INSPECTORS GUIDE

Personnel Security

HSS
Office of Health, Safety and Security

Office of Security Evaluations
Office of Independent Oversight

August 2007

PERSONNEL SECURITY

INSPECTORS GUIDE

August 2007

U.S. Department of Energy
Office of Security Evaluations
HS-61
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 Security Evaluations
HS-61
DOE-HQ
1000 Independence Avenue SW
Washington, DC 20585-1290
or via email: michael.stalcup@hq.doe.gov

Foreword

As part of the mission of the Office of Health, Safety and Security, and to enhance the inspection process, the Office of Independent Oversight (HS-60) has prepared the Personnel Security Inspectors Guide as one in a series of inspectors' guides. The guides incorporate safeguards and security criteria used by the U.S. Department of Energy (DOE) with information gleaned from independent oversight activities to assist inspectors in evaluating safeguards and security protection programs across the DOE complex. Federal and contractor employees may also wish to use the guides to assist in the planning and conduct of surveys and self-assessments. However, an inspectors guide does not represent DOE safeguards and security program implementation policy. Therefore, applicable DOE directives, as well as approved local procedures, must be used to evaluate DOE/National Nuclear Security Administration safeguards and security programs. Users of the guides must also remember that changes can occur in DOE safeguards and security directives that will outpace efforts to maintain the currency of the references listed in a guide, and care must be taken to be knowledgeable of current requirements. A loose-leaf notebook format is used so that sections can be easily removed and copied.

This page intentionally left blank.

Contents

Contents (continued)

Acronyms

AAAP	Accelerated Access Authorization Program
BI	Background Investigation
CES	Case Evaluation Sheet
CFR	Code of Federal Regulations
CI	Counterintelligence
CMPC	Classified Matter Protection and Control
CPCI	Central Personnel Clearance Index
CRD	Contractor Requirements Document
DEAR	Department of Energy Acquisition Regulation
DOE	U.S. Department of Energy
EBT	Evidential Breath Test Device
FACTS	Foreign Activities Central Tracking System
FBI	Federal Bureau of Investigation
FV&A	Foreign Visits and Assignments
HRP	Human Reliability Program
HS-60	Office of Independent Oversight
HS-61	Office of Security Evaluations
HS-70	Office of Security Policy
IG	Inspector General
ISSM	Integrated Safeguards and Security Management
JTA	Job/task Analysis
LOI	Letter of Interrogatory
LSPT	Limited-Scope Performance Test
MAA	Material Access Area
NNSA	National Nuclear Security Administration
ODC	Oversight Document Center
OJT	On-the-Job Training
OPM	Office of Personnel Management
OPSEC	Operations Security
PPM	Protection Program Management
PSC	Personnel Security Clearance
PSF	Personnel Security File
PSI	Personnel Security Interview
PSO	Program Secretarial Officer
QNSP	Questionnaire for National Security Positions
QRB	Quality Review Board
SAP	Special Access Program
SF	Standard Form
SNM	Special Nuclear Material
SO	Office of Security
SOMD	Site Occupational Medical Director
SSAP	Safeguards and Security Awareness Program

Acronyms (continued)

SSD	Safeguards & Security Director
SSSP	Site Safeguards and Security Plan
STS	Security Termination Statement

Section 1

INTRODUCTION

Contents

Purpose

The Office of Security Evaluations (HS-61) 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 (HS-60) Appraisal Process Protocols and to the Independent Oversight 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 U.S. 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 directives (including policies, orders, and manuals); rather, it is intended to provide practical guidance for planning independent oversight activities and collecting and analyzing inspection data.

One significant consideration in developing HS-61 inspector's guides is to provide a repository for the collective knowledge of HS-61's inspectors that can be enhanced and updated as inspection methods improve and HS-61 inspection experience accumulates. Every attempt has been made to develop specific guide-lines 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

Historically, HS-60 has included the personnel security clearance (referred to interchangeably as an access authorization in this inspectors guide) program, human reliability program (HRP), safeguards and security awareness program (SSAP), and the foreign visits and assignments (FV&A) program in the characterization of the personnel security topic. Even though these four programs fall under different program managers, all of the programs were included since the purpose of these programs is to ensure that access to sensitive information, classified matter, and special nuclear material (SNM) will be granted only after it has been determined that such access will not endanger security and is consistent with the national interest. Additionally, each of these programs contains requirements that are intended to ensure continuing awareness of security responsibilities among program officials and DOE/National Nuclear Security Administration (NNSA) employees, contractors, and consultants. A set of performance measures for the personnel security program topic is included in Appendix A and should be consulted by inspectors during all phases of an inspection activity. In doing so, inspectors will maintain a consistent focus on the personnel security program during planning, data collection, analysis, and report preparation.

The appropriate granting of an access authorization or clearance, making program officials and employees aware of their security responsibilities, and controlling foreign national 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 matter and SNM. This is especially important since DOE/NNSA is responsible for the nation's nuclear weapons complex, and individuals with an access authorization (and a need-to-know) may have direct access to nuclear weapons, classified parts, Restricted Data, SNM, or other classified matter. Therefore, determination of 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 a clearance.

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 6 provide detailed guidance for inspecting each major personnel security subtopic:

- Section 2 – Management
- Section 3 – Personnel Security Clearance Program
- Section 4 – Safeguards and Security Awareness Program
- Section 5 – Human Reliability Program
- Section 6 – Unclassified Visits and Assignments by Foreign Nationals

The subtopic sections are further divided into several sub-elements to assist the reader in understanding subtopical organization.

Section 7 (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 8 (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 Collection and Analysis Tools) contains tools and worksheets that may be helpful to inspectors during data collection.

Using the Topic-Specific Tools

Sections 2 through 6 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 from management.

- Personnel security clearance program: Distinctive for determining the eligibility of individuals for access to classified matter and SNM, the program addresses appropriate types of access authorizations, pre-employment checks, adjudication of cases, and reinvestigations.

- Safeguards and security awareness program: This program is maintained through the presentation of initial, comprehensive, refresher, and termination security briefings that are supplemented by additional materials (e.g., posters, email messages, newsletter articles).

