

Section 4

BADGES, PASSES, AND CREDENTIALS

Contents

References	4-1
General Information	4-1
Common Deficiencies/Potential Concerns.....	4-1
Planning Activities.....	4-2
Performance Tests.....	4-3
Data-Collection Activities.....	4-3

References

DOE Order 5632.1C
DOE Manual 5632.1C-1

General Information

A security badge or pass system is implemented to ensure that only authorized personnel enter, occupy, or leave a security area, and to indicate limitations placed on access to SNM and classified matter.

Badging systems are normally managed within the facility's security organization. However, the actual badging function is often delegated to other groups at the facility. For example, at some facilities, badges are issued and controlled by the protective force; at other facilities, the employment department may handle some badging functions. At large facilities, a group may be specifically dedicated to badging functions.

How the badge system is implemented varies across DOE facilities, depending on the size and complexity of the site. Sites with only one facility usually have a single office that issues badges and passes to employees and visitors.

Sites with multiple facilities may have more than one badge office or a centralized badge office with a number of satellite activities that perform badging functions. Inspectors must be aware of such satellite locations, their functions, and their interface with the centralized activity.

Most sites use computer-generated badges that have a magnetic stripe that is coded for access control. SPOs or other security personnel may use these badges as a stand-alone measure for controlling access to security areas, or in conjunction with a badge check. Although the PSS topic team usually inspects the technical aspects of the coded systems, the personnel security topic team may review procedures for enrolling/deleting personnel in the automated access control system and for issuing and controlling coded badges. Likewise, the computer security topic team may review procedures for the establishment of access controls for the computers that house the automated access control system (e.g., passwords, firewalls, etc.) Because computer-generated badges can be duplicated to near-perfect visual and tactile quality, the review of the facility's program for encoding data on the badges is particularly important at facilities that use those badges as a stand-alone measure to control access to security areas.

Common Deficiencies/
Potential ConcernsImproper Badge
Accountability Procedures

Records documenting the disposition of all badges may lack the required information (that is, date of issue, description and serial number of badge, organization, date of issue/destruction, and name of holder).

Improper Storage of Unissued Badges and Passes

Facilities do not always adequately protect unissued badges and passes against loss, theft, or unauthorized use. Unissued badges may be improperly stored in an unlocked drawer or file cabinet in a badge office or reception area, and left unattended or uncontrolled at times (for example, when the person issuing badges takes a break or leaves to perform other duties). Improper storage can result in the loss of unissued badges and the potential for unauthorized access, which can be a serious problem if the badges are already coded, or if access authorization is controlled by a security officer.

Ineffective Badge Recovery and Untimely Access Termination

Badges of terminated employees are not always promptly recovered before their departure from the site. Recovery of badges issued to long-term visitors, student workers, construction workers, or temporary employees can be a particular problem since such persons do not always follow normal termination procedures when leaving the site. Recovery of badges of employees terminated for cause or misconduct and timely revocation of their access via the automated access control system is particularly important to prevent further access to the site, and eliminate the possibility of misconduct by disgruntled employees.

Failure To Update Badge Photos

If employees do not have a new picture taken when their appearance changes significantly, their badges will not reflect their current appearance. Supervisors, security officials, and protective force officers are responsible for ensuring that the badge pictures are current by reporting to the badging authority any employee exhibiting a significant change in facial appearance.

Incomplete Handling of Lost Badges

When badges are reported lost, all personnel responsible for controlling access to security areas (usually SPOs) must be informed so that they are able to prevent unauthorized personnel

from using the lost badge to gain area access. However, badge offices do not always inform the protective force (or other groups responsible for access control) about lost badges. Even if the protective force is informed, the procedures for getting that information to the security posts or portals may be ineffective or untimely. Effective procedures for timely deletion of lost badges from the automated access control system and for notifying other organizations about lost badges are particular problems. Identifying lost badges at portals is rarely effective since SPOs may not take the time to check the list of lost or stolen badges. Deficiencies in notification of badge checks can lead to the potential for unauthorized access.

Insufficient Understanding of Policies and Procedures

Badging policies and procedures that are adequate in themselves may not be implemented as intended because they are not fully understood. This lack of understanding may be attributable to inadequate training programs or vague, informal, or incomplete procedures.

Planning Activities

During the planning meeting, inspectors should interview points of contact and review available documentation and procedures (for example, SSSPs, personnel security operating procedures, badge system policies, automated access control policies, and visitor control policies) to characterize the badge system policies and implementation. Elements to cover include:

- A general description of all badging systems used at the facility, including those implemented by the operations office or contractors
- The organizations responsible for managing and implementing badging functions; including enrollment/deletion of personnel in the automated access control program, issuance of employee and visitor badges, control and physical protection, accountability of badges and stocks of inserts, and recovery of expired/terminated badges

- Whether any of the badge offices have satellite offices that may perform badging functions
- Procedures for issuing temporary badges to employees who have forgotten them
- General procedures for obtaining a visitor badge or temporary badge
- General procedures for issuing badges to cleared and uncleared foreign nationals
- General procedures for recovering badges from visitors, temporary employees, and terminating employees
- General procedures for escorting uncleared personnel and how escort requirements are displayed on the badge
- General methods for protecting badges, passes, and records, including storage practices (for example, a safe or locked room within an LA), methods for control when the storage area is unlocked (for example, continuous surveillance), and methods for protection of computerized access control/badging systems
- Accountability systems for badges or passes
- Locations where badging functions are implemented
- General procedures for notifying affected organizations and for taking appropriate action in the automated access control system when a badge is reported lost
- Whether operations office surveys that include inspection of badges, passes, and credentials are available for review (if so, were the survey findings identified and corrected?)
- Whether the facility has performed any self-assessments of badges, passes, and credentials (if so, make arrangements to

review the self-assessment report during the inspection).

