

APPENDIX D
SUPPORT SYSTEM
PERFORMANCE TESTS

Part 1: Auxiliary Power Supplies..... D-1
Part 2: Tamper Protection and Line Supervision D-13

Part 1

Auxiliary Power Supplies

Objective	D-1
System Tested	D-1
Scenario	D-1
Evaluation	D-2
Assessing Systems	D-2
Interpreting Results	D-3
Special Considerations	D-3
Responsibilities	D-4
Internal Coordination	D-4
Security Considerations	D-4
Personnel Assignments	D-4
Logistical Requirements	D-4
Auxiliary Power Supplies Testing.....	D-6
Checklist—Auxiliary Power Supplies	D-8

Part 1

Auxiliary Power Supplies

Objective

The objective is to test the effectiveness of auxiliary power supplies to maintain power for continuous operation of critical physical security system components. The most directly applicable DOE requirements are:

Applicability**Order Reference**

Category I and II SNM, Vital Areas

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 7

Classified Matter

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 7

DOE Property and Unclassified Facilities

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 7

System Tested

System - Auxiliary power supplies

Functional Element - Support functions

Components - Uninterruptible power supplies (UPS), engine-driven generators, fuel supplies, batteries, inverters, switches, and interfaces with other security system components (CAS/SAS, security lighting, communications, access controls, and intrusion-detection system); testing and maintenance of auxiliary power supplies.

Scenario

The inspectors should select various sources of auxiliary power for testing. These may include a central battery-powered UPS, remotely located individual battery backups for various security system components and equipment, and one or more diesel or gasoline engine-driven generator. At least one of each type of auxiliary power source should be tested. In deciding which tests to conduct, the inspectors should first determine the configuration and location of auxiliary power sources and the systems and devices (CAS/SAS equipment, radio base stations, intrusion-detection system, access control system, perimeter lighting) powered by each.

The inspectors should observe, if possible, the conduct of routine operational or test activities performed by electrical technicians. Maintenance, replacement, refueling, test, and operational history records should be

reviewed to determine whether they are consistent with the manufacturer's recommendations and the requirements of DOE orders and approved SSSPs.

To the extent possible, the inspectors should conduct actual auxiliary power loss tests that require automatic start-up and full-load testing of all auxiliary power sources. If this is not possible because of safety or security concerns (for example, the total loss of security systems or lighting without adequate compensatory measures), simulations may be substituted. Regardless of the tests conducted, inspectors should verify that auxiliary power sources automatically provide auxiliary power and can carry the required electrical loads for a sufficient period to permit restoration of normal power.

Inspectors should monitor power supply testing at the CAS or SAS to verify that power switchover is properly initiated and that all security systems continue to function as required.

The following guidelines are intended to assist the inspector in conducting appropriate tests.

- At least one of each type of auxiliary power source (central UPS, individual battery packs for sensors, and engine generators) should be tested.
- Fuel supplies should be checked for diesel or gasoline engine-driven generators to ensure the adequacy of fuel quantities and the quality of the fuel. Actual fuel testing for quality is not required if facility records indicate it is performed periodically.
- If possible, testing should include actual emergency loss of normal AC power, automatic switchover to auxiliary power, and demonstration that power sources can assume the full electrical load required.
- Where many individual battery power supplies are used, it is necessary to test only a representative number of these. Additional testing is required only if deficiencies in the tested battery supplies are evident and indicative of a systemic weakness.

Evaluation

Emergency backup power is required to ensure continuous operation of critical security systems.

Assessing Systems

The principal objective in evaluating auxiliary power supplies is to determine whether they are adequate to power all critical equipment for a sufficient time (usually at least eight hours) to permit restoration of normal AC power.

Other factors to consider in the evaluation follow:

- Do all intrusion-detection alarm system components have an auxiliary power source, with automatic switchover upon loss of primary power, which permits continuous uninterrupted operation?
- Is the failure of either primary power or emergency backup power supplies annunciated at the CAS/SAS?

- For batteries, is a low-voltage (voltage drop of 20 percent below rated power) signal annunciated at the CAS/SAS?
- Are power supplies (and fuel) adequate to permit continuous operation under full load for a period of at least eight hours?
- Are environmental control systems and venting adequate to ensure safe and reliable operation of batteries and engine-driven generators? Battery power is reduced as temperature decreases, and evaporation of electrolyte solution increases with temperature, as does a hazard of explosion.
- Are auxiliary power sources and fuel supplies protected adequately to ensure their availability for continuous reliable operation?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance.

