PERSONNEL SECURITY

INSPECTORS GUIDE

July 2000

U.S. Department of Energy
Office of Safeguards and Security Evaluations
OA-10
19901 Germantown Road
Germantown, Maryland 20874

User Comments

This reference material will be updated and expanded periodically. Comments from users are appreciated and will be considered for incorporation. This page is provided for your convenience. Please direct all comments to:

U.S. Department of Energy
Office of Safeguards and Security Evaluations
OA-10
DOE-HQ
19901 Germantown Road
Germantown, MD 20874

Foreword

As part of an effort to enhance the inspection process, the Office of Safeguards and Security Evaluations (OA-10) has prepared the Personnel Security Inspectors Guide as one in a series of inspectors guides. The guides incorporate the security criteria used by the Department of Energy (DOE) and are designed to assist inspectors in evaluating safeguards and security protection programs across the DOE complex. Operations Office personnel may also wish to use the guides to augment surveys and self-assessments. A loose-leaf notebook format is used so that sections can be easily removed and copied for reference.

This page is intentionally left blank.

Contents

Acronyms v

Section 1. Introduction 1-1

Purpose 1-1
General Considerations 1-1
Characterization of the Personnel Security Topic 1-2
Organization 1-2
Using the Topic-Specific Tools 1-3
Validation 1-5
Using the Policy Supplements 1-5
Using the Tools in Each Inspection Phase 1-5
Integrated Security Management 1-6

Section 2. Management 2-1

References 2-1
General Information 2-1
Common Deficiencies/Potential Concerns 2-2
Planning Activities 2-4
Data Collection Activities 2-5

Section 3. Personnel Access Authorization Program 3-1

3.1 Levels of Access 3-3
3.2 Pre-Employment Screening 3-7
3.3 Processing Access Authorization Requests 3-9
3.4 Screening and Analysis 3-13
3.5 Processing Derogatory Information 3-17
3.6 Reinvestigations 3-21
3.7 Interim Access Authorizations 3-23

Section 4. Safeguards and Security Awareness Program 4-1

4.1 Administration and Management 4-3
4.2 Security Education and Awareness Briefings 4-7
4.3 Visual Aids for Security Education and Awareness 4-13
4.4 Safeguards and Security Awareness Coordinator Training 4-15

Section 5. Visitor Control Program 5-1

5.1 Classified Visits 5-3
5.2 Visits by Uncleared U.S. Citizens 5-7

Contents (continued)

Section 6. Human Reliability Program 6-1

References 6-1
General Information 6-1
Common Deficiencies/Potential Concerns 6-2
Planning Activities 6-5
Data Collection Activities 6-5

Section 7. Unclassified Visits and Assignments by Foreign Nationals 7-1

References 7-1
General Information 7-1
Common Deficiencies/Potential Concerns 7-1
Planning Activities 7-2
Data Collection Activities 7-3

Section 8. Interfaces 8-1

Integration 8-1
Integration by the Personnel Security Topic Team 8-2

Section 9. Analyzing Data and Interpreting Results 9-1

Introduction 9-1
Analysis of Results 9-1
Consideration of Integrated Security Management Concepts 9-4

Appendix A. Data Analysis Forms A-1

Acronyms

AAAP	Accelerated Access Authorization Program
BI	Background Investigation
CMPC	Classified Matter Protection and Control
CFR	Code of Federal Regulations
COMSEC	Communications Security
CPCI	Central Personnel Clearance Index
DEAR	Department of Energy Acquisition Regulation
DOE	Department of Energy
ES&H	Environment, Safety, and Health
HRP	Human Reliability Program
ISM	Integrated Safety Management
M&O	DOE Management & Operating Contractors
NATO	North Atlantic Treaty Organization
OA	Office of Independent Oversight and Performance Assurance
OA-10	Office of Safeguards and Security Evaluations
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	Operations Security
OSS	Office of Safeguards and Security
PPM	Protection Program Management
QNSP	Questionnaire for National Security Positions
SCI	Sensitive Compartmented Information
SNM	Special Nuclear Material
SO	Office of Security and Emergency Operations
SSSP	Site Safeguards and Security Plan
VA	Vulnerability Analysis

This page is intentionally left blank.

Section 1

INTRODUCTION

Contents

Purpose 1-1
General Considerations 1-1
Characterization of the Personnel Security Topic 1-2
Organization 1-2
Using the Topic-Specific Tools 1-3
References 1-4
General Information 1-4
Common Deficiencies/Potential Concerns 1-4
Planning Activities 1-4
Data Collection Activities 1-5
Validation 1-5
Using the Policy Supplements 1-5
Using the Tools in Each Inspection Phase 1-5
Integrated Security Management 1-6

Purpose

The Office of Safeguards and Security Evaluations (OA-10) Personnel Security Inspectors Guide provides inspectors with information, guidelines, references, and a set of inspection tools that can be used to plan, conduct, and close out an inspection of personnel security. The guide is designed to promote consistency, ensure thoroughness, and enhance the quality of the inspection process.

The guide is intended to be useful to both novice and experienced inspectors. For the experienced inspector, the guide is organized to allow easy reference, and can serve as a reminder when conducting interviews and data collection activities. For the novice inspector, the guide will serve as a valuable training tool. Under the direction of an experienced inspector, the novice inspector should be able to use the inspection tools and reference materials in the guide to collect data more efficiently and effectively.

Inspectors may also wish to refer to the Office of Independent Oversight and Performance Assurance (OA) Appraisal Process Protocols and to the OA-10 Safeguards and Security Appraisal Process Guide for additional, non-topic-specific information pertaining to the inspection process.

General Considerations

The tools contained in this guide are intended to be used at the discretion of the inspector. Typically, inspectors select the tools that are applicable and most useful on a facility-specific and inspection-specific basis. Although the guidelines presented here cover a variety of inspection activities, they do not and cannot address all program variations, systems, and procedures used at all Department of Energy (DOE) facilities. The tools may have to be modified or adapted to meet inspection-specific needs, and in some instances the inspectors may need to design new activities and new tools to collect information not specifically covered in this guide.

The information in this guide does not repeat all of the detailed information in DOE orders or other applicable directives. Rather, it is intended to complement other guidance by providing practical guidance for planning, collecting, and analyzing inspection data. Inspectors should refer to the guide as well as DOE orders and other applicable guidance at all stages of the inspection process.

One significant consideration in developing OA-10 inspectors guides is to provide a repository for the collective knowledge of OA-10's most experienced inspectors that can be enhanced and updated as inspection methods improve and OA-10 inspection experience accumulates. Every attempt has been made to develop specific guidelines that would offer maximum utility to both novice and experienced inspectors. In addition to guidelines for collecting information, the inspection tools provide guidelines for prioritizing and selecting activities, then analyzing and interpreting results. The specific guidelines should be viewed as suggestions rather than dogma. All guidelines must be critically examined and interpreted on an inspection-specific basis, taking into account site-specific factors.

Characterization of the Personnel Security Topic

The purpose of the DOE personnel security program is to ensure that individuals with access to classified information and special nuclear materials (SNM) do not pose a threat to the nation's security. Additionally, it is intended to ensure continuing awareness of security responsibilities among DOE employees, contractors, and consultants.

The protection of classified information designated Restricted Data and the protection of SNM are unique security interests of the DOE. Measures to protect Restricted Data and SNM are set forth in the Atomic Energy Act of 1954, as amended, which specifies that authorization for access to Restricted Data and SNM must be clearly consistent with the national interest.

DOE must establish the "character, associations, and loyalty" of the individual to determine whether granting an individual access to classified information and material will "endanger the common defense and security." Criteria for determining an individual's character, associations, and loyalty are set forth in Title 10, Code of Federal Regulations (CFR), Part 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material."

The appropriate granting of access authorizations by DOE, the education of employees about their security responsibilities, and the control of visitors are important functions of the personnel security program. It is the only program that determines the eligibility, and continuing eligibility, of individuals for access to classified information and material. This is especially important since DOE is responsible for the nation's nuclear weapons complex, and individuals with access authorization have direct access to nuclear weapons, classified parts, Restricted Data, SNM, or other classified matter. Therefore, eligibility for such access is of paramount importance, and the effectiveness of the personnel security program has a direct impact on the degree of reliability of those individuals who are granted an access authorization.

Organization

This introductory section (Section 1) provides general considerations and descriptive information on the personnel security topic, details on how the guide is organized, and explanations concerning the inspection tools and their use.

Sections 2 through 7 provide detailed guidance for inspecting each major personnel security subtopic:

- Section 2 – Management
- Section 3 – Personnel Access Authorization Program
- Section 4 – Safeguards and Security Awareness Program
- Section 5 – Visitor Control Program
- Section 6 – Human Reliability Program
- Section 7 – Unclassified Visits and Assignments by Foreign Nationals

Each section is further divided into several sub-elements to assist the reader in understanding topical organization and in following applicable standards and criteria.

Section 8 (Interfaces) provides guidelines to help inspectors coordinate their activities both within the personnel security topic team and with other topic teams. Typically, this includes the teams reviewing physical security systems, information security, cyber security, protection program management, and protective force programs. The section emphasizes ways that data collection can be made more efficient by coordinating with other teams, and identifies data that inspectors on other teams can collect that may be pertinent to personnel security. The personnel security team should review and conduct the listed interfaces during the planning phase to ensure that all critical elements are covered, and that efforts are not unnecessarily duplicated.

Section 9 (Analyzing Data and Interpreting Results) contains guidelines on how to organize and analyze information gathered during data collection activities. The guidelines also include statements on the significance of potential deficiencies, as well as suggestions for additional activities that may be appropriate if these deficiencies are identified. After completing each activity, inspectors can refer to this section to determine whether additional activities are needed to collect sufficient information necessary to evaluate the system.
Appendix A (Data Analysis Forms) contains forms and worksheets that may be helpful to inspectors during data collection.

Using the Topic-Specific Tools

Sections 2 through 7 provide topic-specific information intended to help inspectors prepare for and conduct an inspection. The information is organized by subtopic and, further, by sub-element:

- Management: Typically management is ultimately responsible for the overall personnel security program through planning, training, and providing necessary resources. The degree of protection that a personnel security program affords is most often determined by the degree of support received by management.

- Personnel access authorization program: Distinctive for determining the eligibility of individuals for access to classified information and material, the program addresses appropriate levels of access, pre-employment screening, and adjudication of cases. Reinvestigations, along with the interim access authorization program, are also addressed.

- Safeguards and security awareness program: A security awareness program maintained through continuous education, the program includes security briefings, the application of visual aids, and training for security professionals responsible for implementing the education program.

- Visitor control program: Concerned with eligibility and control of visitors to DOE sites and facilities, the visitor control program addresses classified visits, and visits by uncleared U.S. citizens.

- Unclassified visits and assignments by foreign nationals program is concerned with the processing of approvals and control by foreign nationals who visit or are assigned to DOE facilities.

- Human reliability program (HRP): The HRP is addressed relative to personnel security and protection programs in general. The section provides information that can be helpful to inspectors both in understanding the features of the program and examining the program during an inspection.

Each sub-element is further divided into a standard format to assist the reader. Divisions may include the following headings:

- References
- General Information
- Common Deficiencies/Potential Concerns
- Planning Activities
- Data Collection Activities

References

The References section identifies the DOE orders and other applicable policy and guidance documents that serve as the basis for evaluating the inspected program and identifying findings. Policy memoranda are usually included in the policy supplement appendix; however, pivotal memoranda of a permanent nature and other relevant documentation, such as Executive Orders, Site Safeguards and Security Plans (SSSPs), implementation memoranda, memoranda of agreement, procedural guides, and certain manuals may be included in the References section. It is also useful to refer to the applicable orders and other guidance during interviews and data collection to ensure that all relevant information has been collected.

In some cases, the References section may identify memoranda from DOE Headquarters that clarify or revise the policies and standards defined in DOE orders and other guidance. Inspectors must be aware of these clarifications and revisions, since inspection objectives include verifying compliance with DOE directives. Since new memoranda are continually being issued, OA-10 inspectors should determine whether additional memoranda have been issued, and if so, whether they apply specifically to the inspected topic and facility.

General Information

The General Information section defines the scope of the subtopic, provides a framework for identifying and characterizing security interests, furnishes guidelines intended to help inspectors focus on the unique features and problems associated with protecting and inspecting each type of security interest, and discusses commonly used terms.

Common Deficiencies/ Potential Concerns

The Common Deficiencies/Potential Concerns section lists deficiencies and concerns that OA-10 has encountered on previous inspections. That is not to say that the identified deficiencies are evident at every facility. However, these deficiencies have been noted often enough to warrant special attention during inspections. Associated with each potential deficiency or concern is a short discussion that gives more detail. Where appropriate, general guidelines are provided to help the inspector identify site-specific factors that may indicate that an identified deficiency is likely to be present. The information in this section is intended to help the inspector further focus the inspection. By reviewing the section before collecting data, inspectors can be alert for such deficiencies and concerns at the inspected facility during interviews and other data collecting activities.

Planning Activities

The Planning Activities section identifies activities normally conducted by the personnel security topic team during the planning phase of an inspection, including preplanning, review of documents, and interviews with facility representatives. The information in this section is intended to promote systematic data collection, and to ensure that critical program elements are not overlooked.

Data Collection Activities

This section identifies activities that inspectors may choose to perform during data collection. The information is intended to be reasonably comprehensive, although it is recognized that every conceivable variation cannot be addressed. Typically, the activities are selected during the planning effort, and organized by functional element or by the type of system used to provide protection. They include activities that are most often conducted, and reflect as much OA data collection experience and expertise as possible. Activities include tours, interviews, observations, and performance tests, although inspectors do not normally perform every activity on every inspection. Activities are identified by an alphabetical letter for easy reference and assignment of data collection tasks.

Validation

Validation is one of the most important activities conducted during the inspection. It is the procedure OA-10 inspectors use to verify the accuracy of the information obtained during data collection activities. The OA-10 validation process, discussed in detail in the OA-10 Safeguards and Security Appraisal Process Guide, includes on-the-spot validations, daily validations, and summary validations.

Inspectors should ensure that they are validating facts, conclusions and impact, not conjecture. Facts (data points) noted during the inspection of the personnel security program should be validated with facility representatives as they become apparent, if representatives accompany the inspection team. If facility representatives do not accompany the inspection team, the data should be validated during the daily validation meetings with site personnel.

Validation becomes even more difficult when personnel security inspection team members must separate and work independently in order to cover all selected topic elements. For example, one or more team members may be assigned to look at security education, while others check visitor control procedures or review personnel security cases. When this separation is necessary, it is more difficult for team members to coordinate and share information in a timely manner. This makes coordination and validation even more important, not only for team members but for site representatives who may have also been separated as they accompany OA-10 personnel. Since the personnel security topic is widespread, affecting a number of protection activities, it is particularly important that team members keep track of significant information to ensure that it is reiterated and the facts confirmed during the daily and summary validations.

Using the Policy Supplements

It is important that inspectors be aware of policy supplement memoranda, since inspection objectives include verifying compliance with all the various DOE directives. Because new memoranda are continually being issued, inspectors should determine whether memoranda have been issued or whether new directives have been issued that apply specifically to the inspected facility. Requirements of any such memoranda should be identified and included in planning the inspection.

Using the Tools in Each Inspection Phase

The inspection tools are intended to be useful during all phases of an inspection. The following enumerates some of the tools usually considered during each inspection phase.

In the **planning stage**, inspectors:

- Use the General Information section to characterize the program and focus the inspection.

- Perform the activities identified under Planning Activities to collect the information necessary to further characterize the program and focus the inspection. Thorough planning for an inspection cannot be overemphasized.

- Review Common Deficiencies/Potential Concerns to determine whether any of the deficiencies are apparent, and to identify site-specific features that may indicate that more emphasis should be placed on selected areas or activities.

- Assign specific tasks to individual inspectors (or small teams of inspectors) by selecting specific items from the Data Collection Activities section. The assignments should be made to optimize efficiency and ensure that all high-priority activities are accomplished. The guidelines under the Interfaces section should be considered when assigning tasks to ensure that efforts are not duplicated.

- Schedule data collection activities to optimize efficiency by ensuring that high-priority activities are conducted early in the process.

- Review the referenced DOE orders, guidance sections, memoranda, and applicable policy supplements to ensure that they are current.

In the **conduct phase**, inspectors:

- Use the detailed information in the Data Collection Activities section to guide interviews and data collection.

- Review Common Deficiencies/Potential Concerns after completing each data collection activity to determine whether any common deficiencies are apparent at the facility. If so, inspectors should then determine whether subsequent activities should be conducted to further distinguish the deficiency or determine the root cause.

- Review the Data and Results section after completing each data collection activity to determine whether additional data are needed to evaluate the program.

In the **closure phase**, inspectors:

- Refer to the appropriate references (DOE orders, other guidance, policy supplements, etc.) to determine whether the facility is complying with all applicable requirements, including those issued by DOE Headquarters.

- Use the Data and Results section to help analyze the impacts of identified deficiencies.

In the **follow-up phase**, inspectors:

- Review comments received on the final draft report.

- Review and comment on adequacy of the corrective action plan submitted by the site.

- Provide appropriate input to the final report.

- Prepare any policy issues or other reports for Headquarters staff elements.

Integrated Security Management

In the environment, safety, and health (ES&H) arena, DOE uses an approach called integrated safety management (ISM) that has helped to improve management of ES&H programs. As part of the ISM approach, DOE has delineated guiding principles and core functions of safety management that establish the framework for ISM.

The seven ES&H guiding principles of ISM are:

- Line management responsibility
- Clear roles and responsibilities
- Competence commensurate with responsibilities
- Balanced priorities
- Identification of standards and requirements
- Hazard controls tailored to work being performed
- Operations authorization.

The five ES&H core functions of ISM are:

- Define work
- Analyze vulnerabilities
- Identify and implement controls
- Perform work within controls
- Feedback and improvement.

Several DOE sites are considering the benefits of adopting a similar approach for safeguards and security programs. This approach is generally referred to as integrated security management. Development of the safeguards and security policies, such as the integrated security management concept, is the responsibility of the Office of Security and Emergency Operations (SO). If adopted, integrated security management would be formally established through the DOE directives system.

Although not currently a formal policy in the security arena, many aspects of the guiding principles and core functions of DOE's ES&H ISM policy are fundamental to management of any program. In addition, it is sometimes useful to apply ISM concepts in planning and conducting safeguards and security inspections and in analyzing data related to the effectiveness of DOE site safeguards and security programs. Further, the use of ISM concepts can be a useful approach for diagnosing the root causes of identified weaknesses, and thus can benefit the site by organizing inspection results in a manner that highlights root causes.