- Human reliability program: The HRP is designed to ensure that individuals with unescorted access to nuclear explosives and Category I quantities of SNM or who have information concerning vulnerabilities in protection programs for nuclear explosives and Category I quantities of SNM meet the highest standards of reliability and physical and mental suitability. The high standards are necessary to reduce the potential for significant impacts or unacceptable damage to national security.

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

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 directives and other applicable policy documents that serve as the basis for evaluating the inspected program and identifying findings. Due to periodic changes in policy, it is also useful to refer to the applicable directives during data collection activities to ensure that the most current directive is being used.

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, HS-61 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 HS-61 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 collection 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 materials, 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. To further aid inspectors in planning inspection activities, Appendix A includes a detailed inspection plan, a sample document request list, and program performance measures discussed above.

Though specific activities and documents are identified in sections 2 through 6, the following are germane to all of the elements of the personnel security topic and assist in defining the scope of inspection activities.

- Operations/Site Office survey reports and corrective action plans developed to address identified findings
- Facility/program self-assessment reports and corrective action plans
- Approved and pending deviations from DOE requirements for any element of the personnel security topic
- Organization charts or other descriptive materials for each/all of the elements of the personnel security topic
- Maps or other descriptive materials identifying all security (property protection, limited, exclusion, protected, or material access) areas.

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 are 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 HS-60 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. Inspectors should make use of the tools and forms contained in Appendix A in support of data collection activities.

Validation

Validation is one of the most important activities conducted during the inspection. It is the procedure that HS-60 inspectors use to verify the accuracy of the information obtained during data collection activities. The validation process, discussed in detail in the HS-61 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 the SSAP, while others review personnel security files (PSFs). 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 also for site representatives who may have also been separated as they accompany HS-61 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 that the facts are confirmed during the daily and summary validations.

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 and memoranda 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, policy supplements, etc.) to determine whether the facility is complying with all applicable requirements, including those issued by DOE Headquarters and/or NNSA.

- 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 Safeguards and Security Management

The Department is committed to conducting work efficiently and securely. DOE Policy 470.1, *Integrated Safeguards and Security Management (ISSM) Policy*, is designed to formalize a framework that encompasses all levels of activities and documentation related to ISSM.

The guiding principles of ISSM are:

- Individual responsibility and participation

- Line management responsibility

- Clear roles and responsibilities

- Competence commensurate with responsibilities

- Balanced priorities

- Identification of safeguards and security requirements

- Tailoring of protection strategies to work being performed.

The five core functions of ISSM are:

- Define the scope of work.

- Analyze the risk.

- Develop and implement security measures and controls.

- Perform work within measures and controls.

- Provide feedback and continuous improvement.

For the purposes of this Personnel Security Inspectors Guide, HS-60 has highlighted the following four guiding principles and one core function.

Individual Responsibility and Participation. Each individual is directly responsible for following security requirements and contributing to secure missions and workplaces.

Line Management Responsibility for Safeguards and Security. Line management is directly responsible for the protection of DOE/NNSA assets, and as such is required to analyze risk, develop controls, and verify the adequacy of these controls.

Competence Commensurate with Responsibilities. Individuals must possess the experience, knowledge, skills, and abilities necessary to fulfill their responsibilities.

Identification of Safeguards and Security Standards and Requirements. Safeguards and security standards and requirements have been established that, if properly implemented, will provide appropriate assurance that DOE/NNSA assets, workers, and the public are protected.

Provide Feedback and Continuous Improvement. Feedback information on the adequacy of measures and controls is gathered during inspections, surveys, and self-assessments. Opportunities for improving safeguards and security programs are also identified and implemented. Best practices and lessons learned are shared.

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 performance in a structured and consistent manner.

This page intentionally left blank.

Section 2

MANAGEMENT

Contents

References

DOE Order 470.4, *Safeguards and Security Program*
DOE Manual 470.4-5 *Personnel Security*
DOE Order 142.3, *Unclassified Foreign Visits and Assignments Program*
10 CFR 710, Subpart A, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*
10 CFR 712, *Human Reliability Program*
Site Safeguards and Security Plan (SSSP) Preparation Guide

General Information

The personnel security program is a major component in the protection of DOE/NNSA 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 and SNM, but also for re-evaluation for continued access eligibility every five to ten years based on the type of access authorization. It is the only program to focus on individual eligibility for access throughout the life of the clearance—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 matter and sensitive unclassified information, the personnel security program focuses on a continuing safeguards and security awareness program. In addition, in today's environment of more openness and information exchange, added emphasis is now being placed on foreign national visits to DOE sites.

A strong personnel security program 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 HRP participation 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 policies, plans, and resources are adjusted to meet changing threat situations. The personnel security program is usually described in the Management Report of the SSSP. At those facilities where an SSSP is not required, planning and budgeting for the personnel security program must be formally documented in a Site Security Plan.

Another indication of effective management is whether adequate resources are available to perform all personnel security program functions in a timely manner, such as access terminations, adjudication of derogatory information, Central Personnel Clearance Index (CPCI) input, annual recertification of individuals enrolled in HRP, conduct and documentation of awareness briefings, and analysis and mitigation of the threat represented by foreign national visitors. It is important that adequate staffing levels are maintained and that individuals performing critical tasks in the personnel security program are properly trained.

Finally, line management support is essential to ensure the success of all other features of the overall personnel security program, to include the clearance process and the SSAP, which are discussed in detail in subsequent sections.

Common Deficiencies/ Potential Concerns

Individual Responsibility and Participation

Failure to Complete the Annual Security Refresher Briefing Requirement. At many DOE/NNSA facilities, employees are expected to complete a self-paced annual security refresher briefing. When these self-paced briefings are not completed in a timely manner, employees may not be aware of new or revised safeguards and security requirements that could lead to inadvertent security lapses. Though site awareness coordinators and supervisors have employed a variety of techniques to remind employees of the need to complete these briefings, it ultimately falls on the individual to ensure that they are aware of all security requirements.

Numerous Incidents of Security Concerns. Similarly, DOE/NNSA organizations that are experiencing high numbers of incidents of security concerns probably have deficient SSAPs. Though not the only measure of program effectiveness, casual analysis of these incidents often indicate that individuals either do not understand their safeguards and security responsibilities or awareness briefings are not effectively communicating employee safeguards and security requirements. Awareness coordinators must be cognizant of the number, type, and results of investigations of incidents of potential security concern.