- Security system operation relies upon the availability of a continuous, reliable power supply. Testing should verify that all critical security system components have a backup power source. This should include intrusion-detection system equipment, CCTV, access controls, fixed base station communications equipment, all alarm annunciation equipment in the CAS/SAS, and security lighting.
- Failure of individual power supplies (other than central UPS battery supplies and generators) may indicate either an isolated failure or a systemic weakness in the maintenance and test program.
- If “load shedding” is required because auxiliary power sources are unable to instantaneously accept the full load of security equipment (for example, diesel generators require a run-up period and sequential electrical loading), the rationale for sequencing of the load should be assessed. The most critical loads (for example, alarm systems and communications) should be picked up first, followed by the less critical systems/components (for example, CCTV systems and security lighting).
- When assessing battery supplies, it is important to remember that many batteries have a predictable useful life, after which rapid degradation followed by failure can be expected. If all batteries were installed at the same time, it is likely that failure will occur in rapid succession throughout the system.

Special Considerations

Auxiliary power supply configurations vary widely depending upon the system equipment and manufacturer. It is important to fully understand system configuration and the manufacturer’s test procedures before conducting any tests. Test activities should not result in failure of, or damage to, critical security systems or equipment.

Battery power supplies may pose health and safety hazards from caustic solutions and vapors, and the potential for explosion. All safety precautions should be carefully observed.

Responsibilities

Inspectors: Select power sources and fuel supplies for testing. Direct tests and monitor system annunciators and performance. (Typically, one inspector will be stationed at the CAS and at least one with the test team.)

Facility: Conduct routine tests/maintenance. Provide technicians and test devices as necessary. Provide radios for two-way communication. Provide security compensatory measures, as required. Provide safety equipment/clothing as required (for example, protective eyewear).

Internal Coordination

Testing should be scheduled to avoid disruption of other security system tests. If loss of perimeter lighting will result from testing, loss of power testing should be conducted during daylight hours. However, this presents an opportunity to evaluate restrike times for perimeter lighting and should be carefully coordinated with site personnel prior to testing.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Testers

Equipment:

- Radio
- Protective equipment/clothing, as required

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before conducting any test that will affect security system operation

Auxiliary Power Supplies Testing

System Description:	Central and remotely located battery UPS, gasoline/engine generators, inverters/switching devices, battery chargers, and fuel supplies
Capabilities:	Provide a minimum eight-hour power supply for all critical security system equipment with automatic switchover and annunciation upon loss of primary power
Vulnerabilities:	Temperature extremes, battery aging, contaminated fuel supplies, tampering

Concerns

- Batteries require routine servicing and testing to ensure proper charging, electrolyte levels, and corrosion removal. Failure to service batteries or replace them at the end of useful life can degrade operation under emergency conditions.
- Batteries pose health and explosion hazards and should be located in a fire-resistant, environmentally controlled location that avoids high and low temperature extremes, which can increase explosion potential and reduce available power, respectively.
- Generators, batteries, inverters, power switches/busses, and fuel supplies should be protected to preclude tampering. Exterior fuel tanks and filler points are especially vulnerable.
- Power ratings on both batteries and generators can sometimes be misleading. For example, in the case of batteries, below-freezing temperatures can reduce available power by more than 50 percent. Generators may be unable to instantaneously carry the full rated load, especially if the electrical drive shaft is not of the continuously turning type driven by an auxiliary electric motor.

Types of Testing

- Full Loss-of-Power Test

If possible, without unacceptable security system degradation, a test should be performed where all primary (commercial AC) power is disconnected from all security system components. The purpose of this test is to ensure that all system power loads can be handled, usually by the UPS batteries and then by the emergency generators. The loss-of-power test should last at least 10 minutes and preferably one hour to adequately demonstrate system reliability. Proper functioning of all security system equipment (including lighting) should be verified, as well as proper annunciation of all power supply status indicators in the CAS/SAS.

- Remote Power Supply Tests

If remotely located power sources are used, a representative sample should be inspected and tested. Generally, there will be battery packs for intrusion-detection sensors, sensor control units, or communications equipment. The test usually consists of removing the primary power lead to the device and verifying that the device continues to operate on battery power, and that a status indication is received by the CAS/SAS.

