

## Section 6

## COMMUNICATIONS

## Contents

References .....	6-1
General Information .....	6-1
Common Deficiencies/Potential Concerns.....	6-2
Planning Activities.....	6-3
Performance Tests.....	6-3
Data-Collection Activities.....	6-3

---

**References**

DOE Order 5632.1C  
 DOE Order 5632.7A  
 DOE Manual 5632.1C

**General Information**

PSSs cannot operate independently of the human element, and since some sites are quite spacious, there must be a method for communicating quickly, clearly, and reliably. Telephone, radio, and duress alarms provide the necessary communication links among the alarm stations, mobile and fixed posts, response forces, and LLEAs. The effectiveness of communications equipment is based on compliance with DOE orders and performance during equipment testing and performance tests.

DOE policy requires that communications equipment allows the effective protection of safeguards and security interests, providing rapid, reliable, and protected information exchange between onsite protective personnel and central alarm stations.

The design of communication systems must be such that no single event can disable all modes of communication between the CASs and fixed posts or between the alarm stations and LLEAs. Communications equipment and systems are required to be tested daily for operability, and alternate communications capabilities are required to be available immediately upon failure of the primary system. Records of the failure and

repair of all communications equipment are required to be maintained in a form suitable for compilation by type of failure, unit serial number, and equipment type.

The following subjects are covered in this section:

- Telephones
- Radios
- Duress alarms
- Intercoms, public address, pagers
- Audio-recording systems.

Telephone systems are the primary means of communication at most DOE facilities. Although the telephone is often taken for granted, it is important that the telephone system used for security purposes be protected (alarmed, buried cable, or line in a conduit) and have backup provisions, especially when used as a direct-line communication between the central and secondary alarm stations and guard posts. It is also important that a good preventive maintenance system be in place to ensure that the system remains reliable and operates at peak performance.

Although alarm stations and radio communication centers should have both radio and telephone channels of communication with LLEAs, the telephone is normally the primary means of communication between protective forces and LLEAs, and between the site and DOE Headquarters or the DOE Emergency Operations Center (EOC).

Radios are used for voice communications among members of the protective force and alarm stations, and with DOE managers and other participants, when required. Additionally, radios are used to communicate with LLEAs who participate in exercises or respond to emergencies. In order to provide the flexibility necessary for all participants who may be required to participate in radio communications, it is important to have a number of frequencies available, especially during emergency conditions (for example, one frequency for members of the protective force, one for special response teams [SRTs], and one for communicating with LLEAs). Also, it is critical that radios be readily available in sufficient quantities to equip protective force personnel and to facilitate the performance of their duties.

When repeaters are used to increase radio communications range and clarity, it is important that these devices (antennas and other exterior components) be protected from tampering or sabotage. Also, a good radio system will usually have an effective preventive maintenance program in place to ensure that radios and radio components remain functional.

Duress alarms are primarily used to alert protective forces to emergency or duress conditions. It is important that activation of the alarm be accomplished in as unobtrusive a manner as possible, and not announce at the post initiating the alarm. Usually these alarms are hardwired devices that are protected from tampering. Also, radios may include a duress feature. All duress systems should have procedures in place that provide for maintenance and testing to ensure that they remain in good working condition.

Intercommunication (intercom) and public address systems are normally used to provide information or instructions to selected organizations or individuals, or to the general facility population. Pagers and/or cellular phones may be in use as a means of contacting individuals or for sending messages. Pagers and/or cellular phones are often issued to key security, safety, and management personnel who must be notified in case of an emergency. All of these devices are especially important during

emergency situations when speed is critical and when instructions must be disseminated to as many people as possible.

A continuous electronic recording system is used to record all security radio traffic. This will usually include all protective force radio transmissions and duress alarms, and transmissions going into and out of central alarm stations or operations centers. Sometimes, telephone conversations conducted over security channels are also recorded.

## Common Deficiencies/ Potential Concerns

### Telephones

Frequently, onsite telephone lines and switches are not protected against tampering or sabotage.

### Radios

Although radios are required to provide a multichannel capability, some radio systems used at DOE sites do not have enough channels (radio frequencies) available to provide effective communications for all who need to use the radio. If a sufficient number of frequencies are not available, the primary frequency becomes cluttered with radio traffic. It then becomes difficult to transmit messages, transmissions are confusing, and the probability that important information will be lost increases. This problem is intensified during emergencies, when radio traffic normally increases. Also, the lack of sufficient number of frequencies limits the use of the radio when adversaries deliberately jam the primary frequency. When there are an insufficient number of frequencies, inspectors should determine what is being done to manage the available frequencies and to use alternate means of communication.

When encrypted radios are in use, there are often inadequate procedures in place for installing encryption codes or for switching to the secure mode. Inspectors should determine whether problems with encrypting codes are present and what procedures, if any, are in place for installing codes, changing data encryption keys, and switching to a secure mode. Also, radios issued to

SRTs often do not have voice privacy or an encryption mode of operation.

Frequently, no formal, systematic study of radio transmission and attenuation has been conducted at the site to identify dead spots and range limitations, or to determine what effect inclement weather has on the radio system. This is particularly important in facilities constructed with reinforced concrete. If such a study has been completed, inspectors should examine the results to determine what action was taken to correct or mitigate any deficiencies.