Hosting Foreign National Visitors Prior to or Without Approval. Sophisticated on-line FV&A request and approval systems now support a number of DOE/NNSA programs. Even though these programs offer the potential to better control visiting foreign nationals, when employees fail to utilize these programs and host a foreign national prior to or without approval, then unanalyzed and unmitigated risks are being accepted by facility managers. It is essential that employees realize that they are the most important element in the protection program in mitigating the risk represented by visiting foreign nationals.

Line Management Responsibility for Safeguards and Security

Inadequate Involvement of Personnel Security in the 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 and SNM. 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. This means ensuring that sufficient funds, adequate DOE personnel (supplemented with contractor personnel, as appropriate), and case management systems are available to effectively implement the personnel security program and handle all critical personnel security functions. Without adequate resources, clearances cannot be processed efficiently and within prescribed time frames, individuals cannot be properly enrolled or expeditiously removed from HRP, assurances cannot be given that all individuals are aware of their safeguards and security program responsibilities, and control of foreign nationals cannot be achieved.

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, processing unnecessary access authorization requests, minimal participation in the security awareness briefings, and foreign visits that take place without approval). 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.

Competence Commensurate With Responsibilities

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 710) for adjudication of cases with derogatory information and preparation of cases for administrative review. Another example is the need for training of all hosts and escorts of foreign national visitors and assignees. A lack of training can lead to an unauthorized disclosure of sensitive information or classified matter.

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.

Identification of Safeguards and Security Standards and 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 for Category I SNM facilities, and site security plans for other facilities). During planning, it is important that managers consider the impact on the personnel security clearance program, FV&A, and the HRP. For example, the reconfiguration of a facility without considering the impacts on personnel security may result in additional expenses associated with access authorizations for employees for the sole purpose of accessing the facility to reach their place of work, the failure to enroll individuals in an HRP prior to the conduct of work, or major problems in processing and escorting uncleared foreign national visitors.

Feedback and Continuous Improvement

Inadequate Self-Assessment Process. Not all facilities have implemented a comprehensive self-assessment program. 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 and program inefficiencies going undetected and uncorrected for extended periods. Self-assessments by their nature focus on elements of the personnel security program that are not always evaluated during surveys. Therefore, when self-assessments are not conducted for all elements of the personnel security program resources may be misused and the underlying causes for program inefficiencies will not be identified.

Inadequate Surveys. Organizations charged with the responsibility to conduct surveys rarely have the appropriate staff to conduct comprehensive evaluations of the personnel security program. This can lead to surveys that lack depth and subsequently do not evaluate all of the critical elements of the personnel security program. Operations offices and Headquarters elements that conduct surveys must be mindful of this situation and take steps to ensure that an adequate number of competent personnel is assigned to evaluate the personnel security program. This sometimes requires obtaining assistance from other organizations or from support contractors to ensure that proper surveys are conducted.

Inadequate Corrective Action Plans. This is a somewhat common and potentially serious concern 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 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 as 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).

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

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

- Review standard operating procedures to determine if they accurately reflect DOE requirements and support efficient and effective program implementation.

- Determine the number of personnel security positions authorized, the number of positions currently filled, the job descriptions of these positions, and the locations (via organization charts and other diagrams) of the positions in the facility organization.

- Review the primary and secondary duties and responsibilities of the DOE/NNSA personnel security organization staff and contractor

support personnel to determine whether functions have been appropriately distributed to ensure efficiency and in a manner that will not impact overall performance.

- Examine the type and content of on-the-job training programs and training records to determine the level of training attained by personnel security program professionals.

- Examine the turnover of Federal and support contractor staff to determine if the turnover is impacting performance.

- Review the results of recent surveys and self-assessments to determine if feedback programs are producing comprehensive evaluations of the personnel security program, and are resulting in the

- Correction of deficiencies and program enhancements.

Data Collection Activities

Individual Responsibilities and Participation

Data collection activities should be conducted to determine whether individuals understand their responsibilities and whether individual participation is supportive of an effective protection program. Performance testing activities will also take place during the inspection in each of the subtopical elements of the personnel security topic to assist in making this determination. These are discussed in Sections 3 through 6.

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. 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 any backlog of requests for access authorizations, screening investigation reports, additional adjudicative actions, and HRP enrollment and recertifications

- Determining the extent of any temporary or short-term use of personnel or other resources to reduce backlogs.

- 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 personnel security clearance organization's ability to respond to "surge" situations.

Competence Commensurate With Responsibilities

C. It is important that inspectors determine how well the personnel security program staff is trained. Interviews of supervisors and staff should be conducted to determine, if applicable, the reason why training provided by the National Training Center was not made available to the staff. The effectiveness of implementing the personnel security program sub-elements will also provide insights into how well the staff has been trained.

D. If a formal in-house training program is in place, inspectors may elect to review a sample of training records or certifications to determine what training is available and who has completed the training. Also, needs and job task analyses and lesson plans should be reviewed. If these tools have not been developed, it will call into question the effectiveness of the training program. Time permitting, 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.

E. 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).

Identification of Safeguards and Security Requirements

F. Selected processes should be mapped and interviews conducted to determine whether standard operating procedures reflect the operational environment and actual program processes. These data collection activities may also be used to identify process inefficiencies, deficiencies in training, and failures to meet DOE requirements.

G. Inspectors should determine how management communicates its goals and objectives, and stress the importance of personnel security. Inspectors should determine what performance measures are used to track achievement of performance objectives and what programs are used to maintain an appropriate level of safeguards and security awareness.

H. Inspectors should determine whether the persons responsible for the personnel security program are in a position to ensure compliance and whether they are receiving adequate management support. This is especially important for implementation of the HRP, SSAP, and FV&A programs. Interviews with managers in the security department and the 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. It might also be necessary to review self-assessments and survey findings and corrective action plans 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.

