Advanced Change Directive (ACD) 470.6 is NNSA's implementation plan for the Committee for National Security Systems (CNSS) Instruction 510. ACD 470.6 was signed July 15, 2019 and governs the use of mobile devices within 'Secure Spaces' as defined by the federal requirement.

What is the requirement?

Each DOE site overseen by NNSA must assess its site facilities, identify all 'Secure Space' according to the ACD 470.6 definition, and develop its own implementation plan to comply with the directive by removing mobile devices (smart watches, tablets, personal and government issued mobile phones) from the identified spaces.

What is a mobile device?

A mobile device is a portable computing device that:

- has a small form factor such that can easily be carried by a single individual
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information)
- possesses local, non-removable data storage
- is powered-on for extended periods of time with a self-contained power source

Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, smart watches, tablets (including iPads), and E-readers. Contact Physical Security (Org. 4238) if you have a question concerning if a device meets this requirement.

What is Secure Space?

Following is the NNSA directive definition of Secure Space:

- 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 National Security System (i.e., classified processor) is physically present. Sufficient electromagnetic and acoustical isolation can be used to segregate Secure Spaces within larger Limited Areas.
- TSCM recurring services area (including SCIFs, SAPs, SIGMA, and all classified conference rooms regardless of the level of classified discussed)
- Classified Video Teleconference rooms and Classified Skype rooms.

In simple terms, Secure Space is any location in which classified discussions and/or processing may take place. Project teams have characterized every building within limited areas to identify these spaces. Most building space within Sandia limited areas—except vestibules or entry areas approved for internal storage—will become Secure Space. All Secure Spaces will be well marked with signs.

Does the requirement affect Sandia issued or government issued laptop computers?

No, the directive specifically states that it does not apply to government laptop computers that meet security requirements.

Are there any other devices that are <u>not</u> impacted by the requirement?

The following are specific examples of devices that do not meet the definition of a mobile device and therefore are not impacted by the requirement:

- Devices with storage capability but no ability to process or transmit/receive information (e.g., flash memory cards/sticks)
- One-way pagers
- Traditional two-way radios

How can I locate where Secure Space begins?
Here are some examples of signage you may see on Sandia; these signs indicate the boundaries of Secure Space.

What is the difference between 'mobile devices' (MDs) and 'portable electronic devices' (PEDs)?
ACD 470.6 uses the term 'mobile device' as defined above. The term 'mobile device' is a subset of the Sandia term 'portable electronic device,' which includes mobile devices. Mobile devices are narrowly defined and do not include all PEDs.

Do these requirements apply to SCIFs?
No, these high security areas have separate requirements in place that already prohibit mobile devices within these areas.

Can mobile devices be brought into limited areas?
Yes. Both Sandia owned and personally owned mobile devices may be brought into a limited area boundary. Neither may be brought into areas designated as Secure Space. Since laboratory policy states that classified conversations cannot occur outside, even if within a limited area, it will be permissible for a mobile device to be brought, for example, through a turnstile into Tech Area 1 in New Mexico, provided that all other requirements are satisfied (e.g., Bluetooth and WiFi disabled).

Can visitors or uncleared MOW bring mobile devices into limited areas?
The updated policy will not distinguish between cleared and uncleared Members of the Workforce.

Do Bluetooth and Wi-Fi still need to be disabled in limited areas outside of Secure Space?
Yes, as stated above, the policy regarding Bluetooth and Wi-Fi within limited areas remains in effect—Bluetooth and Wi-Fi must be disabled inside limited areas. (For Sandia owned devices, Wi-Fi may be enabled *only* in an approved Wireless Access Zone.)

If an emergency occurs in Secure Space, how can I call 911?
Sandia desk phones (VOIP phones) should be used to dial 911 in the event of an emergency. Sandia's telecommunications team is actively working to upgrade equipment to improve connectivity of the VOIP phones during network outages.

How can I be sure which storage locations are OK to use right now, and which are not yet approved?
All new storage locations should be marked with this sign. Any existing storage not marked as approved should not be used.

Why are locks being removed from some of the external storage boxes?
Locks were removed in order to ensure that the boxes are available on a first come, first served basis and to eliminate costs associated with key maintenance and replacement.

Can I leave a GPS bike computer (e.g., a Garmin) attached to my bike in the rack?
Yes. A bike computer may remain on the bike in the rack or may be removed and stored in one of the designated, approved storage locations. (Note: It is against laboratory policy to store a bike inside a building.)

What happens if I bring a mobile device into a Secure Space?

If the event involves a potential risk to classified, it will be categorized as a Category B or A incident and will be reported to DOE.

If the event does not involve any potential risk to classified, it will be handled according to an internal categorization process, with the first 3 events being assigned as Mobile Device Warnings. A fourth mobile device event within a rolling 12-month period will be categorized as a Category B incident.

Are any mobile devices allowed in Secure Space?

- R&D projects directly involving mobile devices are not exempt. Contact Richard Schademan if your R&D project surrounds or involves mobile devices.
- Authorized mobile devices assigned to protective forces and internal emergency services personnel (e.g., fire, medical, nuclear), whose primary responsibility requires the tactical response to emergencies within Secure Space and who have no other secondary means of communication, are exempt from the requirement. Mobile devices assigned to emergency personnel must remain powered off until required as a secondary means of communication.
- Medical devices themselves are not restricted by the policy. Nothing in the directive alters or supersedes legal or policy requirements regarding accommodation of employees' medical needs, which continues to follow the Essential Job Function process. However, many medical devices pair with peripheral devices which could meet the definition of a mobile device. Nothing in the requirement makes exception paired, mobile devices, and therefore they are not permitted in Secure Space.
- Controlled articles that do not meet the definition of 'mobile device' which are registered and approved through the Controlled Articles Registration Process (CARP) site (e.g., laboratory testing equipment, cameras), are not restricted by this requirement. Mobile devices currently approved as controlled articles are no longer allowed in Secure Space.

How Do I Report?
Members of the Workforce with SRN access—go to SIMP.sandia.gov to access the Mobile Devices Self-Reporting Tool.

Members of the Workforce without SRN access, or to report on behalf of another person—call **321 from a Sandia landline phone or (505) 845-1321 from any phone.**

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2020-13888 O

Sandia National Laboratories