Often, there are inadequate protective measures, or no protection at all, for radio antennas, repeaters, or other exterior radio components to preclude tampering or sabotage.

### Duress Alarms

On occasion, hardwired alarms, switches, and junction boxes are not protected from tampering. Duress alarm capabilities should be provided emergency or auxiliary power for continued operation during commercial power outages.

### Intercoms, Public Address, Pagers

Frequently, public address or paging systems are not provided with backup power and/or are not appropriately protected even when they are used as critical elements of the security communications network.

Intercoms and public address systems are not adequate for use in contacting the majority of facility individuals in case of an emergency.

Key security, safety, and management personnel are not normally provided pagers or cellular phones.

### Audio-Recording Systems

Frequently, the recording system tapes are not kept or stored as part of the alarm station historical data. This media should be treated the same as an alarm log or record and should be maintained for a predetermined length of time.

## Planning Activities

Inspectors review documents and interview points of contact. Elements to cover include:

- Description of the basic communication systems, local transmitters and repeaters, and duress systems
- Types of communication equipment used in CAS, SAS, protective force posts, EOC, and patrol vehicles
- Types of communication equipment issued to each SPO and SPO supervisor
- Reports documenting site performance tests of communications equipment.

## Performance Tests

- Radio Equipment Performance Test (Appendix C)
- Duress Alarms (Appendix C)
- Auxiliary Power Supplies Testing (Appendix D).

## Data-Collection Activities

**A.** Inspectors should tour selected areas, visually inspect equipment, and verify information gathered in interviews and document reviews. Equipment in the CAS and SAS should always be inspected. Selected fixed and mobile protective force posts should also be reviewed for operability and familiarity with communications equipment, primary and auxiliary power supplies, protection against tampering and sabotage, and ease of operations.

### Telephones

**B.** Inspectors should review telephones and telephone equipment to determine whether telephone lines and switches are protected from tampering or sabotage and whether operational features (for example, simplex or duplex, sound powered, or automatic ringdown) are adequate for all contingencies.

**C.** Inspectors should determine what measures are in place to provide backup communications, especially for emergency conditions, in the event that the telephone system fails.

### Radio Systems

**D.** Inspectors should review documents and interview security staff to determine whether an adequate number of radios and radio frequencies are available to the protective force, SRTs, managers, and other participants in routine and emergency conditions. If an encryption system is used, inspectors should determine whether procedures are in place that adequately explain how to install encryption codes, when and how to change encryption keys, and when and how to switch to the secure operating mode.

**E.** By interviewing security staff, inspectors can often determine whether there are transmission problems due to dead spots, range, interference, or severe weather conditions. If these problems exist, inspectors should determine what has been done to mitigate these problems.

**F.** During the inspection of entry portals, vaults, and the PIDAS, inspectors should observe the effectiveness and clarity of communications. This information can assist in properly evaluating the routine use of various communication systems used by security personnel.

**G.** Inspectors should determine whether antennas, repeaters, or other exterior radio components are protected from tampering or sabotage. Also, inspectors should identify the measures used to provide reliable communications in the event of sabotage, including the primary power sources and backup sources.

**H.** Inspectors should determine whether there are procedures for testing radios and, if so, how often the tests take place and what actions are taken when deficiencies are found.

**I.** Inspectors should examine preventive maintenance procedures to determine whether there are provisions for maintaining base, mobile,

and handheld radios and for battery replacement and charging. Inspectors should also determine whether there are alternate methods or compensatory measures when radio equipment is unavailable.

### Duress Alarms

**J.** Inspectors should determine whether protective force posts are equipped with hardwired duress alarms and, if so, whether they are protected against tampering (for example tamper switches, junction boxes, and line supervision). If handheld radios do not include a duress feature, inspectors should determine whether there are alternate means of indicating a duress condition. Also, inspectors should identify the primary and secondary locations where duress alarms are monitored to determine whether the alarm annunciation is adequate and whether protective personnel can easily identify it. Further, the auxiliary power provisions (for example battery or generators) should be identified to determine whether they are adequate for all duress alarm systems, including radios.

**K.** Inspectors should determine the method and frequency for testing duress alarms, including hardwired and radio. These tests can be observed at the primary monitoring station or at the individual guard posts. Also, the operator logs at the central alarm and secondary alarm stations can be examined to verify that tests are performed at the required frequency.

### Intercoms, Public Address, Pagers

**L.** Inspectors should review documentation and interview security staff to determine how the intercom systems, if any, are used in communicating security information to the facility population. Some elements to consider include:

- When and how pagers/cellular phones are used for security purposes
- Provisions for use of high-noise areas or electrical interference environments.

**M.** Inspectors should verify operability by observing equipment being used or by conducting operability tests.

#### Audio-Recording Systems

**N.** Inspectors should interview security staff to determine whether audio-recording systems are recording all security radio traffic, and whether duress alarms and telephone conversations are recorded. Also, inspectors should determine if recordings are being appropriately maintained.

Further, inspectors can determine by listening to recordings whether radio checks and testing are being performed as required, and whether radio transmissions are clear during a range of conditions, including extreme weather. This involves listening to recordings selected from various times of the day, and under different weather conditions, including periods of severe weather such as thunderstorms. Inspectors should determine whether anyone reviews the recordings on a routine basis and whether any action is taken on the information taken from the recordings.

This page is intentionally left blank.