Feedback and Continuous Improvement

I. Inspectors should coordinate with the protection program management team concerning the review of the self-assessment program. They should determine whether self-assessments are performed regularly and whether they review all aspects of the personnel security program. It is helpful to compare the results of the facility self-assessments to inspection findings or other audit results to learn whether the self-assessments are equally as effective.

J. Inspectors should determine whether corrective action plans have identified all causal factors, specific actions (with milestones) to address all causal factors, and specific individuals who are responsible for implementation of the corrective actions.

K. Inspectors should review the role of DOE/NNSA oversight by reviewing recent survey reports to determine how DOE/NNSA implements their responsibilities and whether survey results agree with the results of independent oversight activities. Specific items to cover include how DOE/NNSA reviews the contractor personnel security program functions on surveys, how DOE/NNSA tracks the program status, and how DOE/NNSA and the facility interact on a day-to-day basis.

Performance Test

Inspectors should select all deficiencies indicated as closed and collect data and test to verify that they have in fact been adequately corrected.

The page intentionally left blank.

Section 3

PERSONNEL SECURITY CLEARANCE PROGRAM

Contents

References

DOE Manual 470.4-5, *Personnel Security*
Department of Energy Acquisition Regulation (DEAR)
48 CFR 970.2201-1-2(a)(1)(ii), *Labor Relations*
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
10 CFR 710, Subpart A, *Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*
Atomic Energy Act of 1954 (as amended)

The process of determining eligibility is at the heart of the personnel security program, and is the first line of defense against the insider threat.

The DOE personnel security clearance program establishes a structured and uniform approach for determining eligibility. 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 to classified matter and SNM, and 10 CFR 710, which establishes criteria and methods for resolving questions of eligibility of individuals for access. DOE/NNSA personnel security organizations and contractor personnel security organizations are responsible for implementation of the personnel security clearance program.

Only individuals whose jobs require access to classified matter or SNM are to be processed for security clearances. Additionally, pre-employment checks are required of employees being hired for positions requiring such access by DOE/NNSA management and operating contractors who operate DOE-owned facilities and those contracts that contain a 48 CFR 952.204-2 security clause.

The Federal Bureau of Investigations and the Office of Personnel Management (OPM) are the primary providers of security background investigations (BIs) to the DOE/NNSA personnel security organization. The DOE/NNSA personnel security organization will also accept the results of other government agency BIs that meet DOE requirements. After the DOE/NNSA personnel security organization has received the results of a BI, they are reviewed and adjudicated in accordance with the criteria set forth in 10 CFR 710. Under the requirements of the reinvestigation program, individuals granted a DOE clearance must be reinvestigated every five years for a "Q" access authorization, and every ten years for an "L" access authorization (see Figure 1).

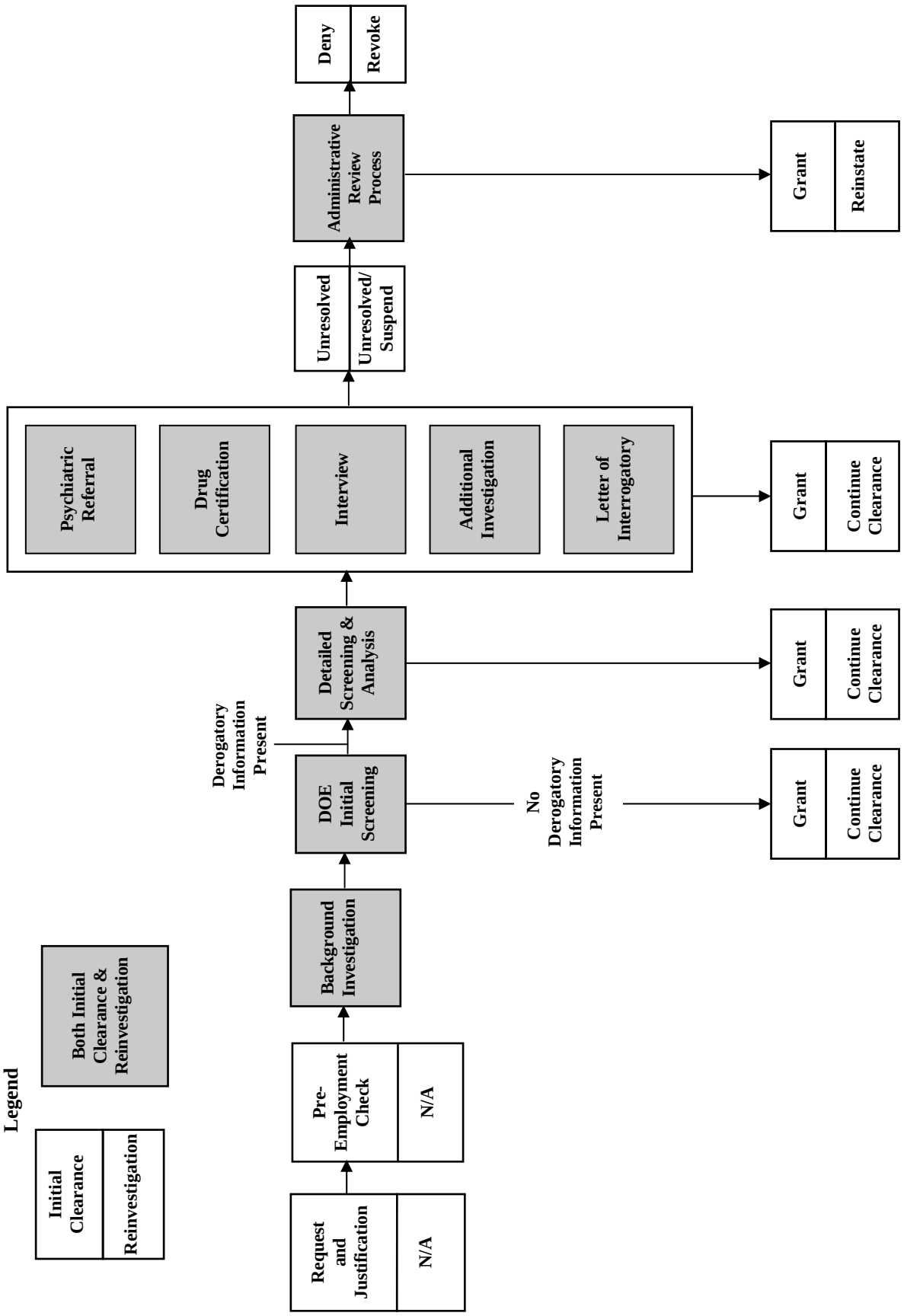

Figure 1. DOE Clearance Process

Section 3.1

Pre-employment Checks

Contents

General Information

Pre-employment checks are conducted to identify any readily available derogatory information that would preclude employment for a potential contractor employee. Pre-employment checks include verification of citizenship, a credit check, verification of a high school degree or diploma granted by an institution of higher learning within the past five years, personal references, former employers, and a local law enforcement check. When submitting a request for an access authorization, the contractor provides documentation certifying that a pre-employment check has been conducted, and the results. The pre-employment checks and resulting suitability review must be completed prior to submission to the DOE/NNSA personnel security organization for processing.