- **Power Status Indication Test**

As part of the loss of power and remote power supply testing, annunciation of the status of all power sources at the CAS/SAS should be verified. The annunciation should indicate which source of power is being used and the status of the primary AC power source, any battery backups, and the emergency generators. The annunciator system should also provide a status indication whenever battery power drops below 80 percent of full-rated power. This test involves the simulation of reduced output and requires assistance from facility electrical technicians.

Test Guidelines

- The foregoing testing should usually be conducted during daylight hours for safety and security reasons. If loss of power testing will affect perimeter security lighting, daylight testing should include turning on all lighting or arranging for special compensatory measures for testing during periods of darkness.
- At least one of each type of auxiliary power supply should be tested.

Checklist

Auxiliary Power Supplies

Interview Items

Types of power supplies in use _____

Makes/models _____

Where located/how protected _____

Systems connected to each type power supply _____

Operational test frequency _____

Environmental protection equipment _____

Physical protection measures _____

Fuel supplies and locations _____

Special equipment (status annunciators, inverters, battery chargers) _____

Maintenance history/records _____

Power rating adequate to meet needs of all equipment (KWH or amp rating) _____

Frequency and duration of generator operation (15 to 30 minutes monthly recommended) _____

Tour/Visual Inspection Items

Physical protection OK? _____

Environmental controls (HVAC, ventilation) OK? _____

Fire and electrical safety OK? _____

Fuel supplies adequate? _____

Gasoline fuel replenished each 6 months? _____

Status annunciators (audible/visual) adequate? _____

Battery electrolyte and specific gravity OK? _____

Battery connections OK (no corrosion)? _____

**Data Collection Sheet
Auxiliary Power Supply Testing**

Test Method

	Zone Tested	Zone Number	Full Loss of Power	Remote Power Supply	Power Status Indication	Duration of Auxiliary Power
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments						

This page is intentionally left blank.

Part 2

Tamper Protection and Line Supervision

Objective	D-13
System Tested	D-13
Scenario	D-13
Evaluation	D-14
Assessing Tamper Protection	D-14
Interpreting Results	D-15
Special Considerations	D-15
Responsibilities	D-15
Internal Coordination	D-16
Security Considerations	D-16
Personnel Assignments	D-16
Logistical Requirements	D-16
Tamper Protection/Line Supervision	D-17
Checklist—Tamper Switches	D-20

Part 2

Tamper Protection and Line Supervision

Objective

The objective is to test the effectiveness of components used to indicate that detection and alarm devices or transmission lines to annunciators have failed or been tampered with. The most directly applicable DOE requirements are:

Applicability

Category I and II SNM, Vital Areas

Classified Matter

DOE Property and Unclassified Facilities

Order Reference

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 8

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 8

DOE Manual 5632.1C-1,
Chapter VI, Paragraph 8

System Tested

System - Tamper protection

Functional Element - Support functions

Components - Tamper switches (contacts, magnetic switches, plungers), line supervision circuits, signal processing equipment. Testing and maintenance.

Scenario

The inspectors should select tamper alarms and line supervision circuits for testing in conjunction with intrusion detection and CCTV system testing. During site tours in preparation for intrusion-detection system and CCTV testing, the inspectors should look for the related tamper/line supervision components to be tested.

The inspectors should select tamper-protection devices for testing based on consideration of the number, type, deployment, and operational history of the components. If facility alarm technicians are conducting tamper-protection testing or maintenance, the inspectors should observe the procedures to determine whether they are consistent with DOE orders and the approved SSSPs, and whether they are effective in testing system performance. These test and maintenance activities are an indicator of maintenance program effectiveness and provide assurance that the inspectors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of deficiencies.

The inspectors conduct tests by opening tamper-protected enclosures (that is, sensor covers, junction boxes, CCTV housings) and creating open and short conditions in electrical circuits to determine whether any of these actions could occur without annunciation at the CAS and SAS.

The inspectors monitor tamper and failure annunciation in the CAS/SAS. They also observe the operation of related systems (such as the CCTV) and the actions of CAS/SAS operators.

The number of tamper devices and line supervision circuits tested depends on the time available, the importance of the protected system in the overall protection program, and the variation in the individual protection zones. The following guidelines are intended to assist the inspector in selecting devices and circuits for testing:

- Test at least two of each type of tamper alarm device. If more than one line supervision (failure indication) method is employed, one of each type should be tested.
- If practicable, test tamper alarms and line supervision circuits in conjunction with other tests (CCTV and intrusion-detection system).
- If the first few tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not devote extensive time to testing numerous devices and circuits. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine whether a deficiency is an isolated instance or evidence of a systemic problem.