In view of the potential benefits of integrated security management, OA has taken a proactive approach to designing this Personnel Security Inspectors Guide to reflect certain aspects of the integrated security management concept. Specifically, OA has organized the relevant section of this Personnel Security Inspectors Guide (i.e., Section 2, Management) to parallel certain aspects of the ISM principles and core functions. Also, Section 9, Analyzing Data and Interpreting Results, includes a brief discussion of the use of the integrated security management concepts as an analytical tool.

For the purposes of this Personnel Security Inspectors Guide, OA has established four general categories that encompass the concepts embodied in the guiding principles and core functions of ISM. These four categories are listed below:

Line Management Responsibility for Safeguards and Security. This category encompasses the corresponding ISM guiding principles that relate to management responsibilities (i.e., line management responsibility for safety, clear roles and responsibilities, and balanced priorities).

Personnel Competence and Training. The category encompasses the ISM guiding principle related to competence of personnel (i.e., competence commensurate with responsibilities). It also encompasses DOE requirements related to ensuring that personnel performing safeguards and security duties are properly trained and qualified, and the need for sufficient requirements and an appropriate skill mix.

Comprehensive Requirements. This category encompasses the corresponding ISM guiding principles and core functions that relate to policies, requirements, and implementation of requirements (i.e., identification of safeguards and security standards and requirements, protection measures tailored to security interests and programmatic activities, operations authorization, define work, analyze vulnerabilities, identify and implement controls, and perform work within controls).

Feedback and Improvement. This category encompasses the corresponding ISM core function (i.e., feedback and improvement) and DOE requirements related to DOE line management oversight and contractor self-assessments.

It is important to note that the categories above are only used to organize information in the Inspectors Guide in a way that will help inspectors gather data about management performance in a structured and consistent manner. OA will not use the guiding principles or core functions as a basis for ratings, and will not cite them as the basis for findings (unless and until a formal policy is promulgated). Further, OA has only identified general categories of information that would be expected to be in an integrated security management program. OA did not attempt to specifically define guiding principles for the safeguards and security arena because the development of such policies is the responsibility and prerogative of SO.

Section 2

MANAGEMENT

Contents

References 2-1
General Information 2-1
Common Deficiencies/Potential Concerns 2-2
Planning Activities 2-4
Data Collection Activities 2-5

References

DOE Order 472.1B
DOE Manual 472.1-1
Site Safeguards and Security Plan (SSSP)
Preparation Guide
Office of Management and Budget (OMB)
Circular A-76

General Information

The DOE personnel security program (to include the HRP) is a major component in the protection of DOE security interests and represents an important part of the annual budget.

The scope of the personnel security program is broad. It not only provides for the determination of individual eligibility for access to classified matter, but also for re-evaluation for continued access eligibility every five years based on the need-to-know. It is the only program to focus on individual eligibility for access throughout the life of the access authorization—from grant to termination. Although other programs, such as the counterintelligence awareness program and the operations security (OPSEC) program, are designed to increase employee awareness relative to foreign intelligence collection activities and the unwitting release of classified and sensitive unclassified information, the personnel security program focuses on security awareness through a continuing security education program. In addition, in today's environment of more "openness" and information exchange, added emphasis is now being placed on classified, unclassified, and foreign national visits to DOE sites, including visitor control, all included as part of the personnel security program.

A strong personnel security program (to include the HRP) represents a logical and cost-effective approach to protecting against the "insider threat." Insiders represent a major threat since they have authorized access that effectively bypasses some elements of protection systems and may have extensive knowledge of a facility. Since the human element may represent the weakest link in any protection program, it is important that management recognizes the significance of an effective personnel security program. Coupled with human reliability programs for those individuals who have access to Category I quantities of SNM or who are assigned nuclear explosive duties, the personnel security program can produce an even more meaningful degree of protection.

The insider protection program in the SSSP Preparation Guide provides guidance concerning the use of personnel security factors in risk reduction. Although the guidance is largely subjective, any determination of the level of assumed risk without considering personnel security is likely to be flawed.

Effective security planning is also an important management function that can make the difference between a weak and a strong protection program. It is important that management include personnel security representatives in all security planning to ensure that risks involving cleared and uncleared personnel are appropriately addressed and factored into the overall protection strategy. Also, management is pivotal in ensuring that personnel security plans and policies are adjusted to meet changing threat situations. The personnel security program is usually described in the Facility Description and Operating Plan portion of the SSSP. Management planning and budgets for personnel security resources are often described in the resource plan portion of the SSSP, although not all facilities include a resource plan in the SSSP.

Another indication of effective management is whether adequate personnel resources are available to perform all personnel security program functions in a timely manner, such as access terminations, Central Personnel Clearance Index (CPCI) input, submission of requests for investigations, and screening of security forms. It is important that adequate staffing levels are maintained and that individuals performing critical tasks in the personnel security system are properly trained.

Finally, management support is essential to ensure the success of all other features of the overall personnel security program, to include the personnel access authorization process, the security education program, and visitor control, which are discussed in detail in subsequent sections.

Common Deficiencies/ Potential Concerns

Line Management Responsibility for Safeguards and Security

Inadequate Involvement of Personnel Security in Overall Protection Program. Often, personnel security concerns are not fully or adequately considered in the implementation of the overall security program. This lack of involvement may be indicated by the omission of personnel security professionals from threat analysis studies, management level meetings, and budget allocation deliberations. It is important for management to consider personnel security concerns in administering the overall security program because of the intrinsic impact of the personnel security program on individual access to classified matter. Lack of participation by personnel security professionals is usually a sign of insufficient management support for the personnel security program, which in turn may indicate that the program or elements of the program are deficient.

Inadequate Resources. A primary means of demonstrating management support for the personnel security program is providing sufficient resources. Primarily, this means ensuring that sufficient funds and adequate DOE personnel (supplemented with contractor personnel, as appropriate) are available to effectively implement the personnel security program and handle all critical personnel security functions. Without adequate resources, access authorizations cannot be processed efficiently and within prescribed time frames, access authorization requests will be delayed, initial and reinvestigation results cannot be screened and analyzed in a timely manner, and a backlog of interviews or other actions required to resolve derogatory information or support processing for administrative review will result. Also, a high number of backlogged cases could cause a facility to sacrifice quality for quantity, resulting in decisions to grant access authorizations without sufficient adjudication.

Lack of Management Attention or Support. Deficiencies in a number of personnel security subtopic elements usually indicate a general lack of management support (for example, delays resulting from processing unnecessary access authorization requests, minimal participation in the security education and awareness briefings, and lack of proper visitor control). When there is an accumulation of deficiencies, and the results of interviews with personnel security professionals indicate that they are unable to accomplish their assigned tasks due to overload, it is likely that there is a need for additional management commitment and support. Also, many personnel security specialists are assigned secondary duties and thus have insufficient time for their primary personnel security duties.

Reduction and Downgrading of Access Authorizations. Because of budgetary impacts and the risk of unauthorized access, management has recently become more involved in the excess access authorizations issue. The DOE community has realized for some time that many cleared people are either cleared at too high a level, or do not need an access authorization at all. For example, some people have “Q” access authorizations merely to gain physical access to their workplaces, even though their job assignments do not involve access to Category I or II quantities of SNM or Secret Restricted Data. Headquarters and Operations Office personnel have implemented various means to reduce or downgrade the number of access authorizations; however, additional reductions are necessary. It is important that management be committed to the reduction and downgrading of access authorizations, and that access authorizations be granted only to individuals with a valid need-to-know. In some cases, senior Operations Office management interaction with senior contractor management is necessary to overcome the traditional thinking that “all employees must have a Q access authorization.”

Personnel Competence and Training

Inadequate Training. The success of any personnel security program largely depends upon the capability of the people assigned. Management can enhance the capability of these individuals by ensuring that they are adequately trained. This is especially true for some of the more critical functions. For example, the training of personnel security staff in analyzing derogatory information and conducting interviews is key to the proper application of the criteria (10 CFR, Part 710) for adjudication of cases with derogatory information and preparation of cases for administrative review.

Also important is the type of training received. Most personnel security specialists receive training in case review and interviewing techniques; however, many specialists fail to make the connection between derogatory issues and national security. Although inspectors must determine whether deficiencies in the personnel security program result from a lack of personnel or poor utilization of existing staff, deficiencies will usually be found if personnel security functions are assigned to untrained and inexperienced people. Personal prejudices and biases of adjudicators usually result when inadequately trained personnel are performing these critical functions.

Comprehensive Requirements

Inadequate Planning. Frequently, management gives inadequate consideration to personnel security issues during planning activities. Also, personnel security concerns may not be adequately covered in the appropriate planning documents (for example, the SSSP and supporting Vulnerability Analyses [VAs] for Category I SNM facilities). During planning, it is important that managers consider the impact on access authorizations, security education requirements, and visitor control. For example, the reconfiguration of a facility without considering the impacts on personnel security may result in an inordinate number of unnecessary access authorizations or major problems in processing and escorting uncleared visitors.

Feedback and Improvement

Inadequate Self-Assessment Process. Not all facilities have implemented a comprehensive self-assessment program. Others lack the expertise to implement such a program effectively. Therefore, they rely on periodic security surveys to provide data for self-assessment of the local personnel security program. The lack of an effective self-assessment program can result in deficiencies going undetected and uncorrected for extended periods.

Inadequate Corrective Action Plans. This is somewhat common and potentially serious deficiency that can result in deficiencies not being corrected. Organizations frequently fail to effectively accomplish one or more of the following actions: (1) analyze (root cause and cost effectiveness) and prioritize deficiencies so that resources can be used to correct the most serious first, (2) establish a corrective action schedule with milestones so progress can be monitored and slippages identified early, (3) assign responsibility for completion to specific organizations and individuals, (4) continually update the plan as known deficiencies are corrected and new ones are identified, and (5) ensure that adequate resources are applied to correcting deficiencies. Frequently, facility managers devote their resources to "putting out brush fires" (that is, correcting the most recently identified deficiency instead of the most serious, and habitually correcting symptoms rather than the root causes of systemic deficiencies).

Incomplete or Inadequate Deficiency Tracking Systems. Tracking system inadequacy is a common and potentially serious deficiency often found in the management area. Tracking system problems can result in not correcting deficiencies in a timely manner, or not correcting them at all. The two most common problems found in tracking systems are incompleteness and inaccuracy. Often, the system is incomplete because supervisors or operators fail to list all deficiencies. They are inaccurate when corrective actions are shown as complete when they are not, or when they have not adequately dealt with the problem. Occasionally, inappropriate corrective action based on inaccurate tracking data creates new problems.

No Root Cause Analysis of Deficiencies. Another potentially serious management deficiency is the failure of organizations to determine the underlying cause of deficiencies. This usually results in the same deficiencies recurring. Many times, the organization corrects the surface problem or symptom rather than identifying and correcting the underlying cause—the root cause. If performed correctly, a root cause analysis may reveal the causes of errors (e.g., ambiguous procedures or insufficient training). Unless management accurately determines the root cause of identified deficiencies, it is likely that similar deficiencies will recur.

Planning Activities

During the planning meeting, inspectors interview points of contact and review available documentation, including facility personnel security staffing levels. Significant elements to cover include:

- The SSSP to determine whether management has provided meaningful personnel security input, whether any exceptions to DOE policy have been approved and, if so, whether the exceptions have been appropriately justified, documented, and approved at the required level.

- Pertinent portions of the VAs to determine whether personnel security is included as a viable part of the overall site protection system.

- Any available resource plans to determine the extent of budget planning for personnel security in the current budget cycle and in the out years.

- The number of personnel security positions authorized, the number of positions currently filled, the job descriptions of these positions, and the locations of the positions in the facility organization.

- Personnel security organization charts.

- The duties and responsibilities of the DOE personnel security staff (are functions appropriately distributed to ensure efficiency?).

- Number and duties of contractor personnel.

- The type of training available to personnel security program professionals, both in-house and other.

- Whether the facility has performed any self-assessments of their personnel security program (if so, arrange to review the self-assessment report and any corrective action plans during the inspection).

- Whether the Operations Office surveys that include inspection of personnel security resources are available for review (if there were survey findings, were required corrective action plans developed and were deficiencies corrected?).

- The rate of turnover among personnel security staff, and the reasons for such turnover.

Data Collection Activities

Line Management Responsibility for Safeguards and Security (Includes Supervision and Allocation of Personnel Resources)

A. Usually, the extent of personnel security involvement in the overall security activity can be determined through interviews with managers, supervisors, and personnel security professionals. Interviews may provide some indication of the extent to which personnel security professionals participate in meetings, budget discussions, and management level decisions. In most cases, interviews can also disclose whether supervisors are aware of staff concerns, daily staff activities, bottlenecks in the workflow, and other personnel security issues. Finally, interviews can help inspectors determine the level of understanding of managers and supervisors concerning the impact of personnel security on the effectiveness of the protection system as a whole.

B. It is important that a number of self-assessments be reviewed to determine whether they reflect thorough coverage of the personnel security area, and if so, whether identified deficiencies have been corrected in a timely and effective manner. If self-assessment tracking systems are in place, inspectors may be able to determine whether deficiencies are being tracked and whether self-assessments of the personnel security program are truly meaningful and useful to management.

C. Although DOE orders do not define the number of positions required to operate a personnel security program, inspectors can often gain insight into whether adequate resources are devoted to the program by:

- determining the extent of backlog of requests for access authorizations and if cases with derogatory information are adequately reviewed and adjudicated expeditiously

- examining any facility evaluations of personnel security staffing levels (OMB Circular A-76 studies)

- reviewing budgets, budget requests, and staffing requests for the past two years to identify justification for increased resources and reasons for any denial of requested resources

- determining the magnitude of the personnel security task in terms of the number of cleared personnel for whom security records are maintained, and the average number of requests for initial access authorizations and reinvestigations processed each month over the past year
- determining the personnel security organization's ability to respond to "surge" situations.
- soliciting the views of supervisors, screeners, and analysts concerning the adequacy of current staffing and training programs
- examining the amount of paid and unpaid overtime by personnel security staff during the past year.

D. The number of positions authorized can be compared with the number of individuals assigned to determine the causes for vacancies, if any (for example, lack of requests or justification for additional personnel, budget constraints, hiring freezes, lack of qualified applicants). If possible, inspectors may be able to compare tasks with job descriptions to determine whether assigned personnel are doing what the position requires. Finally, it is beneficial to identify contractor or other resources assigned to support the personnel security function.

E. Interviewing managers and supervisors and reviewing pertinent documents are good ways to determine whether management has taken action to reduce or downgrade existing access authorizations. A good indication of management commitment is to determine whether Operations Offices have developed action plans for access authorization terminations and downgrading, and whether they are working closely with their contractors to establish aggressive termination and downgrading goals. It is important that the goals balance the need to eliminate unnecessary access authorizations against the need to retain enough cleared people to meet rapidly changing programmatic requirements. Also, it is important to determine what method is being used to monitor progress in this area (for example, surveys or self-assessments).

Personnel Competence and Training

F. It is important that inspectors interview personnel security program managers responsible for training to determine whether the training programs are complete and effective. Aspects to cover include whether the training programs are formal, whether they are based on needs and job task analyses, and whether there are written lesson plans that cover all relevant elements.

G. If a formal program is in place, inspectors may elect to review a sample of training records or certifications to determine whether personnel are receiving the training. Inspectors may also elect to attend a training session to determine whether the training covers relevant information and is appropriately tailored to the needs of the audience.

H. It is helpful to interview selected personnel security program managers and supervisors to determine their level of satisfaction with available training programs. Elements to cover include whether the training is relevant to the needs of the users, whether enough classes are offered to provide training to individuals who require it (or whether there are long waiting lists), and whether the personnel security organization has been responsive to requests for more or different training. If the personnel security staff indicate dissatisfaction with the quality or availability of training classes, inspectors can follow up those concerns with personnel security managers to gather their views. In some cases, inspectors may find that security managers cannot offer more training classes because of a lack of resources or qualified trainers.

I. Inspectors may elect to review a sample of position descriptions of specific individuals who have responsibilities for the personnel security program to verify that responsibilities are actually reflected at the individual's level. Inspectors can also review individual position descriptions and performance goals of persons in the operations and production departments that have responsibilities related to personnel security (e.g., hosts) to determine whether individuals are held accountable for their performance in the personnel security functions program.

J. Inspectors should review actual versus authorized staffing levels for personnel security positions to determine whether the program is operating short-handed. Inspectors must be especially watchful for non-personnel security responsibilities being assigned to key program personnel, detracting from their ability to perform personnel security duties.

Comprehensive Requirements (Includes Plans, Orders, and Records)

K. Document review is helpful in determining the magnitude of the personnel security planning effort. The SSSP and other associated planning documents are good sources for determining whether personnel security factors are included in the planning process. Also, implementing instructions and other memoranda relative to the personnel security Order 472.1B and DOE Manual 472.1-1 may give inspectors information on the emphasis given to personnel security during planning. A review of job descriptions and job task analyses is a good way to determine whether personnel security positions are receiving adequate attention or whether the documentation on these positions is merely perfunctory. Interviews with personnel involved in the planning process may reveal whether personnel security issues are considered during planning and, if so, whether the degree of significance placed on personnel security is suitable as compared to other security concerns, such as the protective force, physical security systems, and information security.

L. Inspectors should determine whether the persons responsible for the personnel security program are in a position to ensure compliance. This may involve reviewing the facility's policies and procedures to determine whether the manager has the authority to enforce compliance and resolve issues identified during self-assessments or other similar activities. Additionally, interviews with managers in the security department and operations and production departments should be conducted to determine whether the security organization has any problems getting the operations or production personnel to implement required procedures. If initial interviews indicate questions about the operations or production organization's commitment to implementing required personnel security measures, inspectors may elect to conduct more detailed interviews and document reviews to determine whether problems exist. This detailed review may involve examining findings identified in self-assessments, surveys, and inspections to determine whether corrective actions were implemented in a timely manner, or whether repeated memoranda from the security organization were necessary before the operations or production personnel took action.

M. Inspectors should determine how management communicates its goals and objectives and stresses the importance of personnel security. Inspectors should determine what incentives are used to encourage good performance and what programs are used to maintain an appropriate level of security awareness.

Feedback and Improvement

N. Most organizations have some type of central, integrated system to identify and follow the status of deficiencies identified during self-assessments, operations office surveys, and inspections. Inspectors should determine what system or systems are being used. Sometimes it is a comprehensive system that includes all safeguards and security-related deficiencies. Other times, each area, including personnel security, has a separate tracking system. Self-assessment programs are the key to effective management oversight of personnel security.