Common Deficiencies/ Potential Concerns

Derogatory Information Not Forwarded to DOE

Contractors may not always forward derogatory information revealed during pre-employment checks. This failure may result from an oversight, or from ineffective procedures for providing information to the DOE/NNSA personnel security organization. It is important that all derogatory information obtained during pre-employment checks be forwarded to allow the DOE/NNSA personnel security organization to properly scope the investigation being submitted to OPM or the Federal Bureau of Investigation (FBI). In some cases, the DOE/NNSA personnel security organization may complete adjudicative actions prior to submitting the investigation.

Incomplete Information

Apart from derogatory information that may be identified during the pre-employment check and proof of citizenship, other required information may not be included on the Questionnaire for National Security Positions (QNSPs) that is submitted along with the request for access authorization (for example, highest degree held, personal references, previous employers, and part-time employment). Incomplete information results in a delay in processing the clearance request.

Planning Activities

- Obtain the names of new hires and hire dates for cleared employees to determine whether the pre-employment check was completed prior to submission of a request for an access authorization.
- Review a list of cleared employees whose clearances were reinstated and who were not continuously employed by the same contractor.
- Review the methods used to determine the accuracy and completeness of pre-employment checks.

- Determine whether contractors submit written statements providing the results of their pre-employment checks, including all derogatory information.

- Determine whether DOE/NNSA personnel security organizations have a process to ensure pre-employment checks are completed prior to submission to the investigative agency.

Data Collection Activities

A. Inspectors should determine whether the DOE/NNSA personnel security organization survey program addresses pre-employment checks.

Performance Tests

B. Inspectors should review a number of recently submitted contractor clearance requests to determine whether statements indicating the results of pre-employment checks were forwarded to the DOE/NNSA personnel security organization. The contractor PSFs, or personnel files associated with these requests, should also be reviewed to determine whether information in the files coincides with information forwarded to the DOE/NNSA personnel security organization, and whether the contractor ensures that pre-employment checks include all required elements.

C. Inspectors should obtain a list of contractor new hires and verify that pre-employment checks were completed and that suitability for employment was established prior to their hire date.

Section 3.2

Types of Access Authorizations

Contents

General Information

Requests for access authorizations are certified by appropriate personnel at the DOE/NNSA personnel security organization office or contractor facility. The key elements of the process include certifying that requests for access authorizations are necessary, ensuring that the type of access authorization is consistent with the work performed, and ensuring that the clearance is terminated and security badges are returned when the need for access no longer exists.

The initial request for access authorization must be complete, fully justified, and include the pre-employment check results (see Section 3.1) before it is submitted for processing.

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

Common Deficiencies/ Potential Concerns

Unjustified Requests for Clearance

Access authorizations are often requested when the justification is questionable. Certification procedures must support the DOE requirement that clearances be initiated only when the duties of a position require access to classified matter or to SNM and be consistent with the work performed. A DOE Federal employee must review all clearance requests and justifications to ensure that they meet these criteria. Requests not meeting these criteria should not be processed.

Inappropriate Type of Access Authorization

In some cases the requested type of access authorization 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 DOE/NNSA personnel security organization is responsible, and has the authority, to determine whether individuals require an access authorization and if so, what type. Inspectors would not normally question the DOE/NNSA personnel security organization's judgment on individual cases; however, inspectors should determine whether the DOE/NNSA personnel security organization has adequate procedures for determining whether requests are fully justified. Inspectors should also determine whether the DOE/NNSA personnel security organization reviews categories of personnel (for example, janitors and cafeteria workers) for the appropriateness of their access authorization types.

Changes in Status

Status changes for cleared personnel may warrant terminating or reducing the type of clearance. Job changes, misconduct, reassignment of duties, organizational restructuring, foreign travel, prolonged absence, and the results of inspections might affect justification for continuing a personnel security clearance.

A particular problem exists in controlling clearances granted to contractors employed for specific jobs with limited duration. Often, the DOE/NNSA personnel security organization lacks an adequate system for tracking the status of the clearance to determine the need for it to continue after job completion. As a result, the clearance may not be terminated in a timely manner and security badges may not have been returned. If this happens, the number of contractor personnel who no longer need access continues to grow, increasing the possibility of unauthorized personnel gaining access to DOE/NNSA facilities.

DOE Manual 470.4-5 allows a contractor to request that an individual retain a clearance upon job completion, but only if the contractor verifies that the individual will be reemployed or reassigned by the contractor within the next three months to a position that will again require a clearance. In some cases, clearances may be improperly continued for up to 90 days 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 if they are not properly tracked and controlled.

Planning Activities

- Review procedures used to determine types of access authorizations for contractor and subcontractor personnel.

- Obtain a list of all inactive classified contracts.

- Obtain a list of personnel with access authorizations, and for contractors, the associated contract.

Data Collection Activities

Request Procedures

A. Inspectors should interview individuals responsible for handling requests for access authorizations to determine how the process is conducted, and how the need for access is certified. Justification for the access must be based on the duties of the position, that the duties require access to classified matter or SNM, and that the type of clearance is appropriate. It is usually helpful for the responsible individuals to explain, step by step, how they determine the need for access and the type of clearance.