Evaluation

To ensure proper operation of the overall security system, reliable measures for detecting tampering and failure of critical security system components are necessary.

Assessing Tamper Protection

The primary objective in evaluating the tamper-protection subsystem is to determine whether it clearly annunciates equipment tampering or failure at the CAS/SAS. Other points to be considered in the evaluations are:

- Are all tamper and failure conditions indicated at the CAS/SAS in both the access and secure modes (if applicable to the protected equipment)?
- Are all junction boxes in accessible locations equipped with tamper alarms?
- Are all intrusion-detection systems and emergency exit alarms provided with tamper indication and line supervision, indicating the type and location of the alarm?
- Are all alarm lines continuously supervised to detect open, short, or signal substitution conditions?
- Does the CCTV system have a loss-of-video signal indication for each camera?

- Do new intrusion-detection systems for SNM and vital equipment facilities use continuously polled digital line supervision with unique digital address codes and pseudo-random polling (or, alternatively, encryption)?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results.

- Tests that indicate that a knowledgeable adversary could defeat tamper/supervision protection without being detected in a significant fraction of the attempts are evidence that system protection is not reliable. The significance of this finding must be analyzed in the context of the site-specific protection objectives, redundancy, and the effectiveness of other complementary systems.
- In some cases, facility tests indicate that tamper indication and line supervision function correctly, but inspector tests indicate that the protection can be defeated or does not function reliably. In such cases, it is reasonable to conclude that there are deficiencies in the test and calibration procedures and the quality assurance program.
- Facility tests that indicate that the sensors are calibrated according to specification, in conjunction with inspector tests that confirm that the sensors are capable of reliably detecting tampering or failure, are evidence that the tested portion of the system is effective, and that test and maintenance procedures are effective. However, the limitations of the tests must be recognized. For example, not all modes of defeat (for example, signal substitution) may have been tested and the test may not have stressed the system to the limit (for example, multiple attempts prior to system reset).
- Facility tests that indicate that one or more tamper or supervision devices are not functioning according to specifications may simply be an indicator of an isolated instance of component failure. However, such deficiencies may also be an indicator of systemic deficiencies with the test and maintenance program or the age and condition of the devices. If facility tests indicate that devices are out of calibration, the inspectors should consider instructing the facility's technicians to test a representative sample to determine the extent of the problem.

Special Considerations

Tamper and line supervision tests are usually conducted in conjunction with related tests of CCTV equipment and the intrusion detection and access control systems to increase the efficiency of data gathering.

Responsibilities

Inspectors: Select the tamper alarms and line supervision circuits for testing. Direct testing and monitor alarm annunciation. (Typically one inspector will be stationed at the CAS and at least one at the tested device.)

Facility: Conduct routine testing. Provide security technicians. Provide test devices as necessary. Provide SPOs to ensure security during tests, as required. Provide radios for two-way communication. Provide personnel to conduct tests at the direction of inspectors.

Internal Coordination

Tests should be scheduled to avoid conflict with other tests involving the protective force.

Security Considerations

Follow all normal security procedures.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Tester

Equipment:

- Radio
- Test devices (for example, voltmeters and other electrical test devices)

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS and other alarm monitoring stations before testing is conducted
- Station one inspector in the CAS
- Coordinate to prevent any undesired armed response to alarms by the protective force

Tamper Protection/Line Supervision

System Description:	Tamper sensors (magnetic switches, contact closures, plungers), line supervision signal generators and processors, end-of-line resistors, and status indication annunciators
Capabilities:	Indication of physical tampering (usually opening a protected enclosure) and signal line open, short, or signal substitution condition
Vulnerabilities:	Improper alignment or sticking of switches or contacts, gaps in protection, improper annunciation of status indication