O. Inspectors should review the self-assessment program in detail. They should determine whether self-assessments are performed regularly and whether they review all aspects of the personnel security program. Selected self-assessment reports should be reviewed to determine whether the root causes are identified when deficiencies are found. It is helpful to compare the results of the facility self-assessments to inspection findings or other audit results to elarn whether the self-assessments are equally as effective.

P. Inspectors should determine who actually performs the self-assessments. At the operations office this may be security survey staff, as they perform the annual survey. If the persons who actually perform personnel security functions conduct the self-assessments, there should be some form of independent verification or evaluation of the results. Inspectors should determine whether deficiencies identified during self-assessments are entered into the tracking system, and how corrective actions are selected and achieved.

Q. Inspectors who should determine whether an organization has a tracking system and how it operates. In conjunction with the survey program topic team, they should determine whether the tracking systems have a means of monitoring the status of all inspections, surveys, self-assessments, and other similar activities. Also, inspectors should determine whether there is a formal system to independently verify that corrective actions have been completed and that the original problem has been effectively resolved. Inspectors may elect to select a sample of personnel security deficiencies from several sources and determine whether they were entered into the tracking system. Finally, they can select a sample of deficiencies indicated as closed to verify that they have in fact been adequately corrected.

R. Inspectors should determine whether corrective action plans exist for deficiencies and whether deficiencies are analyzed and prioritized. They should determine whether schedules and milestones have been established, and whether specific responsibilities to ensure completion have been assigned down to the individual level. Inspectors should also determine whether root cause analyses are performed. If so, the inspectors should request documentation on root cause analyses for significant deficiencies listed in the tracking system and the rationale for the particular course of corrective actions chosen. As a related activity, inspectors may elect to review how resources required for corrective actions are introduced into the budget process.

S. Inspectors should review the role of DOE oversight by interviewing selected DOE security or survey managers to determine how DOE implements their responsibilities. Specific items to cover include how DOE reviews the contractor personnel security program functions on surveys, how DOE tracks the program status, and how DOE and the facility interact on a day-to-day basis. Additionally, key facility managers should be interviewed to gather their views on the same subjects.

Section 3

PERSONNEL ACCESS AUTHORIZATION PROGRAM

Contents

3.1 Levels of Access 3-3
3.2 Pre-employment Screening 3-7
3.3 Processing Access Authorization Requests 3-9
3.4 Screening and Analysis 3-13
3.5 Processing Derogatory Information 3-17
3.6 Reinvestigations 3-21
3.7 Interim Access Authorizations 3-23

The process of determining eligibility for access authorization is at the heart of the personnel security program, and is the first line of defense against the insider threat. A sufficient number of trained personnel must be allocated to this effort to ensure the credible and timely processing of requests, and the screening and analysis of initial access authorizations and reinvestigations. Also of importance is the availability of qualified staff to ensure the proper processing of cases containing unresolved derogatory information, which requires following the Administrative Review procedures outlined in 10 CFR 710 and DOE Manual 472.1-1. A lack of trained personnel security specialists, or ineffective utilization of existing staff, may be the root cause of many programmatic deficiencies in the personnel security access authorization program. Further, the element of Reinvestigations, designed to periodically reinvestigate individuals already holding access authorizations, is important. A lack of trained personnel will have an adverse impact on this important element.

The DOE personnel access authorization program establishes a structured and uniform approach for determining eligibility for DOE access authorizations. The basis for this program is the Atomic Energy Act of 1954, as amended, which provides statutory authority for establishing and implementing a DOE security program for controlling access of Restricted Data and SNM.

Only individuals whose jobs require access to Restricted Data, SNM, or classified information are to be processed for access authorization. Additionally, pre-employment screening is required of employees being hired for positions requiring such access by DOE Management and Operating (M&O) contractors who operate DOE-owned facilities.

The Office of Personnel Management (OPM) is the primary provider of security background investigations (BIs) to DOE. DOE may also accept the results of other government agency BIs that meet DOE requirements. After DOE has received the results of a BI, they are reviewed and adjudicated in accordance with the criteria set forth in 10 CFR, Part 710. Under the requirements of the reinvestigation program, individuals granted DOE access authorization must be reinvestigated every five years (see Figure 1).

The following sections provide a guide for inspecting the Personnel Access Authorization subtopic and its elements.

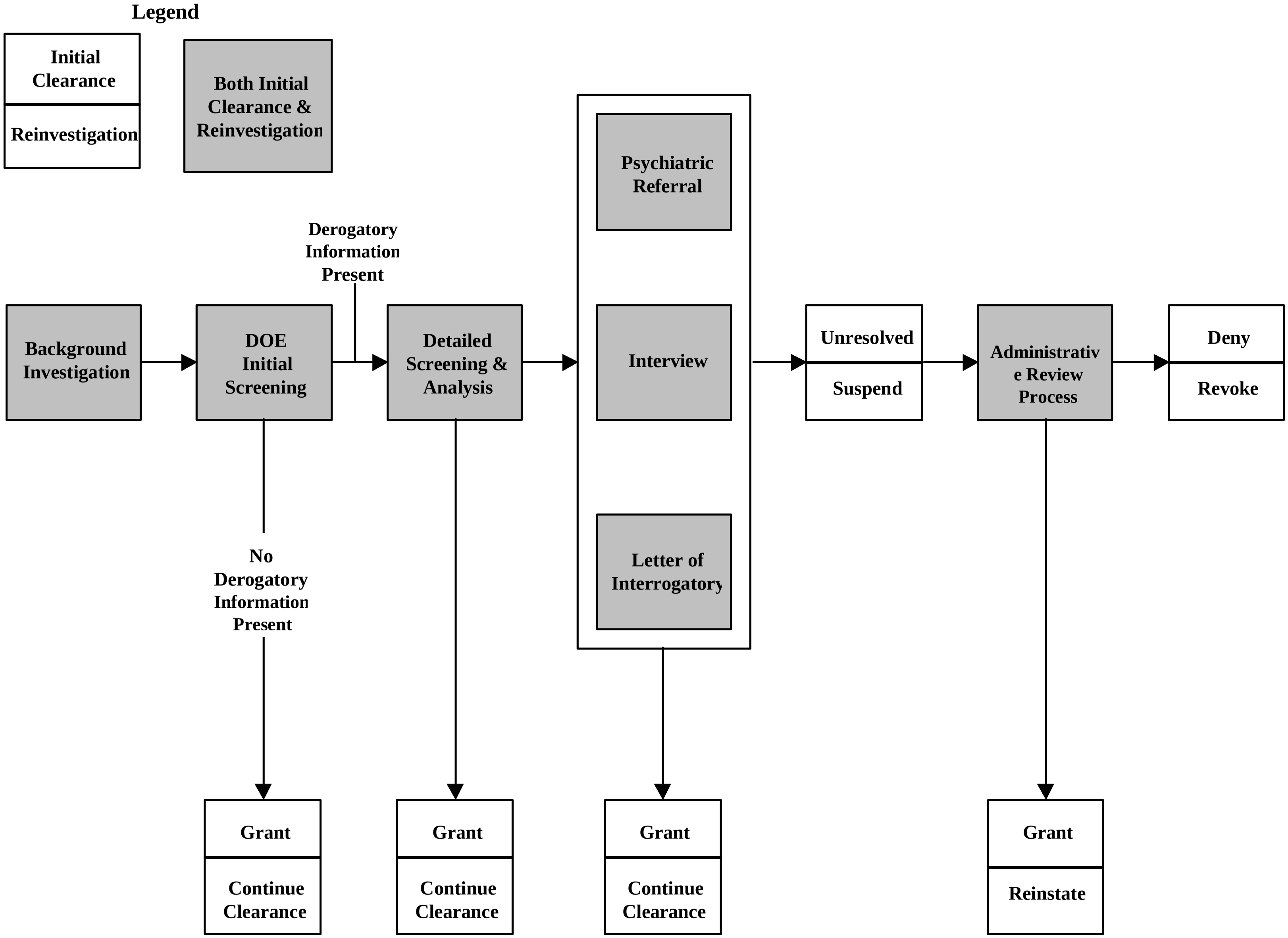

Figure 1. DOE Access Authorization Process

Section 3.1

Levels of Access

Contents

References 3-3
General Information 3-3
Common Deficiencies/Potential Concerns 3-3
Planning Activities 3-4
Data Collection Activities 3-5

References

DOE Order 472.1B
DOE Manual 472.1-1

General Information

DOE policy for determining appropriate levels of access to classified information or SNM is found in DOE Order 472.1B and DOE Manual 472.1-1, Chapter 1, "Access Authorization

Requests for access authorization are certified by appropriate personnel at the DOE office or contractor facility. The key elements of the process are certifying requests for access authorization are necessary, ensuring that the level of access is consistent with the work performed, and ensuring that the access authorization is terminated when the need no longer exists.

The initial request for access authorization must be complete and fully justified before it is submitted for processing. The process of granting access authorization (that is, pre-employment screening, processing initial requests, background investigations conducted by OPM contractors, review and adjudication of background investigation reports, and the decision to grant or deny the authorization) is a timely process and involves considerable cost and effort. Therefore, only those access authorizations that are clearly necessary should be requested.

Although resources are addressed in Section 2, Management, inspectors should specifically determine whether sufficient personnel are assigned to security access authorization processing. If not enough adequately trained personnel are assigned to this function, significant deficiencies and backlogs in the access authorization processing system can result.

Common Deficiencies/ Potential Concerns

Unjustified Requests for Access Authorization

Access authorizations are often requested when the justification is questionable. Certification procedures must support the DOE requirement that access authorizations be initiated only when the duties of a position require access to classified information or to SNM, and are consistent with the work performed. Requests not meeting this criteria should not be processed or forwarded.

Inappropriate Access Level

In some cases the requested access level is higher than the position requires. For example, a facility may request a "Q" access authorization for a position that requires access to Confidential information only, or for an individual who does not necessarily need access to a security area containing SNM to accomplish assigned work. The Operations

Office is responsible, and has the authority, to determine whether individuals require access and at what level. Inspectors would not normally question the Operations Office's judgment on individual cases; however, inspectors should determine whether the Operations Office has adequate procedures for determining whether requests are fully justified. Inspectors should also determine whether the Operations Office reviews categories of personnel (for example, janitors and cafeteria workers) for the appropriateness of their access levels.

Unjustified Retention of Access Authorizations

Changes in the status of cleared personnel may justify terminating or reducing the level of access authorization. Job changes, misconduct, reassignment of duties, organizational restructuring, foreign travel, prolonged absence, and the results of inspections are of the some events that might affect justification for continuing access authorization.

A particular problem exists in controlling access authorizations granted to contractors employed for specific jobs with limited duration. Often, the Operations Office lacks an adequate system for tracking the status of the authorization to determine the need for it to continue after job completion. As a result, the authorization may not be terminated in a timely manner. If this happens frequently, the number of contractor personnel who no longer need access continues to grow, increasing the possibility of unauthorized personnel gaining access.

In some cases, although prohibited by DOE order, access authorizations are continued at the holder's request in order to enhance future job opportunities, or to create a "pool" of cleared personnel to meet anticipated requirements. These situations also increase the possibility for unauthorized access.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to levels of access. Elements to cover include:

- Procedures used at the facility to certify requests for access authorization.
- Identification of all personnel who are responsible for certifying requests for access authorization and their positions, organization, and location.
- General procedures used to determine access levels for contractor and subcontractor personnel.
- Approximate number of personnel with access authorizations and the access authorization types.
- Procedures, if any, used to review the need for continued access.
- Identification of all classified areas in the facility.
- Operations Office surveys that include inspection of procedures used to determine access levels (if available, were findings identified and corrected?).
- Approved or pending exceptions to DOE requirements and policy clarification memoranda.
- Self-assessments of the procedures for determining levels of access (if self-assessments have been performed, arrange to review the self-assessment report and corrective action plan during the inspection).

Data Collection Activities

Certification Procedures

A. Inspectors should interview individuals responsible for handling requests for access authorization to determine how the process is conducted, and how the need for access is certified. It is important that the justification for the access is based on the duties of the position, that the duties require access to classified information or SNM and that the level of access authorization is appropriate. It is usually helpful for the responsible individuals to explain, step by step, how the need for access and the level of access is determined.

Procedures for Reviewing Continuance of Access Authorization

B. Inspectors should review selected personnel security files to determine whether the procedures for verifying continued need for access authorizations are implemented as described. In particular, inspectors should note the portions of the request dealing with justification and certification to determine whether they are properly implemented.

C. Positions requiring access should be compared with the number of individuals currently holding access authorizations. If there are more access authorizations than required by positions, inspectors should determine the justification for the additional access authorizations.

D. Inspectors should request operational departments to provide the files for a sample of cleared individuals who have changed positions. If the individuals' duties no longer require access to classified information or SNM, inspectors should determine whether action was taken to terminate the authorizations, or otherwise change the level of access.

E. Inspectors should interview supervisors and cleared personnel to determine whether their job requirements establish the need for their particular access authorization. If an individual rarely handles classified material, inspectors should determine whether the Operations Office considered adjusting the level of access or canceling the authorization entirely.

F. Inspectors should review files on contractors to determine whether their duties justify access. Inspectors should obtain a sample list of terminated contractor and subcontractor personnel to determine whether action was taken to terminate their access authorizations in a timely manner.

This page is intentionally left blank.

Section 3.2

Pre-employment Screening

Contents

References 3-7
General Information 3-7
Common Deficiencies/Potential Concerns 3-7
Planning Activities 3-8
Data Collection Activities 3-8

References

DOE Order 472.1B
DOE Manual 472.1-1
Department of Energy Acquisition Regulation (DEAR)
48 CFR 970.2201(b)(1)(ii)

General Information

In conformance with the referenced DEAR, pre-employment screening of DOE Management and Operating (M&O) contractors is conducted to identify any readily available derogatory information that would preclude employment for a potential contractor employee. (In some instances, an M&O contractor may require pre-employment screening for its subcontractors.) Pre-employment screening by the contractor involves checking public records, law enforcement agencies, credit organizations, references, and educational institutions. When submitting a request for access authorization, the contractor provides documentation certifying that this pre-employment screening has been conducted, and the results.

Before this requirement was added to the DEAR, derogatory information was identified only through costly, full field BIs. Under the current DEAR, a BI is requested only after the contractor has made an initial determination of the applicant's qualifications and suitability. Pre-employment screening, which is conducted regardless of the type of access authorization requested, is the primary basis for this determination.

Common Deficiencies/ Potential Concerns

Derogatory Information Not Forwarded to DOE

Contractors do not always forward derogatory information revealed during pre-employment screening. This failure may result from an oversight, or from ineffective procedures for providing information to DOE. It is important that all derogatory information obtained during pre-employment screening be forwarded to DOE to allow DOE to scope the investigation being submitted to OPM.

Incomplete Pre-employment Screening

Apart from derogatory information, other required information may not be included on the Questionnaires for National Security Position (QNSPs) submitted (for example, highest degree held, personal references, previous employers, and part-time employment). Incomplete information results in a delay in processing the access authorization request.

Some M&O contractors and other contractors managing DOE-owned facilities may require their subcontractors to conduct pre-employment checks. If this is the case, inspectors should view this as a requirement when reviewing the subcontractor's program.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to contractor pre-employment screening. Elements to cover include:

- Identification of cleared contractors currently used by the facility
- The approximate number of pre-employment checks currently being processed by the facility
- The names, positions, and locations of individuals responsible for reviewing pre-employment screening results
- Methods used to determine the accuracy and completeness of pre-employment screening
- Whether contractors submit written statements providing the results of their pre-employment checks, including all derogatory information
- The approximate number of recent cases in which derogatory information was found during pre-employment screening
- The approximate number of recent cases in which derogatory information was not found until after submission of the access authorization request to the investigating agency
- Facility self-assessments of contractor pre-employment screening (if self-assessments have been done, arrange to review the reports and corrective action plans during the inspection)
- Any Operations Office surveys that include inspection of pre-employment screening (if available, were survey findings identified and corrected?)
- Approved or pending exceptions to DOE requirements.

Data Collection Activities

A. Inspectors should review a number of recently submitted contractor access authorization requests to determine whether statements indicating the results of pre-employment screening were forwarded to DOE. The contractor personnel security files, or personnel files associated with these requests, should also be reviewed to determine whether information in the files coincides with information forwarded to DOE, and whether the contractor ensures that pre-employment screening includes all elements required by the DEAR (that is, highest degree attained, law enforcement agency checks, personal references, previous employers, and part-time employment).

B. Inspectors should determine whether the DOE Operations Office survey program addresses pre-employment screening.

C. Inspectors should determine how many employees were not submitted for access authorizations as a result of derogatory information uncovered through pre-employment screening.

Section 3.3

Processing Access Authorization Requests

Contents

References 3-9
General Information 3-9
Common Deficiencies/Potential Concerns 3-9
Planning Activities 3-10
Data Collection Activities 3-10

References

DOE Order 472.1B
DOE Manual 472.1-1

General Information

Specific procedures in DOE Order 472.1B and DOE Manual 472.1-1 describe each step in the processing of DOE access authorizations. Paperwork flows from initiation of the request, through certification of need, to verification of completeness, to forwarding of the request to the appropriate investigative agency by DOE. It ends with the notification of grant, continuation, or denial of the access authorization by DOE. Staffing, training, procedural guidance, and oversight significantly affect the success or failure of this process.

DOE Order 472.1B provides specific elements to help the inspector determine compliance with DOE policy in this topic.

Common Deficiencies/ Potential Concerns

Backlogs of Access Authorization Requests

As discussed in Section 2, Management, personnel security organizations may lack enough trained personnel to process the volume of work required. As a result, backlogs of requests for access authorizations develop, and the Operations Office fails to meet specified time frames. When available personnel attempt to speed up the process, mistakes and omissions often result.

Inaccurate or Unresponsive Processing Activities

The most important factors in determining the adequacy of personnel access authorization processing are accuracy, efficiency, and timeliness. Processing involves repetitive actions and a large volume of work, both of which contribute to clerical errors and employee “burnout.” Significant backlogs of work, or a large number of data entries in the CPCI that are late, incomplete, or inaccurate, may indicate inadequate management attention. A number of management tools, such as a quality assurance review by a second person, can significantly reduce the number of clerical errors.

Inadequate Training or Procedures

Personnel security staff often do not receive formal or on-the-job training for assigned tasks, resulting in delay, larger backlogs, additional mistakes, and incomplete reviews. Inadequate procedures for the processing activity can also cause turbulence, inefficiency, and delay.