B. Inspectors should request that operational departments provide sample files for cleared individuals who have changed positions. If the individuals' duties no longer require access to classified matter or SNM, inspectors should determine whether action was taken to terminate the clearances, or otherwise change the type of access authorization.

Performance Tests

C. Inspectors should review personnel security files to determine whether their duties justify the clearance. Alternatively, inspectors may interview selected cleared personnel to determine their access requirements.

D. Inspectors should obtain a sample list of terminated contractor and subcontractor personnel to determine whether action was taken to terminate their clearances and return security badges in a timely manner.

E. Inspectors should compare the list of inactive contracts with the site's list of cleared individuals to determine whether any individuals are no longer working on an active contract and therefore require termination of clearance.

Section 3.3

Processing Access Authorization Requests

Contents

General Information

Paperwork flows from initiation of the access authorization request, through certification of need, to verification of completeness, to forwarding of the request to the appropriate investigative agency by the DOE/NNSA personnel security organization. It ends with the notification of grant, reinstatement, or denial of the clearance by the DOE/NNSA personnel security organization. Staffing, training, procedural guidance, and oversight significantly affect the success or failure of this process.

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 DOE/NNSA personnel security organization fails to meet specified timeframes. 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 clearance 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 Procedures

Inadequate procedures for the processing activity can cause turbulence, inefficiency, and delay.

Inadequate/Untimely Information From Contractors

Contractor organizations may not always inform DOE of changes in status, additional information, the applicable contract number, or the cancellation of a clearance 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 a clearance, or when an individual has terminated employment, the DOE must be notified immediately, and the request for access authorization must be canceled/ terminated.

Failure to Return OPM 79A

DOE/NNSA personnel security organizations are required to return OPM 79A after a clearance is granted or continued for a Federal employee. This action is necessary for OPM to complete its responsibility regarding determining an individual's suitability for Federal employment.

Planning Activities

- Review a description of the facility's personnel security clearance processing system, tracking system, and procedures.
- Determine the average time it takes the DOE/NNSA personnel security organization to submit requests for investigations to OPM and the FBI.
- Determine whether any problems have been encountered by the DOE/NNSA personnel security organization in reviewing QNSP (SF-86) packages.
- Review methods for processing naturalized citizens and dealing with individuals holding dual citizenship.
- Examine procedures for entering information into the CPCI.
- Examine procedures for the return of OPM 79A.

Data Collection Activities

Staffing

A. Inspectors should interview program managers in the DOE/NNSA personnel security organization to determine whether sufficient personnel are assigned to the 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.

Processing

B. Inspectors should determine how the DOE/NNSA personnel security organization resolves and tracks derogatory information identified on Part II of the QNSP.

Naturalized/Dual Citizenship

C. Inspectors should verify that the procedures for processing naturalized citizens and dealing with individuals holding dual citizenship are in accordance with DOE directives.

Performance Tests

D. Inspectors should determine whether all required information is 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. In preparation for this performance test, inspectors should coordinate with the Office of Personnel Security (SO-30.2) for the production of a CPCI report indicating the date of entry for information related to the selected files.

E. Review selected PSFs to ensure appropriate return of the OPM 79A.

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

Section 3.4

Screening and Analysis

Contents

General Information

Screening and analysis of the background investigation reports or other reported information (self-reporting, security infractions, employee concerns programs, Inspector General (IG) investigations, pre-employment check results, and other sources) is one of the most important aspects of the overall personnel security clearance program.

Upon receipt of completed reports of investigation, the screening and analysis functions include checking to ensure that all items on the SF-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 710), has been made by the personnel security specialist to determine whether the reported information raises substantial doubt concerning eligibility for a clearance.

Screening and analysis does not include an evaluation of the adjudication of derogatory information, which is covered in Section 3.5.

Common Deficiencies/ Potential Concerns

Lack of Timely Screening and Analysis

Lack of timely screening and analysis usually results in a backlog of access authorization requests and reinvestigation cases, and time limits set by DOE to either grant a clearance or begin action to resolve derogatory information may not be met. Backlogs can place pressure on management, especially on the personnel security specialists assigned to do the work. When pressure builds, screening and analysis may be rushed, resulting in a reduction in 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 omissions, 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/Inaccurate Procedures

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 clearance program, it is important that it receive adequate management oversight and support.

Reports of Personnel Security Interest

To ensure an individual's continued eligibility to hold a DOE access authorization, information of security interest (e.g., incidents of security concern/infractions, disciplinary action, unusual behavior) must be reported to the DOE/NNSA personnel security organization. Often such sources as human resources, company investigative departments, employee relations, supervisors managers are reluctant to share this information. Consequently, individuals with unresolved derogatory information continue to have access to classified matter and/or SNM. Establishing open lines of communication and written procedures that include reporting requirements for all of applicable organizations will encourage proper reporting of items of personnel security interest.

Planning Activities

- Determine the level of staffing assigned to screening and analysis. Review procedures used for the screening and analysis functions, including the evaluation of derogatory information.
- Determine whether there is a formal procedure in place that requires the reporting of information of security interest to the DOE/NNSA personnel security office.
- Review the current caseload and impact.
- Determine timeframes required to process cases, compared to DOE requirements.

Data Collection Activities

Personnel Resources

A. Inspectors should review the workload, overtime, and turnover rate 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 assigned duties, timeliness, workload, procedures, and available training.

Supplemental Tools

B. Inspectors should determine whether specialists consider letters of interrogatory, personnel security interviews, supplemental investigations, requests for information from outside sources, or psychiatric evaluations to obtain additional information to adjudicate a case. Case evaluation sheets (CESs) should reflect the rationale for these considerations.

Receipt of Reports

C. Inspectors should determine if reports of security interests (e.g., security incidents and infractions, written disciplinary actions, terminations for cause, Equal Employment Opportunity complaints) are being received and screened in a timely manner.

Performance Test

D. Inspectors should review randomly selected files to determine whether initial screening and notification of grant of clearance are completed within seven days of the receipt of completed investigations in clear cases and whether required follow-up actions are initiated within 30 days of receipt of the completed investigations.

