Advanced Change Directive (ACD) 470.6 – Frequently Asked Questions

The following information is current as of January 13, 2020 and is subject to change.

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.

How do other NNSA sites currently manage mobile devices?
Sandia and Lawrence Livermore are currently the only sites in the complex that allow mobile devices into Limited Areas.

What are the top 5 challenges for Sandia in implementing ACD 470.6?
- Sandia is one of the largest National Security Enterprise complexes with hundreds of buildings across 7 states.
- Implementation across all sites will require significant infrastructure resources, most immediately, a sharp increase in cell phone storage capacity.
- Funding for implementation of the requirement has not yet been determined.
- Mobile devices are an integral part of work efficiency at Sandia.
- Personal connectivity is a major component of work-life balance, and therefore an important consideration for employee satisfaction and retention.

Who is responsible for implementing the requirement?
Implementation planning and execution will be coordinated through cross-functional teams including experts from Safeguards & Security, Facilities & Emergency Management, Infrastructure Services, CIO & IT Services and Environment, Safety & Health.

What is a mobile device?
A mobile device is a portable computing device 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, and E-readers.

What is the difference between ‘mobile devices’ and ‘portable electronic devices’?
Advanced Change Directive (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 (devices with data processing or transmitting/receiving capabilities) and storage devices (devices with storage capability, but no ability to process or transmit/receive information). Only mobile devices are impacted by ACD 470.6 requirements.

**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.

**Does the requirement affect Virgin Pulse GoZone pedometers?**
No, GoZone pedometers are not impacted. MOW may order GoZone pedometers through Virgin Pulse (you must create an account to enroll in Virgin Pulse; see ‘Devices & Apps’ link in Virgin Pulse profile to order).

**What is Secure Space?**
Secure Space will be identified in Phase 2 of the implementation. 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.
- Areas (Buildings, Rooms, etc.) where classified discussions no matter the level take place.
- Classified Video Teleconference rooms and Classified Skype rooms.

**What is Non-Secure Space?**
Non-secure space are areas in which no classified processing or discussions take place within a Limited Areas. Requirements for separation between Secure Space and Non-Secure Space as outlined in the directive must be established and maintained.

**What mobile devices can be brought into secure spaces, once they are identified?**
No mobile devices regardless of ownership (personally-owned, Sandia-owned or other government agency [OGA] owned) can be brought into secure space once it has been identified.

**Who determines if my area or the area I work in is secure or non-secure space?**
Management in partnership with Security will evaluate and determine what space is secure or non-secure.

**Are any mobile devices exempt from this requirement?**
- 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.
- Nothing in the ACD alters or supersedes legal or policy requirements regarding accommodation of employees’ medical needs. A cross-functional team is assessing current policies and processes.
- Controlled articles registered and approved through the Controlled Articles Registration Process (CARP) site (i.e. laboratory testing equipment, cameras) are exempt from the requirement.

**What is the current projected implementation timeline?**
**Phase 1: Planning**
- Develop plan to remove personally owned mobile devices from all Limited Area buildings by January 1, 2020.
- Sandia owned devices follow current policies.
Phase 2: Characterize Limited Areas to come into Full Compliance
  o Characterize all SNL buildings within Limited Areas as either 'Secure Space' or 'Non-Secure Space' by September 1, 2020.
  o As buildings are characterized and configured, all mobile devices (personal and government) will be prohibited in buildings identified as ‘Secure Space.’

Phase 3: Consolidate
  o Consolidate classified processing within buildings where feasible to further refine the 'Secure Space' footprint.

Are Sandia-owned iPhones or iPads impacted in Phase 1 (on January 1)?
No, Sandia-owned devices are not impacted in Phase 1; they continue to follow current polices. They will, however, be impacted in Phase 2.

What happens if I bring a personally owned mobile device into a Limited Area building (with the exception of designated, approved storage areas) after January 1, 2020?
Submit a report using the self-report tool at SIMP.sandia.gov. Until October 1, 2020, provided that the personal mobile device did not come into proximity with any classified discussions or processing, and did not enter a VTR or SCIF, the event will be recorded as a non-incident, non-compliance (NINCs), which is a violation of corporate policy. If any of the above occurred, the event will be reported as a Category A or Category B incident.

What happens if I bring a mobile device into a secure space once it is identified?
Submit a report using the self-report tool at SIMP.sandia.gov. The event will be reported as a Category A or Category B incident.

How Do I Report?
Members of the Workforce with SRN computer access: Go to SIMP.sandia.gov to access the Mobile Devices Self-Reporting Tool.
Members of the Workforce without SRN computer access, or to report on behalf of another person: Call 321 from a Sandia landline phone or (505) 845-1321 from a non-Sandia phone.

Will I receive a security incident if I bring a mobile device into an area in which it is prohibited?
SIMP will conduct an inquiry into the event to determine if a security incident occurred.

Do Bluetooth and Wi-Fi still need to be disabled in Limited Areas outside of secure space?
Yes, the policy regarding Bluetooth and Wi-Fi within Limited Areas remains in effect.

Do the current eligibility requirements still apply for bringing a mobile device into a Limited Area?
No, the former PEDS100, including the eligibility requirements, are no longer in effect. Per the revised policy, all MOW, including cleared, uncleared and Foreign Nationals, are subject to the same requirements and restrictions regarding possession and use of personal mobile devices.

How will I be able to distinguish secure space from non-secure space?
Standard signage will be posted which 1) identifies the area as secure space and 2) states what devices are prohibited.

Do these requirements apply to SCIF’s or Vault Type Rooms?
No, these high security areas have separate requirements in place that already prohibit mobile devices within these areas.