Inadequate Information from Contractors

Contractor organizations do not always inform DOE of changes in status, additional information, or the cancellation of an access authorization request, thus further delaying requests submitted for contractor personnel or adding unnecessary cost. It is important that individuals responsible for processing the requests be kept informed of any changes. When an individual is no longer a candidate for a position requiring access authorization, or when an individual has terminated employment, the DOE should be notified immediately and the request for access authorization should be canceled.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to access authorization request procedures. Elements to cover include:

- A general description of the facility's access authorization processing system, including identification of organizations and personnel responsible for the activity
- Problems encountered, if any, in reviewing QNSPs (Standard Form 86) packages
- Methods for processing naturalized citizens and dealing with individuals holding dual citizenship
- Routine procedures for entering access authorizations into the CPCI
- Methods for processing interim access authorizations
- Operations Office surveys that include inspection of access authorization processing procedures (if available, were findings identified and corrected?)
- Approved or pending exceptions to DOE requirements
- Facility self-assessments of access authorization processing procedures (if available, arrange to review the self-assessment reports and corrective action plans during the inspection).

Data Collection Activities

Staffing

A. Inspectors should review staffing documents and interview staff members to determine whether enough personnel are assigned to the access authorization processing activity to ensure timely and efficient processing. It is helpful to determine whether backlogs exist, and whether they are primarily caused by a lack of personnel, or inappropriate use of existing personnel.

If an office has established production quotas for each of the employees in the access authorization process, these quotas can be examined to determine whether they are realistic and contribute to or detract from reaching objectives.

Training

B. Inspectors should determine whether assigned personnel are sufficiently trained to effectively perform assigned tasks. Security personnel should be interviewed to determine whether they are familiar with processing procedures, and whether they fully understand their responsibilities. Personnel should be asked to explain the process, including what action they would take under a number of different circumstances (for example, how they handle cases involving mental illness).

In addition to formal training attended, established in-house training should be reviewed to determine its content, relevance, and effectiveness.

Personnel Security Files

C. A number of personnel security files should be randomly selected from listings provided by the site being inspected. The listings should identify cases processed by the site in a particular time frame, usually the preceding 12 to 18 months. Separate listings should be prepared for each type of action taken (security interviews, letters of interrogatory, psychiatric referrals, clear cases, etc.). The inspector should randomly select a number of cases from each list and review each selected case to determine the appropriateness of the actions take by the site. A reasonable number of cases should be reviewed in order to determine that no systemic problem exists in the site's adjudication of cases.

D. Inspectors should determine during their review of randomly selected personnel security files whether data are arranged in the files in accordance with DOE requirements or in a similarly uniform manner to facilitate data handling and retrieval.

E. Inspectors should examine QNSPs (Standard Form 86) and fingerprint cards for errors or omissions. Inspectors should determine how often QNSPs are returned to the contractor because of errors or failure to forward derogatory information found during pre-employment screening.

F. Inspectors should verify that the procedures for processing naturalized citizens and dealing with individuals holding dual citizenship are in accordance with DOE regulations. Also, procedures for handling interim access authorizations should be examined to ensure that they are in accordance with DOE regulations.

CPCI Entry

G. Inspectors should determine whether all routine actions related to access authorizations are entered into the CPCI. Selected files should be compared to data in the CPCI to determine whether the input was made in a timely manner, whether it was accurate, and whether entries are made as required by DOE policy.

This page is intentionally left blank.

Section 3.4

Screening and Analysis

Contents

References 3-13
General Information 3-13
Common Deficiencies/Potential Concerns 3-14
Planning Activities 3-14
Data Collection Activities 3-14

References

DOE Order 472.1B
DOE Manual 472.1-1
Memorandum, Director, Office of Security and Emergency Operations to Distribution, Subject: Access to Investigation Reports Provided by the Office of Personnel Management and the Federal Bureau of Investigations, April 12, 2000.

General Information

Screening and analysis of the background investigation reports or other reported information is one of the most important aspects of the overall personnel security program.

Upon receipt of completed reports of investigation, the screening and analysis functions include checking to ensure that all items on the Standard Form 86 have been covered, that the scope of the investigation has been met, and that an evaluation of the reported information, favorable and unfavorable (in relation to the Criteria in 10 CFR, Part 710), has been made to determine whether the reported information raises substantial doubt concerning eligibility for access authorization. Reported derogatory information may be offset when considered with other reported mitigating information, for example, a single DUI arrest five years ago has not been repeated and the report of investigation contains no additional alcohol concerns.

The Screening and Analysis subtopic is a challenge to the inspector because of the common sense judgment required of DOE Operations Office personnel in adjudicating the reports of investigation and determining an individual's eligibility for access authorization. Inspectors should not place themselves in a position of questioning these judgments. Rather, they should determine whether adequate procedures are in place and being followed, and whether quality assurance functions are being performed.

The adjudication process, and determination of what constitutes substantially derogatory information requiring an administrative review, may be interpreted differently from one DOE site to another. Inspectors should be aware that each site is unique, and that one process is not necessarily better than another. What is important is that procedures are effective and produce the desired result.

The only way to appropriately implement DOE policy and law written into 10 CFR, Part 710 is to ensure that screening and analysis functions are supported by adequate training and effective management. The key factors in determining the adequacy of the screening and analysis functions are whether all security issues have been identified, and whether all issues have been mitigated or resolved and appropriately documented before determining that an access authorization will be granted or continued.

Common Deficiencies/ Potential Concerns

Lack of Timely Screening and Analysis

Lack of timely screening and analysis usually results in a backlog of authorization requests and reinvestigation cases, and time limits set by DOE may not be met. Backlogs can place pressure on management, and especially on the personnel security specialists assigned to do the work. When pressure builds, cases may be processed too quickly, resulting in inadequate case review or unfocused interviews. These, in turn, reduce the quality and efficiency of the entire processing activity. Backlogs can also develop because of understaffing.

Screening and Analysis Not Thorough

Screening and analysis of case files may not always be thorough, and may fail to identify discrepancies and derogatory information. Such failure could result from insufficient time to review cases, inadequate training or poor supervisory attention. Quality assurance functions, such as second tier reviews and supervisory review of selected cases, can alleviate these problems.

Inadequate Training or Procedures

Personnel security specialists performing screening and analysis are not always provided initial or ongoing training. It is important that these individuals be thoroughly familiar with techniques necessary for effective screening, analysis, interviewing, and Administrative Review preparation and participation. Also, policies and procedures designed to facilitate the process may be inadequate or out of date. Since the screening and analysis process is critical to the personnel security program, it is important that it receive adequate management oversight and support.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents relating to screening and analysis functions. Elements to cover include:

- Staffing levels authorized and assigned to the personnel security activity
- A general description of the screening and analyzing functions, including the handling of derogatory information, accomplishment of a 5 percent review of clear cases, interviews, letters of interrogatory, and case referrals
- Identification and location of supervisor and security specialist personnel responsible for screening and analysis
- Current case load and backlogs
- Time frames required to process cases, compared to DOE requirements
- Operations Office surveys that include inspection of screening and analysis functions (if available, were findings identified and corrected?)
- Approved or pending exceptions to DOE requirements
- Self-assessments of screening and analysis functions (if available, arrange to review the self-assessment reports and any corrective action plans during the inspection).

Data Collection Activities

Personnel Resources and Training

A. Inspectors should review the workload and overtime of personnel security specialists to determine whether sufficient resources have been allocated to perform effective screening and analysis. These individuals should be interviewed to determine their perceptions of performance, timeliness, and workload.

B. Inspectors should review personnel training records to determine whether personnel security specialists have received formal training.

Review of Case Files

C. In accordance with recent guidance (April 12, 2000, memorandum from the Director of the Office of Safeguards and Security), OA personnel are permitted to review OPM information, such as case files, as part of an assessment of the personnel security program. The same guidance allows OA personnel to review Federal Bureau of Investigation information contained in a personnel security file. When reviewing such information, OA personnel must comply with the provisions of the applicable guidance (e.g., copies of FBI information may not be made without prior FBI authorization). Inspectors should review case files by selecting a number of files from listings that show types of actions taken to gather more information (interviews, referrals to psychiatrists, letters of interrogatory, etc.) to determine whether the screening and analysis functions have been satisfactorily accomplished and are timely. If backlogs exist, inspectors should determine the causes. Interviews with security specialists will often reveal the reasons for backlogs.

D. Inspectors should review case analysis sheets from a selection of files known to contain derogatory information to determine whether the derogatory information has been appropriately resolved or mitigated. Case analysis documentation must show what the derogatory information is and the thoughts presented by the analyst as to why or why not the derogatory information poses a threat in one of the areas of the criteria (10 CFR, Part 710).

Interviews, Transcripts, and Summaries

E. Interviews add substantive information to the record by the development of pertinent facts taken from the subject's statements. Inspectors should examine the interview records to determine whether each issue is fully developed in light of the criteria (10 CFR, Part 710) to determine any vulnerability that could make the subject a potential security risk.

F. Inspectors should determine whether specific information provided by the subject has clarified the issues, or whether the investigative record needs to be extended because of security concerns.

G. Inspectors should review selected interview transcripts and summaries to determine whether they contain: a pre-interview discussion with the subject being interviewed, briefly explaining the reason for the interview (that is, a question has been raised concerning the individual's eligibility); the authority for the interview; an explanation of Section 1001 Title 18 and the Privacy Act; a statement explaining why interviews are recorded; and a statement that the subject is voluntarily participating in the interview.

H. Inspectors should review interview transcripts and summaries to determine whether they provide a clear, objective evaluation of the entire case. Transcripts should be objective, thorough, accurate, concise, well-organized, and not distorted or biased.

Supplemental Tools for Case Adjudication

I. Inspectors should determine whether analysts consider supplemental investigation, psychiatric evaluation, or security interviews to obtain additional information to adjudicate a case. The inspector's review should determine whether analysts use these tools because of a lack of resources, or because no further information from other sources is available to help adjudicate a case.

Action Taken on Receipt of Investigation Results

J. Inspectors should determine whether initial screening and notification of grant of access are completed within seven days of the receipt of completed investigations in clear cases; whether required follow-up actions are initiated within 30 days of receipt of the completed investigations; and whether personnel security interviews, when required, are scheduled within 30 days of determination to interview.

Section 3.5

Processing Derogatory Information

Contents

References 3-17
General Information 3-17
Common Deficiencies/Potential Concerns 3-17
Planning Activities 3-18
Data Collection Activities 3-18

References

10 CFR, Part 710

General Information

Upon receipt of completed investigations the screener checks the investigation reports to ensure that the items listed on the QNSP (Standard Form 86), or other related forms, have been covered, and that the DOE investigation requirements for the particular type of access authorization have been met.

Reports of investigations are analyzed to evaluate them in relation to the criteria in 10 CFR, Part 710, and to determine whether they contain derogatory information sufficient to raise substantial doubt about access authorization eligibility. If there is substantial doubt, a number of alternatives are available for resolution, including letters of interrogatory, interview, psychiatric evaluation, and additional investigation. If the derogatory information cannot be satisfactorily resolved, the case can be referred to the Office of Safeguards and Security (OSS) with a request for review and advice, or for authorization to proceed with an administrative review.

Upon receipt of authorization to proceed with an administrative review, 10 CFR, Part 710 and DOE Manual 472.1-1 provide for initiation and conduct of a hearing by the DOE Office of Hearings and Appeals. Upon completion of the hearing, the hearing officer's recommendations, accompanied by the hearing transcript, are submitted to the OSS for a final determination.

Common Deficiencies/ Potential Concerns

Backlog of Cases with Derogatory Information

A significant backlog of cases containing derogatory information might result from a lack of personnel resources or training. The processing of derogatory information is one of the most important aspects of the personnel access authorization program, and requires an adequate number of thoroughly trained individuals who can make well-informed judgments based on the criteria (10 CFR, Part 710) and other policy guidance. Well-trained personnel are especially critical for conducting effective interviews.

Inadequate Process for Resolving Derogatory Information

In some cases, derogatory information is not satisfactorily resolved before access authorization is granted. Since interpretation and resolution of information are somewhat subjective, it is important that the criteria (10 CFR, Part 710) and provisions of DOE Order 472.1B are followed as closely as possible. If derogatory information falls within the criteria, it can be resolved locally, or it can be forwarded with recommendations to OSS. If the background investigation is complete in all respects, and if the reported information is clearly outside the scope and intent of the criteria, an access authorization can be granted. It is important that guidance be in place for interpretation and resolution of derogatory information.

Deficient Process for Administrative Review

Frequently, the administrative review process does not contain all the steps outlined in 10 CFR 710. Proper handling of subpoenas, court reporter requirements, findings and recommendations, and the hearing officer's report is important to ensure proper disposition of the case.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to the processing of derogatory information. Elements to cover include:

- Identification of individuals responsible for screening and analysis, sending letters of interrogatory, conducting interviews, and referring cases to consultant psychiatrists
- Interview procedures
- Procedures for determining referrals to OSS for advice or for authorization to conduct an administrative review
- Procedures for requesting and conducting an administrative review
- Operations Office surveys that include inspection of the processing of derogatory information (if available, were survey findings identified and corrected?)
- Approved or pending exceptions to DOE requirements
- Facility self-assessments addressing the processing of derogatory information (if available, arrange to review the self-assessment reports and any corrective action plans during the inspection).

Data Collection Activities

Staff Level and Training

A. Inspectors should review staffing to determine whether adequate personnel resources are assigned to process derogatory information. Training records should be checked to determine whether these individuals have been properly trained. The persons responsible for letters of interrogatory and interviewing are especially important and should be interviewed to determine their proficiency. The results of the interviews should be compared with a selected number of case files to determine whether information provided in the interview is consistent with the file documents and with DOE policy.

Review of Case Files

B. Inspectors should review files containing derogatory information to determine whether information was satisfactorily resolved under the provisions of DOE Order 472.1B and the criteria of 10 CFR, Part 710. Inspectors should keep in mind that all reported derogatory information must have been reviewed, evaluated, and adjudicated, even if the activity exceeded the time limits of the questions on the Standard Form 86 in terms of the criteria.

C. Inspectors should review letters of interrogatory and interview transcripts to determine whether they justify case results. Cases referred for additional investigation should be examined to determine whether the referral was justified, or whether the decision on access authorization could have been based on information available before the referral.

D. Inspectors should review cases in which access authorizations were suspended to determine whether proper procedures were followed, and whether appropriate documentation exists to justify suspension of the authorization.

This page is intentionally left blank.

Section 3.6

Reinvestigations

Contents

References 3-21
General Information 3-21
Common Deficiencies/Potential Concerns 3-21
Planning Activities 3-21
Data Collection Activities 3-22

References

DOE Order 472.1B
DOE Manual 472.1-1
10 CFR, Part 710

General Information

The DOE reinvestigation process is designed to ensure the continued eligibility for access authorization of individuals employed in classified programs of DOE. It applies to all individuals possessing DOE access authorization except: 1) members of the armed services, 2) employees of agencies of the Department of Defense and their contractors, and 3) employees of other Executive Branch departments or agencies and their contractors who hold DOE “Q” non-sensitive or “L” access authorizations.

DOE orders require that all individuals holding access authorizations be re-evaluated every five years. This requirement may increase the backlog of reinvestigation cases. Also, upon reinvestigation, a number of cases may be found to contain derogatory information that needs to be resolved. A backlog may exist at some DOE sites.

Common Deficiencies/ Potential Concerns

A system must be in place to ensure that individuals submit updated QNSPs through their employer to DOE in order to ensure that DOE initiates a reinvestigation to meet the five-year requirement. Upon receipt of the reinvestigation, DOE must review the case in a timely manner to identify any security issues and address the security issues in a timely manner in that the individuals have current and continuing access pending this review.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to the reinvestigation process. Elements to cover include:

- Identification of individuals responsible for processing reinvestigation cases

- Procedures followed when derogatory information is found during a reinvestigation

- Whether the facility maintains schedules or other tracking documents relative to the reinvestigation program

- Operations Office surveys that include inspection of the reinvestigation program (if available, were findings identified and corrected?)

- Approved or pending exceptions to DOE requirements

- Facility self-assessments of their reinvestigation program (if available, arrange to review the self-assessment reports and corrective action plans during the inspection).

Data Collection Activities

A. Inspectors should review the personnel security files to determine whether reinvestigations are initiated within the time frames required by DOE Order 472.1B.

B. Inspectors should review contractor records to determine whether reinvestigation cases are submitted to DOE in a timely manner.

C. Inspectors should determine whether the continuing need for access authorization is certified by the requesting organization, and whether reinvestigation cases are reviewed against the 10 CFR, Part 710 criteria in the same manner as initial investigations.

Section 3.7

Interim Access Authorizations

Contents

References 3-23
General Information 3-23
Common Deficiencies/Potential Concerns 3-23
Planning Activities 3-24
Data Collection Activities 3-24

References

DOE Order 472.1B
DOE Manual 472.1-1
10 CFR, Part 710

General Information

Only under exceptional circumstances will an individual be permitted to have access to classified matter or be allowed to occupy a critically sensitive position prior to completion of the appropriate investigation. For example, if a project essential to the DOE would be seriously delayed unless a particular individual was granted access to classified matter, granting this individual an interim access authorization prior to completion of the access authorization process might be considered as an exceptional circumstance. In all cases, interim access authorizations are considered temporary measures, pending completion of the required investigation (which must be in process). Interim access authorizations are approved only by the Office of Security Affairs.

Requests for interim access authorizations are made only in cases where access to classified matter requires the individual to have a "Q" access authorization or when access to National Security Information requires a Top Secret access authorization. Employees requiring "L" or Secret access authorizations are not processed for interim access authorizations.

A supplement to the interim access authorization process is the accelerated access authorization program (AAAP). The AAAP is a program established to provide DOE with all of the information necessary to grant an interim "Q" access authorization prior to completion of the regular access authorization process. Applicants for the program must volunteer and consent in writing before they can participate. The program consists of completion of a National Agency Check with credit, drug testing, psychological assessment, and counterintelligence scope psychophysiological detection of deception testing. Drug screening is conducted in accordance with guidelines promulgated by the Department of Health and Human Services. A Medical Review Officer selected and approved by DOE must review all results of drug tests. Polygraph examiners must be DOE certified with extensive experience.

Common Deficiencies/ Potential Concerns

Interim Access Authorization/ AAAP

The granting of interim access authorizations are a temporary measure pending completion of a favorable background investigation and, if derogatory information is revealed in the investigation, favorable resolution of the derogatory information. DOE personnel Security Officers must address derogatory information in a timely manner since individuals with interim access authorization have current access. Some sites may improperly allow individuals with interim access authorizations to access certain categories of classified information (computer security [COMSEC], North Atlantic Treaty Organization [NATO], Weapons Data, or Special Access Programs, sensitive compartmented information [SCI]) which is not allowed until final “Q” authorization is granted.