Section 3.5

Adjudicating Derogatory Information

Contents

General Information

The evaluation of how well the DOE/NNSA personnel security organization adjudicates derogatory information is a challenge to the inspector because of the common sense judgment required to determine an individual's eligibility for a security clearance. Inspectors should not normally place themselves in a position of questioning these judgments. Rather, they should determine whether adequate procedures are in place and being followed, training is sufficient, the Adjudicative Guidelines are being followed, recommendations for resolution are fully documented and supported on the CES, and whether quality assurance functions (peer and supervisory reviews) are being performed.

Reports of investigations and other sources of derogatory information are analyzed to evaluate them in relation to the criteria in 10 CFR 710, and to determine whether they contain derogatory information sufficient to raise substantial doubt about clearance eligibility. If there is substantial doubt, a number of alternatives are available for resolution, including letters of interrogatory, interview, psychiatric evaluation, information from outside sources, and additional investigation. If the derogatory information cannot be satisfactorily resolved, a cleared individual's access authorization is suspended and the case is referred to the Office of Security (SO) with a request to proceed with an administrative review. If derogatory information cannot be resolved in an applicant case, the case is referred to SO with a request to proceed with an administrative review.

Common Deficiencies/ Potential Concerns

Inadequate Documentation of Recommendations or Conclusions

While most DOE/NNSA personnel security organizations normally employ adequate adjudicative actions (letters of interrogatory, interviews, and psychiatric evaluations) to resolve derogatory information, personnel security specialists may not always fully document their actions, conclusions, and recommendations on the CES. The CES must show evidence that the adjudicative guidelines were used as a basis for determining resolution of security concerns. Not documenting all previously identified derogatory information, the results of actions to resolve the current security concern, and the rationale for their recommendation could be an indication that the security concerns have not been resolved. Further, this lack of documentation impacts the efficiency and effectiveness of peer and supervisory reviews.

Deficient Process to Suspend Access In Conjunction With Submission for Administrative Review

Sometimes, the DOE/NNSA personnel security organization does not take timely action to

suspend access in conjunction with submitting a case for administrative review. When this occurs, individuals with significant, unresolved derogatory information will continue to have access to classified matter and/or SNM.

Planning Activities

- Review procedures for preparing letters of interrogatory, interviews, forwarding cases for psychiatric evaluation, and for administrative review processing.

- Determine whether organizational procedures provide sufficient guidance for properly documenting the adjudication of derogatory information on the CES, and to properly organize materials in the PSF.

- Review procedures for entering information into CPCI after the adjudication of derogatory information.

- Review the procedures for requesting and conducting an administrative review to include clearance suspension, CPCI entry, and badge return (if appropriate).

- Determine whether OPM 79A is being returned after actions to resolve derogatory information have been completed.

Data Collection Activities

Staff Level

A. Inspectors should review staffing to determine whether adequate personnel resources are assigned to process derogatory information.

Performance Tests

B. A number of PSFs should be randomly selected for review from listings provided by the site being inspected. The listings should identify cases processed by the site in a particular timeframe, 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, administrative review referrals, etc.). If backlogs exist, inspectors should determine the causes. Interviews with security managers will often reveal the reasons for backlogs.

C. Inspectors should review CESs from a selection of files known to contain derogatory information to determine whether the derogatory information has been appropriately resolved or mitigated and the adjudicative guidelines were use as a guiding factor or as a basis for resolution. Case analysis documentation must show what the derogatory information is and the thoughts presented by the specialist as to why the derogatory information does or does not pose a threat in one of the areas of the criteria.

D. Inspectors should review cases in which the clearance was suspended to determine whether proper procedures were followed (i.e., notification of appropriate DOE/NNSA or contractor managers, proper escorting for those authorized continued access to authorized areas, and/or retrieval of security badges), and whether appropriate documentation exists to justify suspension of the clearance. This test may require coordination with the physical security system topic team.

Section 3.6

Reinvestigations

Contents

General Information

The DOE reinvestigation process is designed to ensure the continued eligibility for a security clearance for individuals requiring access to classified matter or SNM.

DOE orders require that individuals holding a "Q" access authorization be re-evaluated every five years, and those holding an "L" access authorization be re-evaluated every 10 years.

Common Deficiencies/ Potential Concerns

A system must be in place to ensure that individuals submit updated QNSPs through their employer to the DOE/NNSA personnel security organization in order to ensure that a reinvestigation has been initiated in accordance with requirements. Upon receipt of the reinvestigation, the DOE/NNSA personnel security organization must review the case in a timely manner to identify and address any security issues (as described in Section 3.5), since these individuals have current and continuing access pending this review.

Planning Activities

- Review procedures followed when new derogatory information is found on a QNSP completed for reinvestigation.
- Review procedures for the administration of the reinvestigation program that explain how the reinvestigation program is to be accomplished to ensure timely submission of all cases due for reinvestigation each fiscal year
- Determine whether reinvestigations with derogatory information are given priority adjudicative attention.
- Determine whether the facility maintains schedules or other tracking documents relative to the reinvestigation program.

Data Collection Activities

A. Inspectors should review the PSFs to determine whether reinvestigations are initiated within the required timeframes.

B. Inspectors should review the DOE/NNSA personnel security organization records and tracking system to determine whether reinvestigation cases are submitted to OPM or the FBI in a timely manner.

C. Obtain a CPCI list from Headquarters showing which individuals are overdue for reinvestigation.

Performance Test

D. Test for accuracy and timeliness of CPCI data entry for reinvestigations and associated derogatory codes.

This page intentionally left blank.

Section 4

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

Contents

References

DOE Order 470.4, *Safeguards and Security Program*
DOE Manual 470.4-1, Chg 1, *Safeguards and Security Program Planning and Management*
DOE Manual 470.4-5, *Personnel Security*
Executive Order 12968, *Access to Classified Information*
Executive Order 12958, *Classified National Security Information*, as amended
Executive Order 12829, *National Industrial Security Program*
Presidential Decision Directive/NSC-12, *Security Awareness and Reporting of Foreign Contacts*
32 CFR 2001 and 2004, *Classified National Security Information Directive No.1*, Subpart F, *Security Education and Training*
32 CFR 2003.20, *Classified Information Nondisclosure Agreement: SF-312*

The DOE/NNSA SSAP is designed to ensure that all individuals are informed of their security responsibilities associated with DOE/NNSA programs and activities. The program also alerts individuals to actual or potential threats, and motivates them to maintain a high level of safeguards and security awareness. DOE requires formulation, implementation, and maintenance of a structured SSAP in all DOE/NNSA and contractor organizations where there is a requirement for a security clearance, access to SNM, or protection and control of nuclear matter.