If I don’t currently have a Sandia owned cell phone, may I request one?
Sandia is closely monitoring the growth of the Sandia-owned mobile device population and will implement appropriate governance in upcoming months. The policies that govern the acquisition and use of Sandia mobile
devices are being reviewed and updated in anticipation of increased usage and requests. Sandia cell phones require a business need.

May I use my Sandia owned cell phone for personal texts and/or calls?
Incidental personal use of Sandia IT equipment is allowed but the personal use must be consistent with the requirements identified in IT002, Use Sandia’s Information Technology Resources Policy.

Are communication alternatives being explored to help members of the workforce stay connected during the work day?
Yes, IT is currently exploring communication solutions that include email to text capabilities and external browsing/email capabilities on the SRN. Release date is TBD.

What can I do to prepare?
- Update emergency contact information by providing Sandia mobile and/or desk phone numbers to family, friends, schools, child care centers, etc.
- Consider adjusting commuting routines to allow for safe storage of personal cell phones and other devices, especially during the initial weeks of implementation.

Where can I store my personally owned mobile device?
You may store mobile devices in your vehicle, at Limited Area entry turnstiles, or in the following designated, approved storage locations at Limited Area building entrances (list also available at PEDs.sandia.gov). Locations will be marked with signage.
- 701: Northeast entrance and northwest entrance
- 800/801: Main entrance of Bldg. 800 Property Protection Area (PPA)
- 810: Main lobby
- 822: Main entrance (personal phones may traverse through the 822 breezeway, but may not enter building 821)
- 880: North vestibules B and D
- 887: Northwest entrance lobby and southwest entrance vestibule
- 898: Main lobby entrance in the PPA
- 960: Main lobby (west side of building)
- 962: Main lobby
- 6577 (TA-V): Main lobby
- 6585 (TA-V): Main lobby
- 910 (CA): 1st floor main lobby
- 915 (CA): PPA café wing

- Approved storage locations meet all ACD 470.6 requirements for non-secure space.
- Storage areas will be marked with signage.
- Inside a Limited Area, mobile devices may be stored in these buildings only, and only within the designated storage areas.
- Current external storage boxes may be used (see map link below). Keys to storage boxes may not be kept overnight.
- Devices may not enter, or be carried through, any other part of the identified buildings, or any limited area building not approved.
- No classified discussions are allowed in the storage areas.
- Since storage will only be available in designated, approved locations, consider leaving personally owned mobile devices at home or in your vehicle.
- Like luggage at the airport, many phones look alike. Consider making your device easily identifiable. And when you leave, make sure you take your own, not someone else’s!

Click here for a map of current mobile device storage locations at SNL/NM. Click here for a map of current mobile device storage locations at SNL/CA.
My building is divided by a Limited Area boundary; part of the building is a Limited Area, and part of the building is a Property Protection Areas (PPA) or General Access Areas (GAA). Are mobile devices permitted in the PPA/GAA portion of the building?
Yes.

May I use existing storage boxes located in Property Protection Areas (PPA) or General Access Areas (GAA) that are adjacent (connected) to Limited Areas, even if they are in the same building (as described above)?
Yes, during Phase 2, existing storage located in PPAs or GAAs adjacent to Limited Areas may be used to store mobile devices. As ‘Secure Space’ and ‘Non-secure Space’ is identified, existing storage will be evaluated and relocated if it does not meet all requirements in the directive.

Will additional mobile device storage be installed?
Currently, there are no plans to install additional temporary storage locations. Additional, permanent mobile device storage lab-wide is a high priority action item in the implementation plan for Phase 2. Facilities is assessing options that are cost-effective and environmentally protected where needed. Updates to storage locations, including new permanent storage solutions, will be posted at PEDs.sandia.gov.

I ride a bike, a bus, or a carpool to work and therefore will not have the option to store my personally owned device in my vehicle. Will there be enough storage?
The project team recognizes the importance of this concern and is working toward permanent solutions that will provide plenty of storage to support all types of commuting alternatives.

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.)

Can my organization order and install phone storage solutions in our own building(s)?
Storage solutions must be acquired and installed by facilities and must comply with all security requirements and building codes. Do not install anything in or on a building without proper approval.

If I have a handicapped placard or other permit that allows me to park inside the Limited Ares, will I be allowed to store my phone in my car (inside the Limited Area)?
Yes. A mobile device may be stored in any vehicle that is authorized to park within a Limited Area.

How does the workforce feel about allowing mobile devices into Limited Areas?
A Counterintelligence survey spanning the past 12 months posed the question: “Do you believe the benefits of allowing PEDs into the Limited Areas outweigh the risks?” Out of 16,135 respondents:
- 41% - Yes
- 59% - No

Is theft of mobile devices from storage areas expected to be a problem?
Sandia has no recorded reports of stolen mobile devices within Limited Areas.

If I am escorting an uncleared individual into a Limited Area, am I still required to brief them about controlled and prohibited articles?
Yes, escorts should still brief uncleared individuals prior to entering a Limited Area:
- Ensure no unauthorized (prohibited) articles enter a Limited Area.
- Ensure Bluetooth and WiFi are turned off on any mobile devices—personally owned or Sandia owned.
- Ensure that the individual is prepared to store any personally owned mobile devices in their possession in a designated, approved storage location.
For more information about ACD 470.6, visit PEDs.sandia.gov.

Access to PEDs.sandia.gov and other hyperlinks in the above FAQ's requires access to the Sandia Restricted Network (SRN). Subcontractor personnel without SRN access may request PEDS information from their Sandia Delegated Representative. Contact Security Connection for answers to your security questions.

SECURITY CONNECTION:
321 from Sandia phone | 505-845-1321 from any phone | security@sandia.gov