All elements of the AAAP must have been completed before an individual is granted an interim access authorization. Participation in this program is voluntary and appropriate documentation (signed release and agreements) must be granted. As with a request for an interim access authorization, documentation showing justification for the interim access and certification that another qualified person holding a current DOE access authorization is not available to do the required work.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to interim access authorizations and the AAAP. Elements to cover include:

- Identification of individuals responsible for processing interim access authorizations and AAAP cases

- Approved procedures currently governing the program

- Correspondence between the DOE Personnel Security Office and the AAAP Test Center.

Data Collection Activities

A. Inspectors should review the personnel security files of individuals processed for interim access authorization, to include interim access authorizations based upon the AAAP.

B. Inspectors should review documentation in each case to determine if all required elements have been completed before granting interim access authorization.

C. Inspectors should determine that individuals with interim access authorization are not given access to requiring specific programmatic approval, such as COMSEC, NATO, Weapons Data, Special Access Programs, and SCI.

Section 4

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

Contents

4.1 Administration and Management 4-3
4.2 Security Education and Awareness Briefings 4-7
4.3 Visual Aids for Security Education and Awareness 4-13
4.4 Safeguards and Security Awareness Coordinator Training 4-15

The DOE safeguards and security awareness program is designed to ensure that all individuals are informed of their security responsibilities associated with DOE programs and activities. The program also alerts individuals to actual or potential threats, and motivates them to maintain a high level of security awareness.

DOE requires formulation, implementation, and maintenance of a structured security education program in all DOE and contractor organizations where there is a requirement for access authorization, access to SNM, or protection and control of nuclear material.

DOE Order 470.1, Chapter IV, provides a structured approach for inspecting this topic.

This page is intentionally left blank.

Section 4.1

Administration and Management

Contents

References 4-3
General Information 4-3
Common Deficiencies/Potential Concerns 4-3
Planning Activities 4-4
Data Collection Activities 4-4

References

DOE Order 470.1, Chapter IV
National Security Decision Directive No. 197, November 1, 1985

General Information

DOE requires that a safeguards and security awareness program be established that addresses access authorization requirements, physical security features of the facility, nature of the work, classification and sensitivity of information, and the number of personnel in the facility for which security protection is provided. Typically, security education programs will include lesson plans, briefing objectives, instructional aids, and evaluation methods.

Managers and supervisors can enhance the program by providing each employee with job-related, facility-oriented security education, regardless of access authorization level. Instruction sessions that are coordinated through local security officials and lesson plans that are kept up-to-date and maintained as a continuous effort can best provide effective, appropriate security training.

Normally, the facility security department is responsible for management of the security education program; however, security briefings and awareness training are often delegated to other facility organizations. At some sites, the initial and comprehensive briefings are presented by the site training department as part of the new-hire program. At large facilities, departmental coordinators or other individuals may provide security briefings for their assigned personnel. Another source useful in evaluating security education is the classification office. This function is usually performed by individuals in organizations outside the security department, and could be located within a number of facilities on site. These individuals might join with the security department to present classification briefings, which are often conducted in conjunction with security's comprehensive briefing.

Many sites must also include contractors, subcontractors, consultants, and access permittees in their safeguards and security awareness program.

Common Deficiencies/ Potential Concerns

Inadequate Documentation

Some facilities have not developed implementation plans and procedures reflecting all DOE requirements. Documents are often vague and incomplete, and fail to fix responsibilities for implementation of the program. If procedures, briefing materials, and attendance records are not in place, information for administering the program might not be readily available to supervisors and briefers, and consequently the program is likely to be deficient.

Inadequate Security Awareness

Security awareness programs that lack management support and that are given inadequate priority, guidance, or resources can result in inadequate security awareness levels of facility personnel, thereby placing DOE assets at risk.

In some cases, managers do not make good use of security awareness program communication channels in addressing security problems. By using security awareness channels, briefings and awareness media can maximize communication of security subjects.

Security Education Programs Not Established

Frequently, subcontractors and small prime contractor organizations choose not to establish security awareness programs, and their employees participate in the program of a large prime contractor. It is important that the prime contractors that conduct security awareness programs have procedures in place to ensure participation by their subcontractors. If contractor and subcontractor personnel who have access to classified matter or SNM do not receive the required security awareness briefings, and are not exposed to security awareness media, the probability of inadvertent disclosure of classified information increases.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to security awareness. Elements to cover include:

- Whether management and supervisory support are reflected in the security awareness documentation

- Appointment of a safeguards and security awareness coordinator

- Identification and location of organizations and individuals responsible for administering the program

- Whether security surveys are being conducted to ensure that contractors, subcontractors, consultants, and access permittees have security awareness programs

- Whether copies of materials produced to support local safeguards and security awareness programs are periodically provided to the Director of Safeguards and Security for evaluation

- Operations Office surveys that include inspection of security awareness (if available, were findings identified and corrected?)

- Approved or pending exceptions to DOE requirements

- Facility self-assessments of security awareness education (if available, arrange to review the self-assessment reports and corrective action plans during the inspection).

Data Collection Activities

Security Awareness Documentation

A. Inspectors should examine policies and procedures to determine whether a structured security awareness program has been implemented, adequate records are kept, and whether instructional materials are received and updated by a responsible individual. Records should be examined to determine whether they are current and complete, and whether they reflect briefings by type, date, and individuals attending the briefing. Record-keeping systems must be capable of providing an audit trail.

B. Security personnel should be interviewed to determine the adequacy of security education documentation and training materials. A lack of adequate information, lesson plans, or instructional aids could indicate inadequate management support or budget constraints. If problems exist, inspectors should attempt to determine their causes.

C. Inspectors should determine whether a security education and awareness coordinator has been appointed, and whether there is adequate guidance on the conduct of briefings (including initial, comprehensive, refresher, foreign travel, and termination).

Security Education and Awareness Levels

D. Inspectors should interview employees to determine their knowledge of the subjects contained in the security awareness program and whether they recall information provided in the briefings and media. Opinions and perceptions should be solicited to determine whether security awareness education is effective and receiving support.

E. Inspectors should interview managers and supervisors to determine how well security awareness education supports their organizations, and whether the program addresses their vital areas of concern. It might be helpful to determine when a security issue was last discussed during a manager's meeting, whether security-related topics are frequently discussed, and when a manager last attended a security education refresher briefing. Determining the level of management support for the program requires the inspector to exercise professional judgment; detailed discussions with management may be necessary if inspectors perceive that there is inadequate support for the program.

F. Inspectors should determine whether the number of security infractions and violations is unusually high. If it is, inspectors should carefully analyze available information to determine whether it results from a lack of security awareness training, or whether awareness training has intensified employee participation in detecting and reporting security infractions and violations.

Security Education for Contractor Personnel

G. Inspectors should determine by interviews and document reviews whether the Operations Office has made any special provisions or delegation of authority for oversight of contractor and subcontractor security awareness education.

H. If contractors, subcontractors, consultants, or access permittees have established their own security awareness education programs, inspectors should determine by interview and document review whether the site office supports their programs through guidance, instructional materials, and frequent visits.

This page is intentionally left blank.

Section 4.2

Security Education and Awareness Briefings

Contents

References 4-7
General Information 4-7
Common Deficiencies/Potential Concerns 4-8
Planning Activities 4-10
Data Collection Activities 4-11

References

DOE Order 470.1, Chapter IV

General Information

Security briefings are at the heart of the safeguards and security awareness program. The briefings include:

- **Initial security briefings** inform cleared and uncleared individuals of local security procedures and access control requirements, prior to their assuming duties. These briefings are the employees' introduction to security and set the tone for their understanding of security responsibilities and DOE facility requirements.

- **Comprehensive briefings** are designed to ensure that individuals who have been granted DOE security access authorizations are fully aware of their security responsibilities before they have access to classified information or SNM.

- **Refresher briefings** are conducted approximately every 12 months, and are intended to reinforce security policy for individuals who possess DOE access authorizations and have access to classified information or SNM. These refresher briefings serve as continuing education and a reminder to employees of their ongoing security responsibilities. They also serve as a tool in communicating new security information, changes in policy, and site-specific information affecting security procedures.

- **Foreign travel briefings** are required for all travelers who hold a DOE access authorization and are traveling to sensitive countries. These briefings are designed both for traveler safety and for the protection of national security information. They are normally informal, oral presentations, supported by country-specific handouts and visual aids. Upon return, travelers should be debriefed regarding any unusual occurrences during travel. It is difficult to ensure that all travelers receive the briefing, since the security organization becomes aware of foreign travel only when it is reported. Although DOE has no recognized program to ensure compliance, this topic should receive the same emphasis that other security briefings are given.

- **Termination briefings** are designed to remind individuals of their continuing security responsibilities when their access authorizations are terminated. These briefings provide the last opportunity to remind individuals of their continuing legal obligation to protect classified information and to report proposed travel to sensitive countries. The terminating individual should be made aware of the penalties for failure to safeguard classified information. The briefings are normally oral, informal presentations supported by videotapes and training aids, if available.

The content of each briefing is described in DOE Order 470.1, Chapter IV. In addition to the information required by the order, site-specific material is normally covered, including facility security requirements, recent security infractions, and current security problems.

Common Deficiencies/ Potential Concerns

Inadequate Documentation

Written implementation procedures, lesson plans, instructional aids, and training records reflect how the facility conducts its security education program. The presence and quality of these materials can indicate whether the program is effective. Without adequate documentation and instructional material, security awareness education is likely to provide little assurance that employees receive the required security information.

Some computer-based training programs fail to include safeguards that will assure that an individual has actually reviewed the material before being given credit for completion.

Lack of Qualified Instructors

Individuals with instructional skills are a valuable asset to the awareness program. Although it is sometimes difficult to acquire talented and enthusiastic instructors, a lack of proficient instructors can result in listless presentations that convey very little lasting information.

Inadequate Briefing Content and Instructional Material

In some cases, briefings do not address all subjects required by DOE Order 470.1, Chapter IV. Some sites use video presentations exclusively. Although some films and slide presentations look very professional, they are often outdated and lack the required subject matter and intent of the DOE order. Additionally, when videos are the only source of information, the interaction between instructor and student—so important in effectively conveying vital information and demonstrating management support—is lost.

At some sites, approved lesson plans, which incorporate all training objectives and ensure that trainees are provided with standard information, have not been revised or are not available.

It is usually more effective if presentations, especially during refresher briefings, are varied; include new material, examples, and anecdotes; and reflect the current security procedures and facility environment. Sites that use Web-based training may not have a program that assures an individual completes the required training before the individual is given credit for the training.

- **Initial briefing.** At many sites, a member of the employment department, or someone outside the security organization, gives initial briefings. For many new employees, this is their first exposure to a tightly controlled security environment. Therefore, it is important that the person conducting the briefing be thoroughly knowledgeable and capable of discussing all aspects of the security program.

  Deficiencies in the initial briefing can result in unauthorized personnel gaining access to classified information, vital areas, or SNM. Many new employees are uncleared when they are briefed. If such topics as escort duties, access control procedures, and facility classified areas are not presented properly, the results can degrade the overall security program.

- **Comprehensive briefing.** In some cases, the comprehensive briefing is combined with the initial briefing and given at the same time. This is not a violation of DOE policy, and no problem exists if the uncleared employees receive an access authorization within a short time. However, if a long period of time passes before the employees receive their access authorizations, they may forget vital information contained in the comprehensive briefing, and thus may not be fully aware of their security responsibilities when they finally have access to classified information or SNM.

At some sites, new employees are asked to sign Standard Form 312 during in-processing, before receiving the comprehensive briefing. This form is an agreement between the individual and the government certifying that the employee agrees to protect classified information. It should not be signed until the employee has received the comprehensive briefing and fully understands the agreement. The person authorized to accept the agreement on behalf of the government is usually a member of the security department. If this individual is not a federal employee, it is important that there be written authorization permitting this individual to sign the Standard Form 312 acceptance block.

- **Refresher briefing.** A common problem with the refresher briefing is that management does not ensure attendance by all cleared employees, including supervisors, subcontractors, and vendors. Without the support of site and contractor management, attendance at these briefings is usually poor.

  Also, security education and awareness coordinators do not always ensure that the refresher briefings contain all the subjects required by the DOE order. Often, the briefing focuses on a specific topic of collective interest, excluding required topics that may be considered common knowledge or less important. Since the refresher briefing is the most effective method of keeping employees current, it should be as complete as possible.

  Significant deficiencies in control and presentation of refresher briefings may indicate inadequate management attention or insufficient resources devoted to administering the refresher briefing program. Often, support is inadequate because of the significant cost, time, scheduling, and resources required to make the briefing a success, and to ensure that everyone receives the briefing.

- **Foreign travel briefings.** Some sites fail to maintain up-to-date travel advisories disseminated by the U.S. Department of State and other government agencies. Failure to maintain the current status of foreign country activity could jeopardize both travelers and sensitive information.

- **Termination briefings.** Terminating employees do not always sign their termination statements. In some cases, employees may skip the security activity when checking out, if they are not required to deliver their badges and sign the termination statement before receiving their final paycheck. Consultants and subcontractors may be located off site and may not check out at all. Cleared individuals on disability, students away at college, and offsite employees are often unavailable to sign termination statements or to receive the required termination briefings. It is important to have a system in place to track employee terminations, so that all cleared employees being terminated receive briefings. In those cases where the individual is not available or refuses to sign the termination statement, the records should be annotated and, when required, DOE notified of the situation.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents pertaining to security education. Elements to cover include:

- The organizations and individuals responsible for conducting the security briefings, and whether satellite organizations (that is, contractors, subcontractors, and vendors) conduct briefings for their employees and, if so, whether the site security education and awareness coordinator oversees their programs
- Topics covered during the briefings, how often they are conducted and the approximate number of people that attend the briefings
- When and where briefings are conducted (for example, during in-processing at the employment office, before receiving a badge at the badging facility, or before having access to classified information at the security department)
- Security awareness education budgets and budget requests, focusing on whether adequate resources are provided for security education
- How briefing completion is recorded (that is, attendance rosters, Standard Form 312, or other method) and where the records are maintained
- Whether subcontractors or vendors are included in the briefing program and, if so, how they receive the required briefings and who monitors the process.
- Operations Office surveys that include inspection of security education and briefing programs (if available, were survey findings identified and corrected?)
- Approved or pending exceptions to DOE requirements
- Facility self-assessments of security awareness education and briefing programs (if available, arrange to review the self-assessment reports and corrective action plans during the inspection)
- The facility may be asked to provide the following information for review during the planning meeting, or on site during the inspection:
- Documentation related to procedures and content of initial, comprehensive, refresher, termination, and foreign travel security briefings
- Samples of visual aids used for security education
- Identification of security education and awareness coordinators and trainers, with qualifications and security awareness education training each has received
- A printout listing access authorization grant dates of all employees
- A list of all comprehensive security briefing attendees for the past two calendar years
- A list of all refresher security briefing attendees for the past two calendar years
- A sample of documentation notifying employees of the requirement to attend specific briefings
- A list of personnel who have traveled to sensitive countries on official or unofficial travel during the past two calendar years and the foreign travel briefings they have received
- Documentation of any security incident reports for travelers during the past two calendar years.

Data Collection Activities

Documentation and Qualifications

A. Inspectors should review documentation on security awareness education implementation to ensure that all elements of the DOE order and other applicable directives are present.

B. Inspectors should review the qualifications of the security education and awareness coordinators and security specialists to determine whether they have knowledge of DOE orders, have writing and presentation skills, and are aware of security-related incidents and threats.

C. Inspectors should attend scheduled briefings (or ask appropriate personnel to provide a briefing for the inspectors) to evaluate the information covered, presentation style, briefing room environment, training aids, knowledge and enthusiasm of the instructor, and quality of handout material.

Initial Briefing

D. Inspectors should compare badging dates with initial briefing dates on a sample of 10 to 15 records to ensure that initial briefings were given before badges were issued. Typically, 10 to 15 records constitute a sufficient sample, although it may be prudent to review additional records if deficiencies are noted in the initial sample.

E. Inspectors should obtain a list of newly hired employees from the employment activity and interview selected persons on the list to determine whether they fully understand the security program, still have knowledge of material presented in the initial briefing, and have an opinion of the presentation. They should be asked whether they received any handout material during the presentation and, if so, whether it was useful.

F. Inspectors should attend an initial briefing and evaluate the effectiveness of instruction and course content. Lesson plans, visual aids, and handout materials should be examined to ensure that they adequately support the overall presentation. Question-and-answer sessions should be evaluated to determine the instructor’s ability to respond effectively.

Comprehensive Briefing

G. Inspectors should review a sample of 15 to 20 records to determine the interval between the date of the comprehensive briefing—the date Standard Form 312 was signed—and the date of notification that access authorization was granted.

H. Inspectors should determine whether individuals who sign the acceptance block on Standard Forms 312 are Federal employees or contractors. If they are contractors, inspectors should determine whether they have written authorization to accept the non-disclosure agreement on behalf of the government.

I. Inspectors should interview a sample of five to ten personnel who have recently completed the comprehensive briefing to determine whether site policies and procedures were explained adequately during the presentation and whether the information provided has been useful in their subsequent access to classified information. Inspectors should determine whether these individuals understand the purpose of the briefing and their responsibilities in protecting classified information.

Refresher Briefing

J. Inspectors should conduct interviews and review documents to determine the system for scheduling and presenting refresher briefings. The content of the refresher briefing is similar to that of the comprehensive briefing; however, subjects of common knowledge may be covered in less detail. Other subjects of primary concern, such as 10 CFR, Part 710, should be reviewed and expanded in refresher briefings.

K. Inspectors should review a sample of 15 to 20 records to determine the interval between the initial and refresher briefing. The same records that are reviewed to validate presentation of the comprehensive briefing may also be used to determine that refresher briefings are provided at least every 12 months, as required, and that attendance is documented. Typically, 15 to 20 records constitute a sufficient sample, although it may be prudent to review additional records if deficiencies are noted in the initial sample.

Foreign Travel Briefing

L. Inspectors should review DOE Form 1512.2, "Notification of Proposed Travel to Sensitive Countries," DOE Form 1512.3, "Security Analysis of Proposed Travel to Sensitive Countries," and DOE authorization letters to determine whether the forms were submitted in a timely manner, and whether the traveler departed only after receiving the appropriate approvals.