Once the inspectors have a basic understanding of the management and implementation of the badge/access control system, they determine which organizations, central badge offices, satellite badge offices, storage areas, and access control locations will be reviewed in more depth during the inspection. At most facilities, it will be possible to review all organizations, central badge offices, and access control points. However, at large facilities it will not generally be feasible to review every satellite badge office and access point. In such cases, a representative sample may be selected for inspection.

Performance Tests

The following performance tests yield data specifically applicable to this subtopic:

- Badge accountability check (selecting samples of badges and records, and verifying their accuracy) (Appendix E, Part 2)
- Portal badge checks (Appendix E, Part 4)
- Badge issuance (Appendix E, Part 2)
- Removal from automated access control system (Appendix E, Part 2).

In addition to tests conducted by the PSS topic team, any performance tests conducted by the protective force, personnel security, or information security topic teams that involve badge checks or other aspects of the badge system are directly relevant to this subtopic.

Data-Collection Activities

Badge Construction

A. Inspectors should examine badges to determine whether the badge design and construction precludes inserting a replacement picture without detectable damage to the badge. The inspectors should devote particular attention to temporary badges, passes, and visitor badges.

Documentation and Records

B. Inspectors should review badge/pass system policies and procedures to determine whether they are consistent with DOE requirements and whether the implementing procedures are consistent with site-specific policies.

C. Inspectors should interview selected personnel responsible for administering the badge/access control system to determine whether the site policies and procedures are being implemented as required by DOE orders and as described in site-specific documentation. Inspectors should determine whether these individuals understand the purpose of the badge/pass system and their responsibilities concerning issuance, disposition, storage, and recovery. Inspectors may wish to have personnel responsible for the badge/access control system explain each step in the badging process. It is valuable to observe these individuals issuing a badge to an employee, a visitor, or a contractor.

D. Inspectors should examine the access control/badge/pass disposition records and the record of lost badges for completeness and accuracy. Typically, this determination would involve reviewing a sample of lost-badge records.

Access Controls

E. Inspectors should interview SPOs who implement badge checks at portals and physically observe or test the portal operations to collect information about how the badge policies and procedures are implemented at the site. Alternatively, the PSS team can coordinate efforts with the protective force, personnel security, and information security topic teams to collect the required information. The inspectors should attempt to determine, at selected portals:

- Whether the post orders relating to badge checks are current and consistent with site policies
- Whether there is a copy of the list of lost badges at the post, and whether it includes lost badges of other organizations that are accepted by the facility

- Whether the SPO is familiar with, and implements, the procedures related to checking the list of lost badges
- Whether the SPO is familiar with the markings and indicators on the badges
- Whether the SPO devotes sufficient attention to comparing the person's face to the photograph.

Physical Protection

F. At each badge office selected for review, inspectors should determine whether stocks of unissued badges and passes are stored in a way that assures their protection against loss, theft, or unauthorized use. Storage areas, including satellite locations, should be checked to ensure that stocks are being adequately protected. Specific information to determine includes:

- The methods for storing the unissued badges and passes (for example, safes, locked filing cabinets, locked rooms)
- Whether the storage repositories are protected by alarm systems or security patrols or both
- The frequency of protective force patrols during non-operational hours
- The means of controlling access to the badges or inserts when the repository is open (for example, continuous surveillance)
- Which persons have access to the storage repository or automated access control system (for example, who has the combination to locked safes used to store the badges/inserts or who has the password to the automated system that encodes the badges) and whether those persons are appropriately cleared and have legitimate need to access the repository/computer
- Based on the protection measures in place (for example, the storage practices, alarms, and patrol frequencies), whether storage meets the requirements for storing

confidential matter (as defined in DOE Manual 5632.1C.1).

Badge Recovery

G. Inspectors should review badge records and interview personnel in the badge office to determine whether terminating employees are disenrolled from the automated access control system and whether badges and passes are recovered from them before they leave the site. This can be cross-checked by obtaining, from Human Resources or other appropriate facility departments, a list of employees terminated during a suitable time period (for example, the past three months). The names on the list can then be compared with the automated access control system and badge disposition records to determine whether the badges of these terminated employees were recovered and access was rescinded.

H. Inspectors should review visitor logs and badge records and interview personnel in the badge office to determine whether visitors' badges and passes are being recovered at the conclusion of the visit. Inspectors should determine what actions are taken if a visitor forgets to turn in a badge.

I. Inspectors should interview personnel in the badge office and review badge/pass documen-

tation and the automated access control system to determine whether foreign nationals are being appropriately badged (e.g., cleared foreign nationals are issued standard DOE badges with the individual's country of citizenship noted on the bottom of the badge and uncleared foreign nationals are issued a local site-specific badge colored red).

Badge Reissue Requirements

J. Inspectors should determine whether employee photos are retaken and badges reissued as required. One way to review this requirement is to observe the badge checks at a portal to determine whether badge photographs accurately reflect the facial appearance of the holder. Another way is to interview supervisors and SPOs to determine their level of awareness of the requirement to report to the badge office any employees who exhibit significant changes in facial appearance. A third method is to review records to determine how many employees have had their photographs retaken in a specified time period (for example, one year). A very small number of retaken photographs may indicate that the requirements are not being followed. If that is the case, the protective force topic team should devote additional attention to portal operations to determine whether personnel have current photographs and whether the SPOs report any discrepancies.

This page is intentionally left blank.