Concerns

- Generally, the failure to provide complete tamper indication and line supervision for all security system elements and devices requiring protection is the most significant weakness. All critical components should be covered: intrusion sensors, sensor controls, and communication devices (for example, multiplexers), transmission lines, CCTV enclosures and signal equipment, cable junction boxes, power supply cabinets, and any other critical system support equipment.
- Tamper devices (magnetic switches, plungers, closure contacts) should be inaccessible and located inside a protected space to prevent defeat of the device by a knowledgeable adversary.
- Mechanical tamper devices (for example, plungers) must be serviced to ensure that they do not “stick” in the secured position because of rust, freezing, or accumulation of dirt.
- Indication of the status of both tamper devices and line supervision should be prompt and should continue even after the device returns to a normal condition (although the status indicator may show “return to normal” by change of color). This feature precludes, for example, opening a protected enclosure and quickly taping down the contact plunger to indicate that the tamper condition has returned to normal.
- Line supervision should include the entire circuit to be protected: the protected device (for example, sensor or CCTV camera), local wiring to a control device (for example, multiplexer or control panel), the transmission medium (for example, bi-directional multiplexed cable loop or free-space transceiver), and the final signal processing and annunciation equipment (for example, CAS/SAS monitoring equipment).
- CCTV camera protection should include loss-of-signal monitoring and annunciation as part of the alarm annunciation system. Loss of the actual CCTV image on the television monitors at the CAS/SAS should not be relied upon for this function since failure of the monitor could be confused with loss-of-video signal.
- In some cases, multiple tamper devices are included on a single alarm circuit to reduce wiring and signal processing requirements. This can be a significant weakness since the actual type and location of the alarm, and the number of affected devices, may not be known from the information displayed at the alarm console.

- In the case of line supervision, the type and location of the failure may not be known from the alarm annunciation. System redundancy and the number of sensor signals that may be lost because of a single communication failure should be considered in assessing the impact of such a configuration. If a single point failure (for example, open or short condition) will affect a large number of security system devices, it is especially critical that the nature and location of the failure be clearly annunciated. Otherwise, an adversary could disable the system and gain considerable time to act while maintenance personnel attempt to locate and repair the communications failure.
- Signal lines should be protected by use of metal conduit and, whenever possible, should be buried underground. To the extent possible, interior cable runs should be located within spaces that are protected by active intrusion-detection systems and should be located in inaccessible places.
- Often slow computer response will allow the inspector to open a junction box pull or push tamper switch to “Nonalarm” position. If done rapidly, no alarm will be reported in CAS or SAS.

Types of Tests

- Contact Closure Test

This test is conducted by simply opening a protected enclosure. An alarm should be generated before gaining access to wiring inside the enclosure. The contact switch or plunger should be promptly closed by hand (or using tape). This test should verify that an initial tamper alarm was generated before physically closing the contact, and that the alarm remains after the contact was closed.

- BMS Test

BMS sensors should be tested by opening the protected enclosure one inch to determine whether an alarm is generated. A handheld magnet should then be placed against the switch housing in an attempt to simulate closure of the device by replacement of the BMS magnet. An additional step of placing a magnet against the BMS when the tamper switch is closed and active may be used to determine whether capture of the switch is possible (this test is feasible only if the magnetic switch is accessible when the enclosure is closed). This test should verify that (1) an initial tamper alarm is generated when the closure is opened or when a magnet is brought into contact with the BMS, and (2) that the alarm continues even though a handheld magnet is used to replace the actual magnet of the switch.

- Line Supervision Test

Line supervision tests are conducted by creating an open or short condition in the tested communication signal line. An open condition is created by disconnecting wires/cables from a terminating block or other connecting point. Ground faults are also created at these connecting points. No actual cutting of any signal lines should be performed, nor should grounding be done if damage to equipment will result. An open or short condition should be indicated by an alarm regardless of the duration of the condition. Therefore, return the open or short condition to normal as quickly as possible to verify the line supervision was able to promptly detect the condition. This capability is important to prevent a fraudulent signal being substituted for the normal signal on the transmission line.

Test Guidelines

- Testing should be conducted in conjunction with CCTV, intrusion detection, and access control tests to maximize data-gathering efficiency.
- At least two of each type of tamper alarm devices should be tested.
- At least one of each type of line supervision in use should be tested.
- No test should result in damage to equipment. Line supervision tests should not be conducted if serious disruption of critical security systems (that cannot be compensated for) will occur.

Checklist
Tamper Switches

Interview Items

Installation location _____

Operational test frequency _____

Operational test method _____

Self-checking provisions (if applicable) _____

Maintenance procedures _____

False nuisance alarm history/records _____

Make/model _____

Type(s) used _____

Systems covered _____

Operational test frequency _____

Operational test method _____

Tour/Visual Inspection Items

Cable in conduit/buried? _____

Tampers present? (junction boxes, sensor housings, CCTV enclosures, multiplexors, power supply cabinets)

This page is intentionally left blank.