M. Briefing files should be reviewed to determine whether current information regarding travel advisories, public media, travel tips, and other data on foreign travel is available.

N. Inspectors should review a sample of DOE Form 1512.2, which is required by DOE Order 1500.3 to be retained by the cognizant security office. A sample of travelers to foreign countries should be interviewed to determine the effectiveness of the foreign travel briefings, and whether the travelers were briefed on requirements to report hostile contact. A review of briefing and debriefing records should verify that required actions were taken.

O. Inspectors should interview a sample of three to five employees who have traveled to foreign countries—a list of these employees can usually be obtained from the organization that processes visas—and ask whether they received the foreign travel briefing, and whether their travel was monitored. They should also be asked whether they understood the kinds of observations and activities that they should report upon their return. If deficiencies are noted, it may be prudent to interview additional travelers.

Termination Briefing

P. Inspectors should review termination briefing contents to ensure that they are comprehensive and factual, and that they meet the requirements of the order. Inspectors should determine whether procedures are in place to ensure that termination briefings are conducted and are effective, and that the briefing official verifies with each individual that all classified information and materials are returned to appropriate DOE authorities. Personnel access authorization files of recently terminated employees should be reviewed to determine the existence, completion, signatures, and dates recorded on the termination statement.

Q. If contractors are used, inspectors should contact their security activity or the subcontracting technical representative to determine whether security briefings are being given. Briefing materials should be examined for content. The contract should stipulate that security education briefings are required.

Section 4.3

Visual Aids for Security Education and Awareness

Contents

References 4-13
General Information 4-13
Common Deficiencies/Potential Concerns 4-13
Planning Activities 4-13
Data Collection Activities 4-14

References

DOE Order 470.1, Chapter IV

General Information

Visual aid programs are established and maintained to provide continuing reminders to employees of the need to protect classified information and of other security-related employee responsibilities. Visual aid programs are designed to strengthen employee security awareness between annual refresher briefings.

Recently, the quality of visual aids used in security awareness education has improved. Computer-based training, videotape presentations, slide shows, handouts developed by visual artists, and multicolored posters are frequently used within DOE.

Common Deficiencies/ Potential Concerns

A common problem with visual aids is that the quality of the aid obscures the content. It is important that visual aid content be presented prominently, that it be applicable to local security-related problems, that it support security briefings, and that it be consistent with DOE policies.

Some computer-based training programs fail to include safeguards that will assure that an individual has actually reviewed the material before being given credit for completion.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documentation on the facility’s methods of presentation. Elements to cover include:

- Identification of individuals responsible for obtaining, accounting for, distributing, and displaying visual aids at the facility
- The type and location of computer-based, video or film presentations used for security education
- Operations Office surveys that include inspection of visual aids (if available, were findings identified and corrected?)
- Approved or pending exceptions to DOE requirements
- Facility self-assessments of their visual aids program (if available, arrange to review the self-assessment reports during the inspection).

Data Collection Activities

Policies, Procedures, and Files

A. Inspectors should review computer-based training and visual aid program procedures to determine whether they are adequate and meet DOE standards. All programs should be reviewed for organization, effectiveness, and currency. For example, it is helpful to have a schedule or method in place for changing poster themes and for replacing posters at least every three months. Newsletter files should be examined to determine how often they are distributed, and whether their content is appropriate.

Visual Aids

B. Inspectors should examine computer-based visual aids (posters, videos, handouts, newsletters, and booklets) to determine whether they are current, support security awareness, and are consistent with briefing content and DOE policy. Posters should be checked to determine whether themes relate to security problems and agree with DOE policy. Inspectors should attend briefings to determine whether the visual aids are effective and support briefing content.

Section 4.4

Safeguards and Security Awareness Coordinator Training

Contents

References 4-15
General Information 4-15
Common Deficiencies/Potential Concerns 4-15
Planning Activities 4-15
Data Collection Activities 4-16

References

DOE Order 470.1, Chapter IV

General Information

Personnel selected as security education and awareness coordinators should have sufficient experience in DOE security systems to provide effective leadership in training security programs and to speak authoritatively on all subjects presented in security briefings. The instructional attributes of the briefer have a direct and significant impact on the quality of the site security education program.

At some sites, there may be several security education and awareness coordinators who conduct security education and awareness training at different facilities. Also, the security awareness education program may be delegated to contractor support personnel.

Common Deficiencies/ Potential Concerns

It is difficult to find security education and awareness coordinators who have the skills, experience, and qualifications listed in the DOE order. A good briefer might not have the security experience, and an experienced security person might not have the speaking, writing, editing, and audiovisual skills that go together to make a good briefer or that are required by DOE order. Inadequate training to overcome potential weaknesses can raise additional concerns and directly impact viability of the sites' safeguards and security awareness program.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents relating to the security education and awareness coordinators. Elements to cover include:

- Name, location, and qualifications of the security education and awareness coordinators
- General duties of the security education and awareness coordinators
- If the site has multiple facilities and several security education and awareness coordinators, how they interact and coordinate their activities
- Operations Office surveys that include inspection of security education and awareness coordinators (if available, were findings identified and corrected?)
- Approved or pending exceptions to DOE requirements

- Facility self-assessments of their security education and awareness coordinators (if available, arrange to review the self-assessment reports and corrective action plans during the inspection).

Data Collection Activities

A. Inspectors should determine the qualifications and performance of security education and awareness coordinators by interview and by attending briefings. It is desirable that the coordinators have DOE security experience and be able to speak authoritatively on subjects presented. Briefings that are well-organized and stimulating, with clearly defined objectives, are usually more effective in providing a high degree of awareness for the audience.

B. Inspectors should determine what training the security education and awareness coordinators have received, and whether opportunities for training have been denied. coordinators are required to attend DOE security education training workshops, as well as local training provided by DOE, other government agencies, or contractors.

Section 5

VISITOR CONTROL PROGRAM

CONTENTS

5.1 Classified Visits 5-3
5.2 Visits by Uncleared U.S. Citizens 5-7

The DOE visitor control program addresses security concerns raised by visits and technical exchanges by universities, private industry, other governmental agencies, and foreign governments. Visitors gain access on a daily basis to some of the nation’s most sensitive facilities engaged in various activities, from unclassified, non-sensitive energy research to the development and construction of nuclear weapons.

Visitors may be conducting unclassified work or working on classified projects with appropriate access authorization. For example, U.S. citizens may provide unclassified support services or technical expertise for a classified project; foreign nationals on an unclassified visit or on assignment at a sensitive facility pose a significant potential security risk and raise additional concern (see Section 7).

The DOE visitor control program provides policy guidance for the control and conduct of these visits.

Visitor access control procedures typically include issuing badges. A security badge or pass system is necessary 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. This is especially important as it pertains to visitors. 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. It is important that inspectors be aware of the facility procedures for issuing visitor badges prior to the site visit. Details on the overall subject of badges, passes, and credentials are found in the *Physical Security Systems Inspectors Guide* under the Entry and Search Control subtopic.

This page is intentionally left blank.

Section 5.1

Classified Visits

Contents

References 5-3
General Information 5-3
Common Deficiencies/Potential Concerns 5-3
Planning Activities 5-4
Data Collection Activities 5-4

References

DOE Order 470.1, Chapter VIII
DOE Order 5610.2

General Information

DOE Order 470.1, Chapter VIII, provides procedures for visits to DOE sites by cleared DOE and contractor personnel, and employees and contractors of other government agencies who often require access to classified material.

DOE's responsibility for controlling access to Restricted Data stems from the Atomic Energy Act of 1954, as amended, which places a responsibility on site employees to ensure strict adherence to the "need-to-know" provision. In addition, field organizations are responsible for implementing a visitor control system for facilities under their jurisdiction.

DOE Form 5631.20, "Request for Visit or Access Approval," is required for incoming and outgoing visits except for DOE employees and DOE contractor personnel who possess and present security badges issued by DOE Headquarters and Operations Offices (with access level annotated). Such personnel will be afforded admittance to Property Protection, Limited, and Protected Areas without the prior submission of a DOE Form 5631.20.

Access to Weapon Data is controlled through the Deputy Assistant Secretary for Military Applications (DP-21).

Common Deficiencies/ Potential Concerns

The most common problem with classified visits is the handling of DOE Form 5631.20, often referred to as a 277. If the form is incomplete or not submitted in a timely manner, the visitor may be delayed or unable to gain access to classified areas or information to accomplish assigned tasks.

In some cases, information limiting the visitor's access is not distributed to points of contact and escorts, thereby creating the potential for unauthorized access to classified areas and information specifically excluded on the DOE Form 5631.20.

With the elimination of the DOE Form 5631.20 for classified visits by DOE employees and DOE contractors in possession of security badges issued by Headquarters and DOE Operations Offices, verification of an individual's access authorization level and determination of "need-to-know" remain the responsibility of the individual or organization being visited prior to the release of classified information or granting access to special nuclear material. Inspectors must examine the process used to determine access authorization and "need-to-know" to assure that access is granted only when appropriate. If there is a reliance on a computer-generated access authorization listing (such as the CPCI), the currency and accuracy of that listing must be established.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents on the visitor control program and control of classified visits. Elements to cover include:

- Names and locations of individuals responsible for processing and controlling classified visits, including handling of DOE Form 5631.20, if required
- Names and locations of individuals responsible for issuing access badges to visitors
- General procedures for obtaining a visitor badge or temporary badge, and the procedures for recovering badges from visitors
- Approximate number of classified visits in a typical month or year (including a breakdown according to the areas of the site)
- Reports of Operations Office surveys that include inspection of the visitor control program and any corrective action plans
- Approved or pending exceptions to DOE requirements
- Reports of facility self-assessments of their visitor control program and any corrective action plans pertaining the to visitor control program.

Data Collection Activities

A. Inspectors should review procedures for the control of classified visits to determine consistency with DOE policy. It is important that procedures exist to assure adherence to the dates of the visit, level of access afforded, and areas of the facility to be visited. Particular attention should be directed toward procedures used to communicate the limitations of the visit (that is, the areas and levels of access) between the visitor control office and facility points of contact or escorts.

B. Inspectors should review a sample of 15 to 20 DOE Forms 5631.20 (when their use is required) to determine whether they contain adequate information and were submitted in time to allow the visited site to process the request. If deficiencies are noted, it may be prudent to review additional DOE Forms 5631.20.

C. Inspectors should review a sample of 10 to 15 classified visitor badge requests—lists of visitor badges issued or visitor logs—to ensure that visit requests (DOE Form 5631.20) were received for each badge requested. If deficiencies are noted, it may be prudent to review additional DOE Forms 5631.20.

D. 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. When the policies and procedures are used in conjunction with Headquarters or DOE Operations Office badges, inspectors should determine whether the desired access control is being achieved.

E. 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.

F. Through interviews with staff and personnel who are responsible for requesting visit authorizations, inspectors should determine whether the requirement for an effective “need-to-know” policy regarding National Security Information, Restricted Data, and Nuclear Weapon Data is fully understood and followed.

This page is intentionally left blank.

Section 5.2

Visits by Uncleared U.S. Citizens

Contents

References ... 5-7
General Information ... 5-7
Common Deficiencies/Potential Concerns ... 5-7
Planning Activities ... 5-8
Data Collection Activities ... 5-8

References

DOE Order 5632.1A
DOE Order 5632.6
DOE Order 5632.9

General Information

Uncleared U.S. citizens often visit DOE facilities in the normal conduct of business. Such visits may be by vendors, construction workers, applicants for employment, tour groups, university personnel, industry, and media representatives. It is DOE policy that these visits be controlled.

The visitor control program is designed to limit visitor access only to approved areas and information. The access control system and the visitor's escort ensures that visitors do not gain access to classified information or restricted areas. Effective access controls and trained, responsible escorts enhance the protection of DOE security interests.

Badges and passes for escorted visitors should bear the visitor's name, a serial number, period of visit, and indication on the face of the badge or pass that escort is required; badges that are not removed from the facility need show only a serial number and an indication on the face of the badge that an escort is required. DOE Order 5632.9 provides further guidance on badges and passes for unescorted visitors and construction workers.

Common Deficiencies/ Potential Concerns

Inadequate Visit Justification

A primary concern with unclassified visits by U.S. citizens is whether the visit is necessary to conduct DOE business; therefore, proper justification for the visit is required.

Inadequate Visitor Badging and Access Control System

Visitor badging and access control procedures may be inadequate to ensure that visitors gain access only to appropriate information and areas of the facility. Also, escorts sometimes are not fully aware of their responsibilities and visitor access restrictions.

Visitor Badge Recovery Not Consistently Effective

Recovery of badges issued to long-term visitors, student workers, and construction workers can be a particular problem since such persons do not always follow normal termination procedures when leaving the site. It is important that an effective system is in place to ensure that badges issued to all categories of visitors are recovered when no longer required.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documents on visits by uncleared U.S. citizens. Elements to cover include:

- names and locations of individuals responsible for processing, controlling, and approving visits of uncleared U.S. citizens
- names and locations of individuals responsible for issuing access badges to visitors
- general procedures for escorting uncleared personnel and how escort requirements are displayed on the badge
- the approximate number of visits during the past year by area
- procedures used to ensure that only approved information is provided and only authorized areas are visited
- reports of Operations Office surveys that include inspection of unclassified visits by U.S. citizens (if available) and whether findings were identified and corrected
- approved or pending exceptions to DOE requirements
- reports of self-assessments of the visitor control program.

Data Collection Activities

Access Control and Visit Justification Procedures

A. Inspectors should review visitor access control procedures to determine methods used to verify justification for visits, and whether uncleared visitor access is controlled and limited to only those areas for which access has been approved. Visitor badging records should be reviewed to determine whether uncleared visits were justified and properly approved.

B. Inspectors should review badge and 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.

Badge Recovery

C. Inspectors should review visitor logs and badge records and interview personnel in the badge office to determine whether uncleared 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.

Escort Procedures

D. Inspectors should review escort procedures to determine whether they are adequate and can be understood by individuals performing escort duties. Site personnel who have performed escort duties for uncleared U.S. citizens should be interviewed to determine whether they are fully aware of their escort responsibilities.

Section 6

HUMAN RELIABILITY PROGRAM

Contents

References 6-1
General Information 6-1
Common Deficiencies/Potential Concerns 6-2
Planning Activities 6-5
Data Collection Activities 6-5

References

10 CFR, Part 707
10 CFR, Part 709
10 CFR, Part 710
10 CFR, Part 712 (pending final rule)

General Information

Pursuant to the Atomic Energy Act of 1954, DOE owns, leases, operates, or supervises activities at facilities in various locations in the United States. Many of these facilities are involved in researching, testing, producing, disassembling, or transporting nuclear explosives, which, when combined with Department of Defense-provided delivery systems, become nuclear weapon systems. These facilities are also often involved in other activities that affect the national security.

DOE—and the nation—has the highest interest in protecting these facilities and activities from the potential misuse by employees or contractors who are believed to be unreliable because of mental or physical impairments or other problems or circumstances affecting their judgment. Therefore, the DOE seeks to protect the national interest from unacceptable damage by implementing an enhanced security and safety reliability program designed to assure that individuals occupying positions affording access to certain material, facilities, and programs meet the highest standards of reliability and trustworthiness.

The HRP is designed to meet this objective through a system of continuous evaluation that identifies those individuals whose judgment may be impaired by physical and/or emotional problems, the use of controlled substances, the use of alcohol, or any other condition or circumstance that may represent a reliability, safety, and/or security concern.

The HRP described in this guide reflects the current status of ongoing DOE rulemaking and DOE efforts to consolidate its two previous human reliability type programs into a single, integrated program. The new program is designed to incorporate applicable elements of both the personnel assurance, and personnel security assurance programs, and to expand the program to include additional sensitive job positions. Since this transition is in process, materials for this section have been taken from the most current proposed draft rule (Version 20). Inspectors should refer to existing guidance prior to planning and conducting inspection activities.

The Human Reliability Program

The HRP is a continuous evaluation program. The HRP applies to all applicants for, or current employees of, DOE or a DOE contractor or subcontractor, in a position defined or designated under 10 CFR, Part 712 as an HRP position.

HRP certification is required for each individual assigned to, or applying for, a position that:

(1) Affords unescorted access to a Category I SNM or has responsibility for transportation or protection of Category I quantities of SNM;

(2) Involves working with, protecting, or transporting nuclear explosives, nuclear devices, or selected components;

(3) Affords access to information concerning vulnerabilities in protective systems when transporting nuclear explosives, nuclear devices, selected components, or Category I quantities of SNM;

(4) Has responsibility for control and accountability of Category I quantities of SNM;

(5) Affords access to classified computer systems that would allow downloading and transferring of unclassified information from a classified system;

(6) Has the potential for causing an incident that could result in a nuclear explosive detonation, a major environmental release from a nuclear material production reactor, or an interruption of nuclear explosive production with a significant impact on national security; or

(7) Affords the potential to significantly impact national security that is not included in (1) through (6) of this section and is approved by the Director, Office of Safeguards and Security;

The purpose of the HRP is to ensure that these individuals meet the highest standards of reliability. The objective is to identify individuals whose judgment may be impaired by physical or psychological disorders, use of controlled substances, or habitual excessive use of alcohol.

Evaluation to determine suitability for assignment to HRP is accomplished through initial assessment and recurring annual assessments consisting of:

- supervisory review
- medical assessment (to include psychological evaluations)
- management evaluation (to include drug testing, alcohol testing, occurrence testing, testing for reasonable suspicion, and counter-intelligence polygraph examination)
- DOE security review.

An individual in the HRP must have a "Q" access authorization, which includes an initial investigation and a reinvestigation every five years.

Personnel enrolled in HRP are continuously evaluated for signs of aberrant behavior. Training in observation of aberrant behavior is provided to HRP supervisors and employees to assure that individuals in the HRP are aware of behavior that may indicate a security concern. Other employees and supervisors are responsible for reporting all signs of aberrant behavior.

Alcohol testing for contractor employees will be based, like drug testing, on the provisions of 10 CFR 707, "Workplace Substance Abuse Programs at DOE Sites." DOE Order 343.2 addresses drug testing of Federal employees. Alcohol testing will be random, for occurrence, and for reasonable suspicion. The testing method will normally be by breath analysis.

Common Deficiencies/ Potential Concerns

Inadequate Communication Between Security Organizations and HRP Administrators

Communication and coordination between nuclear explosive safety and security organizations can ensure that security concerns are appropriately incorporated in the implementation of the HRP. When communication or coordination is lacking, and the HRP is being used to mitigate the insider threat or otherwise supplement the overall protection program, the security-related functions may be ineffectively implemented and create potentially significant vulnerabilities.

Inadequate HRP Security Review

An annual security review for personnel in the HRP consists of a review of the DOE personnel security file by personnel security specialists. It is important that these files be reviewed to determine whether any security issues are present that need resolution and equally important how those issues impact HRP duties. A formal process must exist whereby security and HRP concerns are recognized and addressed to reach resolution and/or determination as to further action.

Unidentified HRP Positions

In some cases, positions may not have been identified as HRP positions, as defined by 10 CFR, Part 712. This may result from the lack of a systematic method for identifying HRP positions. Also, some positions that have been designated by the site's HRP certifying official may not seem appropriate as defined by DOE policy.

However, because of the wide differences in the programs at various DOE facilities, the Operations Offices were given considerable discretion in implementing the program, and the facility's interpretation of information available on the HRP should be carefully examined and given every consideration. Of the seven categories of HRP positions identified in 10 CFR, Part 712, category (7) is more general in that it defines the positions as those that have the potential for causing unacceptable damage to national security, but that are not included in category 1 through 7. The positions require the approval of the Director of Safeguards and Security. To avoid these steps, Operations Offices may ignore the category (7) designation and consequently ignore the intent of the rule.

A potential problem may exist when an HRP position is vacated, then temporarily filled by a person who does not meet HRP requirements.

Unassigned HRP Responsibilities

Sometimes, facilities fail to assign, or properly document the assignment of, responsibilities to organizations and persons for various aspects of the HRP. This inevitably results in some elements of the program being partially implemented or not being implemented at all. A method that has been found to be effective is to have responsibility for every aspect of the program specifically assigned in writing, first to an organization and then to a specific position within that organization.

Incomplete HRP Implementation

The HRP may not be fully implemented at some DOE facilities. In such cases, an implementation plan and appropriate guidance must be in place and must have the approval of the DOE Operations Office, with a subsequent review by OSS.

Frequently, if the HRP has not been fully implemented, an implementation schedule has been prepared. If so, inspectors should determine whether the facility is adhering to that schedule and if effective compensatory protection measures are in place.

Inspectors may find that some facilities have not been provided the resources to fully implement the HRP. Such cases may need to be referred for management attention.

Inadequate HRP Drug Testing Program

For a variety of reasons, many sites have not implemented the required HRP drug testing program. In some cases, sites are using established drug testing programs that are in place to meet non-HRP requirements (company policy, drug-free Federal workplace, etc.) to meet the requirements of the HRP. These programs must be examined to determine whether their elements meet HRP requirements.

In carrying out the drug testing program, facilities may not have adequate procedures and materials to provide for tamper-proof, sealed protection of sample specimens or for a continuous chain of custody with individual responsibility from the time the specimen is taken to the completion of laboratory analysis.

Some sites' medical facilities are not adequately staffed to accomplish the testing, medical, and psychological evaluations required. In some cases, only a "medical" examination is performed to fulfill the annual requirement. When a psychological evaluation is performed, the examination may be performed by medical personnel who are not fully qualified to determine the psychological condition of the individual.

The facility may not have enough medical staff to perform adequate testing and evaluations "for cause" and as required for the return to duty from sick leave of HRP personnel. Insufficient medical staff may also delay required annual medical assessments and random drug testing.

Inconsistent or Inadequate HRP Alcohol Testing

Individuals in, or applying for, an HRP position are examined for habitual, excessive use of alcohol. When alcohol abuse is suspected, individuals are examined for evidence of alcohol abuse; when questionable, further evaluation is required, which may include psychological assessment.

Once in the HRP, individuals are required to be examined for habitual, excessive use of alcohol as part of the annual medical assessment. In the HRP, an evaluation is required whenever alcohol abuse is suspected. In addition, individuals in the HRP are prohibited from consuming alcohol within an eight-hour period preceding any tour of work and during the period of work. To assure this, management is required to develop procedures to ensure that persons called in to perform an unscheduled working tour are fit to perform the task assigned.

Inadequate HRP Training Program

Training is one of the most important ingredients in a successful HRP. Persons in HRP positions must fully understand their program responsibilities, and supervisors must be trained to identify aberrant behavior and to take appropriate action. However, at some facilities, only selected personnel have been trained, and first-line supervisors and HRP personnel do not fully understand their responsibilities and therefore may be reluctant to report aberrant behavior of fellow workers.

Improperly Conducted HRP Reviews, Assessments, and Evaluations

If managers, supervisors, and medical and security personnel do not conduct their reviews in a thorough and responsible manner, the provisions of the HRP will become less effective. In such cases, the evaluation process may become reactive rather than proactive.

Inadequate System for Maintaining HRP Data

Some facilities lack a system for maintaining appropriate data on HRP positions, such as evaluations, enrollment records, records of aberrant behavior, justification for identified HRP positions, and records of training received. Such data should be readily available to those responsible for administering the programs.

It is especially important to have a mechanism for ensuring that all vacated HRP positions are filled in a timely manner, and that the appropriate supervisor or coordinator is notified when a position becomes vacant.

Inadequate Reporting of HRP Concerns

In that the HRP is a combined nuclear safety and security program, a concern identified by a site's HRP medical official may be strictly a safety concern and not a security concern and thus, not be reported to the DOE HRP certifying official. In some instances, the concern may overlap and there could exist a security concern that might go unreported to security management.

Planning Activities

During the planning meeting, inspectors should interview points of contact and review available documentation on the HRP. Elements to cover include:

- a review of the site's HRP implementation plan

- the status of the facility HRP program, including a review of all current HRP positions, how long personnel have been in these positions, all positions to be designated under the HRP at a later date, and the implementation schedule for designating these additional HRP positions

- individuals responsible for administering the programs and their location at the facility

- location and content of files maintained on the HRP

- whether the facility has a drug testing program, and, if so, what type of chain of custody procedures, unannounced drug testing procedures, and materials required to effectively conduct the tests are in place; also, whether other drug testing programs are being used for the HRP, and, if so, whether they meet the requirements

- whether training materials are present (including instructor guides and student handouts), and whether a training program is in place for instructors, managers, supervisors, and HRP personnel

- whether managers, supervisors, and HRP personnel receive awareness training in the recognition of aberrant behavior

- whether required reviews are being conducted by managers, supervisors, medical personnel, and security specialists, and where the copies of these reviews are kept

- whether Operations Office surveys or program reviews that include inspection of the programs are available for review, and, if so, whether the findings were identified and corrected

- whether the facility has any approved or pending exceptions to DOE requirements

- whether the facility has performed any self-assessments of its HRP (if so, arrange to review the self-assessment report during the inspection).

Data Collection Activities

HRP Plans, Policies, and Procedures

A. Inspectors should review the site implementation plans and other policies and procedures to determine whether the programs have been fully implemented and positions have been properly identified. If an implementation schedule has been prepared, it should be reviewed to ensure that it is complete, realistic, and being followed. Individuals involved in implementing and maintaining the program should be interviewed to determine their scope, status, and effectiveness.

B. Inspectors should review site plans, policies, and procedures to confirm that they provide for drug testing, supervisory reviews, medical assessments, management evaluations, security reviews, approval authority notification procedures, reassignment and termination procedures, and an effective program for maintaining appropriate data on HRP positions and "Q" cleared employees.

HRP Training Program

C. Inspectors should review training records to determine whether they are complete and adequately maintained. Inspectors should interview managers, supervisors, and HRP personnel to determine whether they have received training and are aware of their responsibilities, especially in reporting unusual conduct.

D. Inspectors should determine whether training materials are sufficient for the training staff and for the training of all personnel involved with the program. If possible, the inspector should attend a training session to determine the effectiveness of training.

HRP Drug/Alcohol Testing Program

E. Inspectors should review drug and alcohol testing procedures and inspect the material used to conduct the tests. It may be helpful to have individuals responsible for conducting drug/ alcohol testing explain the process step by step. Inspectors should review procedures for handling specimens to determine whether an effective chain of custody is maintained and review the administering of the breath alcohol test.

F. Inspectors should interview individuals who have recently been tested. Ask them to describe the procedures that were used during the test to determine whether policy and procedures match actual practice. Review the selection process for random testing to determine whether it is, in fact, conducted on a random basis and review the procedures for alcohol testing when individuals are called in for unscheduled work.

G. Inspectors should review the drug/alcohol testing records to determine whether all HRP employees have received a drug/alcohol test and whether the random testing program has been implemented as described. If some employees have not been tested, determine why they were excluded.

HRP Reviews and Evaluations

H. Inspectors should interview supervisors, medical personnel, personnel security specialists, the HRP certifying official, and individuals in HRP positions to determine whether the required reviews are being conducted, and whether personnel fully understand their responsibilities.

I. Inspectors should examine the HRP evaluations to determine whether all parts have been completed, including supervisory review, medical assessment, and management evaluation. Inspectors should also verify that each individual assigned to an HRP position has completed an updated Questionnaire for Sensitive Positions, Part II on an annual basis (normally part of the supervisory review), and that the forms are submitted in a timely manner.

J. Inspectors should ask to examine any reports of unusual conduct or aberrant behavior to determine who made the report, how it was recorded, and what action was taken.

Maintaining HRP Records and Files

K. Inspectors should examine the system in place for maintaining HRP records. It is important that inspectors verify that the information contained in the files is pertinent to the program, is timely, accurate, and structured and maintained to allow an audit trail of events and actions.

Reporting Requirements

L. Inspectors should determine that a full understanding exists between the site's HRP medical officials, the Operations Office, and Personnel Security organization as to what is a reportable HRP concern.

Performance Tests

M. Inspectors should conduct a performance test(s) of the HRP elements, such as:

- Use an adulterated urine specimen to test the site medical staff's alertness in recognition of an unacceptable specimen
- Test an HRP individual's actions upon notification that he/she is to report for a drug test
- Use an HRP participant to report a security concern and observe actions taken by DOE to address the concern
- Quiz HRP supervisors and employees as to their recognition of aberrant behavior
- Test to see that individuals removed from HRP duties do not enter HRP required areas (either alone or under escort) and do not continue to perform HRP duties while on restriction.

This page is intentionally left blank.

Section 7

Unclassified Visits and Assignments by Foreign Nationals

Contents

References 7-1
General Information 7-1
Common Deficiencies/Potential Concerns 7-1
Planning Activities 7-2
Data Collection Activities 7-3

References

DOE Notice 142.1, July 14, 1999
DOE Notice 205.2 "Foreign National Access to DOE Cyber Systems," November 1, 1999.
"Additional Guidance on Close and Continuing Contact Reporting Requirements," Edward J. Curran, Director, Office of Counterintelligence, All Program Offices, August 17, 1999.

General Information

In the conduct of DOE operations, DOE and contractor facilities often host unclassified visits and assignments by foreign nationals. DOE Policy 142.1 provides DOE policy regarding these visits and assignments. DOE security policy is generally found in the 470 series of orders; however, policy is occasionally coordinated with other elements in the Department. DOE Notice 142.1 is the responsibility of the Office of the Secretary, which develops and prescribes policy and in some instances approves visits/assignments in coordination with heads of other departmental elements.

Each site must meet the reporting and record-keeping requirements of DOE Notice 142.1. The reporting system is to be an integrated part of the approval process and reporting information is to be provided to DOE Headquarters to support Departmental needs.

Common Deficiencies/ Potential Concerns

Inadequate Notice

Previous inspections have shown that visits are frequently requested with less than the required advance notice. In such cases, necessary actions (that is, indices checks with other government agencies, OPSEC working group reviews, classification, effort control, counterintelligence for the conduct of indices checks, and security planning) are not given appropriate consideration, and may not be completed at all.

Inadequate Security Planning for Visits

"Generic" security plans that are used for all visits and assignments that do not require access to a security area or a sensitive subject may not address specific access requirements for each visit, thereby setting the stage for possible compromise of DOE security interests. Security planning is more effective when the unique access requirements of each visit are addressed separately. "Specific" security plans are required for all visits/assignments to security areas, access to a sensitive subject, or access to any DOE site or facility by a foreign national from a sensitive country.

Inadequate Communications

Ineffective communications between the various site organizations often leads to a lack of control and oversight of foreign nationals. Inappropriate issuance, control and retrieval of badges; changes in security areas and their sensitive contents; and poor computer access controls all have a direct and significant impact on the effectiveness of the foreign visitor and assignment program. Non-existent, vague and conflicting policy guidance can further undermine an effective program. In some cases, new guidance has not been promulgated and implemented promptly to ensure that identified weaknesses are corrected expeditiously. In addition, site plans related to control of foreign visitors/assignees sometimes lack sufficient detail to ensure that they can be implemented.

Deterioration of Escort Procedures

Vigilance in escorting foreign nationals, especially long-term assignees, may decline as escorts become familiar with the assignee. It is important that procedures are in place to ensure that escorts are continuously reminded of their responsibilities. Foreign nationals on long-term assignment in laboratory environments may have their own work stations and computer networks, which could allow them to compromise DOE security interests. Security awareness on the part of hosts and escorts and other individuals in the facility must be maintained.

Inadequate Host Actions

Inspection experience has shown that hosts are often not fully knowledgeable of applicable requirements and their responsibilities. Hosts often do not adequately report changes to approvals and plans relative to a visitor's physical location, duties, and approved subject matter. Changes in assigned escorts are often not reported by hosts. Hosts reports are often submitted late, incomplete, or not at all. Without the timely submission of a complete host report, records on visits and assignments cannot be properly analyzed and information so derived used to strengthen the program.

Some sites may not have established a record system that meets the needs of required reporting to DOE Headquarters, or their system may lack all required data.

Inadequate Computer Access Controls

Determining the implications of allowing foreign visitors and assignees access to computer systems is a matter for review by the cyber security team. However, visitor and assignment requests and security plans may not identify which computer systems the visitor or assignee will be permitted to access. A particular problem occurs with foreign personnel who are provided access to computer networks but who are not stationed on site and thus may not be subjected to indices checks and other such measures. Personnel security inspectors reviewing the foreign visits and assignments program should ensure that requests and required security plans have been reviewed by the site cyber security organization. Changes in computer access should also be reviewed to ensure coordination with cyber security.

Planning Activities

During the planning meeting, inspectors interview points of contact and review documentation on unclassified visits and assignments by foreign nationals. Elements to cover include:

- general procedures involved in processing visits and assignments by foreign nationals

- identification and location of individuals responsible for security planning, preparing host reports, and processing unclassified visits and assignments by foreign nationals

- names and locations of individuals responsible for issuing access badges to foreign nationals

- general procedures for escorting foreign nationals and review of procedures for issuance of foreign national badges

- review of escort procedures unique to the site, and identification of all facilities on the site involved in providing escorts for foreign nationals

- approximate number of visits and assignments by foreign nationals during the past year, including areas visited

- reports of Operations Office surveys that include inspection of visits and assignments by foreign nationals, and whether findings were identified and corrected

- approved or pending exceptions to DOE requirements

- reports of self-assessments performed by the facility and correlative action plans.

Data Collection Activities

Plans and Procedures

A. Inspectors should determine if the site has a comprehensive and integrated approach to foreign visits and assignments. This would include review of a sample of specific and generic security plans to determine whether the elements required by DOE Notice 142.1 are covered. A sample of five to ten visit requests should be examined to determine whether they are timely and complete, and have the appropriate level of approval. If deficiencies are noted, it may be prudent to review additional visit requests.

Determination should be made that individual and organizational roles and responsibilities are clearly understood and that an integrated approach exists to assessing the risks to classified and sensitive information the visit or assignment poses. This approach should include identifying the location of classified and sensitive assets, assessment of current security measures, and development of additional protective measures to mitigate the risks.

Inspectors should ensure an appropriately detail plan has been developed which incorporates all required security considerations and administrative processing requirements. Special attention should be given to ensuring that required indices checks, agency coordination and the appropriate security plan have been completed prior to granting approval for the visit or assignment.

Escort Procedures

B. Inspectors should examine escort procedures to determine whether they are adequate and provide the information necessary to promote a high degree of security awareness on the part of escorts and hosts. Additionally, escorts should be interviewed to determine their adherence to program requirements.

Indices Checks

C. Inspectors should review a sample of five to ten indices checks to determine if the results of the checks were forwarded to the requesting Operations Office. Inspectors should determine whether appropriate consideration was given to potentially derogatory information. If deficiencies are noted, it may be prudent to review additional indices checks.

Coordination

D. Inspectors should interview site OPSEC, Counterintelligence, Classification, and Export Control personnel to determine the existence of and effective and integrated approach to assess risks to classified and sensitive prior to approval of the visit or assignment. Inspectors should also determine whether the results of the coordination are included in the security plans.

Host Reports

E. Inspectors should review a sample of five to ten host reports to determine whether they were timely, complete, and forwarded to the appropriate distribution as required. Interview four or five individuals who acted as hosts for sensitive country visitors. Determine each host's knowledge of the specific security plan and the responsibilities pertaining to the visit, as well as each host's input to the host report. If deficiencies are noted, it may be prudent to review additional host reports.

Security Plan Data

F. Inspectors should determine if a current assignment(s) is in effect at the time of the inspection. If so, they should select an assignment(s) and conduct a walk-through of the security plan to determine its accuracy and completeness, interview the host and escorts and other personnel in the area of the assignee's workstation, and review access control procedures into the security area.

Areas with Classified/ Sensitive Data

G. Inspectors should coordinate with the classified matter protection and control (CMPC) inspection team to determine where classified and/or sensitive material/matter is housed at the site and compare this information with areas where foreign nationals are allowed to visit or are assigned. Effort should be taken to assure that security plans recognize the existence of classified and/or sensitive material in, near, or adjacent to foreign nationals and that appropriate protection is afforded.

Non-Compliance

H. Inspectors should review all incidents involving a foreign national visitor/assignee and determine actions taken by the site to identify cause and to assign consequences.

Performance Tests

I. Inspectors should conduct a performance test(s) of the Unclassified Foreign Visits and Assignments elements, such as:

- Using a fabricated site foreign national badge to gain access to unauthorized areas

- Wearing a fabricated site foreign badge and carrying a clearly marked envelope with classification markings, walk a hallway in the area of a foreign national approved assignment to test recognition and actions taken by area workers.

Section 8

INTERFACES

Contents

Integration 8-1
Integration by the Personnel Security Topic Team 8-2
Survey Program 8-2
Protection Program Management 8-2
Operations Security and Cyber Security 8-2
Classified Matter Protection and Control 8-3
Physical Security Systems 8-3
Protective Force 8-3

Integration

Integration is the coordination and interface among inspection teams designed to achieve a more effective and organized inspection effort. This includes an enhanced knowledge of the inspected site, current inspection techniques, and the overall goals of the assessment.

Integration is possibly the most important and productive of the inspection activities. Thorough integration creates a synergism that stimulates the inspection process and enhances the quality and validity of the OA-10 inspection report. This combines with other unique attributes to strengthen the overall OA-10 capacity to provide significant value-added contributions to the safeguards and security community as well as to the DOE as a whole.

The integration process between topic teams must continue throughout all inspection phases to ensure that all pertinent inspection data has been shared. This integration, facilitated by one or more integration teams, is simply an exchange of information and an accompanying discussion regarding how information developed by one topic team influences the actions and information developed by other topic teams. This information should be included with other data considered during analysis.

There are several major objectives of integration. First, it allows topic teams to align their efforts so that their activities complement rather than detract from one another. It would be non-productive to inspect physical security systems at one location, control of classified documents and material at a different, remote location, and personnel security at yet another location. Therefore, topic teams must cooperate to make the best choices regarding what should be inspected at which locations. Early and continuing integration help ensure that the activities of all topic teams are unified and contribute to the overall goal.

A second objective of integration is to allow topic teams to benefit from the knowledge, experience, and efforts of other topic teams. The personnel security topic team may request other topic teams to provide information on personnel security subjects during data collection activities. For example, if Security Education and Awareness Coordinators are located in multiple facilities on the site, other inspection teams can help by interviewing these individuals and supplying information to the personnel security topic team. Also, inspection teams from all other topic areas can be asked to check for, and report on, visual aids used in areas that the personnel security team would not normally visit. Sometimes ideas from one topic team can help another topic team focus inspection activities in a more productive and meaningful direction.

The third reason for integration is to prevent topic teams from interfering with each other. Often, several topic teams concentrate their activities at the same location, resulting in multiple visits over time or a number of visits at the same time. This causes undue disruption at the inspected facility. Integration among topic teams can preclude this problem by having one or two topic teams visit a particular location and collect data for several teams. All topic teams should be aware of what the other topic teams are doing, where they are doing it, and how it will affect their own activities.

Integration by the Personnel Security Topic Team

The personnel security program is an important part of the overall security system at a facility, especially in the areas of unclassified visits and assignments by foreign nationals, security education, visitor control, and personnel access authorizations. If the facility has an HRP, individuals in the program will require frequent evaluations to ensure that they meet the highest standards of reliability. For these reasons, the personnel security topic should not be inspected in total isolation. Inspection activities must acknowledge and reflect this interaction to determine how well the required interfaces are accomplished. This requires integration with inspection teams responsible for other areas. Information developed by the personnel security topic team may have some impact on how the results of inspection activities in other topics are viewed. Similarly, results in other topical areas may have some bearing on how the effectiveness of the personnel security program is viewed.

Survey Program

The survey program topic team may be able to provide data relative to the status of survey coverage of the personnel security program conducted by the inspected site's security organization. In addition, data relative to terminated facilities and/or interests at contractor facilities can be provided by the survey topic team to assist the personnel security topic team in its review of access authorizations.

Protection Program Management

The personnel security topic team often interfaces with the protection program management (PPM) topic team to coordinate management interviews and discuss the involvement of site management in determining and obtaining necessary resources in support of the personnel security program. The PPM topic team normally interviews senior managers and supervisors and may be able to ask specific questions about personnel security, to include management's involvement in reduction and justification of access authorizations; the role of personnel security in the overall protection strategy; and, where an HRP is in place, management's involvement in determining the impact of an HRP on the threat. The PPM team may be able to provide information on the contractor's employment policies and practices, and whether the budget process adequately considers personnel security and HRP requirements. Interviews may include members of both topic teams, thereby limiting the impact on site manager time.

Operations Security and Cyber Security

At many sites, security education programs incorporate OPSEC, cyber security, COMSEC, and other security components into their awareness training. Inspection teams evaluating these areas can provide information on education effectiveness, thereby assisting in the overall evaluation of security education. Such assistance should be coordinated during the planning meeting.

The OPSEC topic team can review OPSEC working group meeting minutes and interview staff to determine whether foreign visitor or assignee issues are addressed.

The cyber security topic team can address foreign nationals' access to computer systems, especially networked systems.

Classified Matter Protection and Control

The control of classified documents and materials topic team can provide information relative to a site's administration of the security infraction program. The number and type of security infractions can be a measurement of the effectiveness of the safeguards and security awareness program. In addition, using infraction data, the personnel security topic team can assure that reports of infractions are filed in an individual's personnel security file and, when appropriate, considered in the determination of an individual's continued eligibility for access. Identified violations of the need-to-know principle and improper levels of access should be reported to the personnel security topic team. In addition, the location of classified and sensitive data on a site (as identified by the CMPC team) can be used to identify potential access to this data by foreign national visitors and assignees.

Physical Security Systems

Coordination with the physical security systems topic team can help determine whether access controls to security areas are adequate to ensure that uncleared visitors, and foreign visitors and assignees are permitted access only to approved areas.

Interaction with members of the systems topic team responsible for inspecting badges, passes, and credentials is of mutual benefit in determining whether unauthorized personnel can obtain access to classified matter.

If there is an inordinate number of cleared personnel whose jobs do not appear to require access authorizations (for example, food service personnel, subcontractors or vendors), it is possible that access controls, physical barriers, or redefined classified areas could reduce the need for access authorizations. The physical security systems topic team can help determine whether appropriate physical barriers are in place to control access to classified information and SNM. Careful planning is advised in redefining classified areas, since the end result may increase rather than decrease the need for access authorizations.

Inspectors should not evaluate the facility based on how they think it should be organized for security or for levels of access. Rather, they should determine whether the facility has followed DOE policies and procedures in implementing their security programs and justifying their levels of access.

Protective Force

The protective force topic team may be useful in assisting the personnel security topic team in evaluating the effectiveness of security education by observing employees entering and exiting security areas to determine whether they properly display badges, and whether they are familiar with contraband introduction requirements, access control procedures, and escort responsibilities. The protective force topic team can test systems in place to administratively deny or limit access of personnel whose access authorization eligibility is under review. Systems to alert protective force personnel to lost badges can also be tested. In addition, the protective force topic team should ensure that protective force post orders contain current and accurate information relative to foreign nationals in a particular area.

In the same manner, the personnel security team should be prepared and willing to provide assistance and support to other topic teams. Information developed on escort procedures may be valuable to security systems, cyber and CMPC topical areas.

This page is intentionally left blank.

Section 9

ANALYZING DATA AND INTERPRETING RESULTS

Contents

Introduction 9-1
Analysis of Results 9-1
Management 9-2
Access Authorizations 9-2
Security Education 9-3
Visitor Control 9-4
Unclassified Visits and Assignments by Foreign Nationals 9-4
Human Reliability Program 9-4
Consideration of Integrated Security Management Concepts 9-4

Introduction

This section provides guidelines to help inspectors analyze data and interpret the results. The guidelines include information on the analysis process and information on the significance of potential deficiencies, as well as suggestions for additional activities that may be appropriate if deficiencies are identified.

When analyzing the data collected on a particular aspect of the site security system, it is important to consider both the individual facets that comprise the security system and the system as a whole. In other words, just because a single facet of security has failed does not mean the security system failed. One must analyze the failure in terms of the entire security system. If this analysis determines that the security system would, despite the failure, have maintained a secure environment, then the overall system must be considered basically sound. Conversely, if the failure is in an area that would result in an insecure environment, then the security system must be considered ineffective.

Analysis of Results

The analysis process involves the critical consideration by topic team members of all inspection results, particularly identified strengths, weaknesses, and deficiencies. Analysis will lead to a logical, supportable conclusion regarding how well the personnel security program is meeting the required standards and satisfying the intent of DOE policy. If more than one subtopic has been inspected, a workable approach is to first analyze each subtopic individually. Then, the results of the individual analyses can be integrated to determine: 1) the effects of subtopics on each other, if subtopics are to be rated separately; or 2) the overall status of the topic, if a single topic rating is to be given.

If there are no deficiencies, the analysis is relatively simple. If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, the analysis must consider the importance and impact of those conditions. Deficiencies must be analyzed both individually and in concert with other deficiencies, and balanced against any strengths and mitigating factors to determine their overall impact on the program’s ability to meet the required standards. Factors that should be considered during analysis include:

- whether the deficiency is isolated or systemic

- whether the responsible individuals previously knew of the deficiency, and what action was taken
- the importance or significance of the standard affected by the deficiency
- mitigating factors, such as the effectiveness of other protection elements that may compensate for the deficiency
- the deficiency's actual or potential effect on mission performance or accomplishment
- the magnitude and significance of the actual or potential vulnerability to DOE security interests resulting from the deficiency.

The analysis must result in conclusions concerning the degree to which the personnel security program meets the required standards and the resulting effect on the ability of the personnel security program to accomplish its mission.

Management

Insufficient staff assigned to process access authorizations can significantly affect the entire Personnel Security Program and most frequently is a problem that must be addressed by management. To interpret the results of the Personnel Security Resources subtopic, the inspector must consider the results of the inspection of other personnel security subtopics. Deficiencies, such as a lack of timely submission of QNSPs, a backlog of reinvestigations, or late or incorrect CPCI data entries, can indicate insufficient resources, insufficient training, or ineffective utilization of existing resources.

Training for personnel who administer and maintain the personnel security program is one of the most important aspects of the program. Experience has shown that most deficiencies identified during past inspections can be attributed to inadequate or non-existent training programs.

When inspectors discover a number of deficiencies in most or all of the personnel security subtopic areas, it is important to attempt to determine the root cause of these deficiencies. This effort may identify a number of systemic problems, and it is likely in such cases that management support is lacking for the overall personnel security program.

Access Authorizations

Requests for access authorization are certified at the DOE office or contractor facility (that is, certified to ensure that the duties of a position require access to classified information or to SNM). The key elements in the processing of a request are: 1) certifying the request, 2) ensuring that the level of access is appropriate, and 3) ensuring that the access authorization is terminated when the need for it no longer exists.

If the position requires access to classified information or to SNM, it is important that the level of access is consistent with the work performed (for example, an individual may not need a "Q" access authorization if the position only requires access to Secret information). Deficiencies in determining levels of access are often the result of inadequate training, insufficient personnel, or an inadequate system for properly reviewing access authorization requests. These deficiencies can result in inappropriate or unjustified requests being submitted for processing, thereby wasting time and money. Also, a lack of control and scrutiny may result in an inordinate number of access authorizations on the facility, thereby increasing the possibility that unauthorized individuals will gain access to classified information or SNM.

Because the access authorization process is a costly, resource-intensive effort, significant deficiencies in handling initial requests for access authorization may indicate a lack of appropriate management support. It is important that an effective system be in place to ensure that the initial request and level of access are carefully reviewed before the request is processed further.

A contractor prescreening program that does not assure proper completion of all paperwork submitted with requests for access authorizations may prevent or significantly delay processing. This screening process should be carefully examined as a potential root cause, since the time consumed by personnel security specialists in rectifying errors in pre-employment screening has a considerable impact on budget and personnel resources.

If pre-employment screening does not meet the requirements of the DEAR, there is no assurance that available derogatory information will be forwarded to DOE to alert or direct the investigative agency in conducting its investigation.

Nevertheless, failure to effectively handle initial requests for access authorization can cause significant delays in granting access authorizations. Such delays can have adverse operational, budgetary, and programmatic impacts when organizations are unable to fill positions requiring access to classified information or SNM.

Failure to screen and analyze results of investigations in a timely manner can also have serious impacts on organizations requiring cleared personnel, and on the quality of the process of granting access authorizations. Such failure could result from lack of resources, inadequate training, or both. It is important that personnel assigned to the screening and analysis function be adequately trained in their duties, and that the process be supported by quality assurance and management attention. The analysis of the data in the BI is one of the most important parts of the personnel security program. If poorly done, it can result in unacceptable delays, the granting of access authorizations to unreliable individuals, or the denial of access to reliable and valuable individuals.

All derogatory information must be resolved or mitigated before an access authorization is granted. Granting or continuing access authorization when derogatory information is unresolved poses an unacceptable risk to national security.

Security Education

Management support and adequate documentation are essential to the success of the security education program and should weigh heavily in evaluating the overall program. An inadequate security education program can increase the potential for inadvertent compromise of classified information. Deficiencies in security education are particularly significant if the information security or physical security systems topic teams find that classified matter is not being adequately protected. If the security education program is ineffective, other topic teams will most likely identify deficiencies, such as a lack of understanding of access control procedures, improper handling of classified matter, or inadequate performance of escort duties. Further, if supervisors display a lack of genuine concern or fail to take appropriate corrective action when employees commit security infractions, the security education program is probably deficient.

Security briefings are the heart of the security education briefing and awareness program. Posters, newsletters, booklets, and other media are important; however, an effective briefing program can provide assurance that the target audience is receiving current security information, and that such information is acknowledged and documented.

Visual aids that fail to deliver effective security-related information to employees, and to support the content of security briefings, diminish the goals of providing continuing reminders of the need to protect classified information, and maintaining security awareness between annual refresher briefings.

A lack of experienced, skilled Security Education and Awareness Coordinators can degrade the effectiveness of the security education program, thereby affecting security awareness and the overall security posture of the facility.

Visitor Control

Inadequate control of classified visits can result in a visitor gaining unauthorized access to classified information, SNM, or sensitive information.

Unclassified Visits and Assignments by Foreign Nationals

DOE approval of unclassified visits and assignments for large numbers of foreign nationals permits access to some of its most sensitive facilities, including national laboratories and nuclear weapons facilities. These visits and assignments can take place without endangering DOE security interests if the procedures in DOE directives are effectively implemented and enforced. Otherwise, foreign nationals may gain unauthorized access to classified or sensitive information or matter.

Human Reliability Program

When evaluating the facility's implementation of the HRP, the presence of an effective drug testing program is an important factor in determining its success. Also, if inspectors find that managers, supervisors, and personnel who occupy HRP positions are not fully aware of their responsibilities, it may indicate that the program is deficient and might not be functioning effectively. Inspectors may find supervisors and "Q" cleared personnel in positions who have not been trained in the recognition of security concerns and unusual conduct. This is another indication of a deficiency in the program and, possibly, a lack of management attention.

Because the HRP may be used to mitigate the insider threat, a facility may cite the presence of a HRP as a contributing factor when considering whether the existing risks are acceptable. Occasionally, a facility will cite the HRP as a factor in accepting a moderate to high risk on a temporary basis, if no short-term hardware or procedural fix is practical. Whenever the HRP is cited as a reason for accepting existing risks, inspectors should carefully examine all aspects of the HRP to determine whether the program is fully implemented, effective, and accomplishing its objectives.

Consideration of Integrated Security Management Concepts

As discussed in Section 1, integrated security management is not currently a DOE policy and OA will not use the guiding principles or core functions as a basis for the evaluation, ratings, or findings. However, the integrated security management concept provides a useful diagnostic framework for analyzing the causes of identified deficiencies. For example, inspectors may find that a required action is not being completed. Upon further investigation, the inspectors may determine that the reason is that there has not been a clear designation of responsibility for completing the required action. This situation may indicate a weakness related to line management responsibilities. In such cases, the inspectors would cite the deficient condition (i.e., the failure to complete the required action) as the finding and reference the requirement. In the discussion and opportunities for improvement, however, the inspectors may choose to discuss the general problem with assignment of responsibilities as a contributing factor.

As part of the analysis process, OA inspectors should review the results (both positive aspects and weaknesses/findings) of the review of the protective force topic in the context of the integrated security management concept. Using this diagnostic process, inspectors may determine that a number of weaknesses at a site or particular facility may have a common contributing factor that relates to one or more of the management principles. For example, a series of problems in security awareness could occur if line management had not placed sufficient priority on security awareness functions and has not provided adequate resources to implement an effective security awareness program. In such cases, the analysis/conclusions section of the personnel security report appendix could discuss the weaknesses in management systems as a contributing factor or root cause of identified deficiencies.

This page is intentionally left blank.

Appendix A

DATA ANALYSIS FORMS

The following forms may help inspectors systematically record and evaluate the effectiveness of individual elements of the personnel security program. These forms can be used at the inspector's discretion. In evaluating each element and assigning ratings, it is important to consider all compensatory systems and mitigating factors. Professional judgment must be used to arrive at the overall ratings.

The worksheet for review of personnel security files (page A-2) is not meant to cover all data that an inspector can obtain from the contents of a file. The worksheet is designed to enable the inspector to note important data relative to cases with derogatory information and the means used to address the information. In addition, the worksheet, when completed, will enable the inspector to have a record of what files were reviewed and a quick read of the number of cases where a problem was identified. This will assist in quickly identifying if a systemic problem exists or not.

Worksheet for Review of Personnel Security Files

Personnel Security File Number	Background Investigation Reviewed to Assure Adequate Coverage	Derogatory and Mitigating Information Summarized and Analyzed on Case Analysis	Interview by PS Specialist and Transcript Prepared in Derogatory Cases	LOI (Derogatory Information Not Serious)	Drug Certifications Used in Accordance with SA Guidance	Referred to Psychiatrist	COMMENTS

Data Analysis Form for Human Reliability Program

SUB-TOPICAL AREA	SATISFACTORY	MARGINAL	UNSATISFACTORY
Designation of HRP Positions			
Supervisory Review			
Medical Assessment			
Management Evaluation			
Security Determination			
Program Administration			
Reporting			
Conclusion: Has the inspected office adequately implemented an effective HRP throughout its area of responsibility?			

The impact of identified deficiencies in any of the above sub-elements must be factored into the overall effectiveness of the HRP.

Integration With Other Topical Areas

Protection Program Management/Planning Topic Team:

- Has the budget process adequately considered the HRP function requirements?
- What impact does the HRP have in addressing the insider threat?

Survey Program Topic Team:

- Do the Operations Office surveys include inspection of the HRP program?

Data Analysis Form for Safeguards and Security Awareness Program

SUB-TOPICAL AREA	SATISFACTORY	MARGINAL	UNSATISFACTORY
Administration and Management			
Management Support			
Initial Briefings			
Comprehensive Briefings			
Refresher Briefings			
Foreign Travel Briefings			
Termination Briefings			
Security Education Briefing and Awareness Coordinator Qualifications and Training			
Hostile Contact Reporting			

Integration with Other Topical Areas

CMPC:

- Analysis of types of infractions may be related to inadequate security education and awareness presentations.

Counterintelligence:

- Foreign travel briefings and debriefings are generally conducted by a site's counterintelligence organization. Material presented in these briefings should be current and meaningful.

Survey Program Topic Team:

- Do the Operations Office surveys include inspection of the Safeguards and Security Awareness Program?