This page intentionally left blank.

Section 4.1

Administration and Management

Contents

General Information

DOE requires that an SSAP be established that addresses security clearance 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, to meet this requirement, briefing plans, briefing objectives, supplemental awareness materials, and evaluation methods will have to be developed and implemented.

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

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

Normally, the facility security department is responsible for management of the SSAP; however, safeguards and security briefings 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 safeguards and security awareness briefings for their assigned personnel.

Many sites must also include off-site contractors, subcontractors, consultants, and access permittees in their SSAP.

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 assign 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.

Security Awareness Programs Not Established

Frequently, subcontractors and small prime contractor organizations choose not to establish SSAPs, and their employees participate in the program of a large prime contractor. It is important that the prime contractors that conduct SSSPs 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 safeguards and security awareness briefings and are not exposed to security awareness media, the probability of inadvertent disclosure of classified information increases.

Coordinator Qualifications

Many sites rely on a single person to meet the responsibilities of the SSAP coordinator as well as being responsible for presenting all briefings. Therefore, it may be difficult for the coordinator to possess skills, experience, and qualifications to fulfill both functions. For example, 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 combine to make a good briefer. Inadequate training of the coordinator to overcome either weakness can raise additional concerns and directly impact viability of the sites' SSAP.

Planning Activities

- Review formal appointment documentation of a safeguards and security awareness coordinator.
- Determine whether copies of materials (briefings, computer-based programs, etc.) produced to support local SSAPs are periodically updated.
- Review the process used to ensure that completion of briefing requirements is properly documented and recorded. (SF-312, DOE Form 5631.29, and attendance rosters)
- Determine whether subcontractor employees are receiving all required awareness briefings.

Data Collection Activities

Safeguards and Security Awareness Documentation

A. Inspectors should examine policies and procedures to determine whether a structured SSAP has been implemented, whether adequate records are kept, and whether briefing 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. SSAP files and records should be reviewed to determine the adequacy of program documentation and briefing materials. A lack of adequate information, briefing plans, or supplemental awareness material could indicate inadequate management support or budget constraints. If problems exist, inspectors should attempt to determine their causes.

C. Inspectors should determine whether an SSAP coordinator has been appointed, and whether there is adequate guidance on the conduct of briefings, including initial, comprehensive, refresher, foreign travel (when applicable), and termination.

D. Inspectors should determine whether comprehensive briefings are conducted prior to security clearance badges being issued.

Safeguards and Security Awareness Levels

E. Inspectors should interview employees to determine their knowledge of the subjects contained in the SSAP and whether they recall information provided in the briefings and supplemental awareness material. Opinions and perceptions should be solicited to determine

whether safeguards and security awareness is effective and receiving support.

Safeguards and Security Awareness for Contractor Personnel

F. Inspectors should determine by interviews and document reviews whether the operations/site office is providing oversight of contractor and subcontractor SSAPs.

G. A list of security terminations should be compared to badge destruction records and CPCI to determine whether security terminations were affected properly. It may also be useful to compare employee terminations with clearance terminations to ensure all clearances were terminated as appropriate. A list of all terminated cleared contracts and the personnel associated with the contract may also be helpful in determining whether clearances are terminated appropriately.

H. If contractors, subcontractors, or consultants, have established their own SSAP, inspectors should determine by interview and document review whether the operations/site office has provided direction for the implementation of these programs and reviewed contractor and subcontractor program materials.

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.

I. Inspectors should determine what training the awareness coordinator(s) have received, and whether opportunities for training have been denied. Inspectors should also determine whether coordinators are attending DOE/NNSA safeguards and security awareness workshops, as well as local training provided by DOE/NNSA, other government agencies, or contractors.

Performance Test

J. Inspectors should determine the qualifications and performance of awareness coordinator(s) by interview and by attending briefings. It is desirable that the coordinators have DOE/NNSA security experience and be able to speak authoritatively on subjects presented.

This page intentionally left blank.

Section 4.2

Safeguards and Security Awareness Briefings

Contents

General Information

Safeguards and security briefings are at the heart of the SSAP. The types of briefings include:

- **Initial briefings** to 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 matter or SNM.

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

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

- **Foreign travel briefings** are required for all travelers who hold a DOE access authorization and are traveling to sensitive countries. These briefings are normally presented by the local counterintelligence organization, but at some sites, they are under the purview of the SSAP. When this is the case, the conduct of these briefings should be included in the evaluation of the SSAP. Briefing preparations, support materials, and presentation methods should be similar to those supporting other SSAP briefings. However, it is sometimes difficult to ensure that all travelers receive the briefing, and therefore, special emphasis must be placed on the evaluation of site procedures for scheduling and conducting these briefings.

Common Deficiencies/ Potential Concerns

Inadequate Documentation

Written implementation procedures, briefing plans, supplemental awareness materials, and program records reflect how the facility conducts its SSAP. The presence and quality of these materials can indicate whether the program is effective. Without adequate documentation and effective program materials, there is little assurance that employees receive the required safeguards and security information.

Documenting the completion of the comprehensive briefing, normally accomplished on an SF-312, *Classified Information Nondisclosure Agreement,* is of special interest. This level of formality is needed to establish a legally sufficient confirmation that the individual has received the comprehensive briefing prior to being issued a security badge and being granted access to classified matter and/or SNM.

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

Inadequate Briefing Content and Material

In some cases, briefings do not address all required subjects. 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.

At some sites, approved briefing plans, which incorporate all program objectives and ensure that attendees are provided with standard information, have not been kept up to date 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.

- **Initial briefings.** At some 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 SSAP.

  Deficiencies in the initial briefing can result in unauthorized personnel gaining access to classified matter, vital areas, or SNM. 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 briefings.** At some sites, new employees are asked to sign an SF-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 matter. 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 necessary that there be written authorization permitting this individual to sign the SF-312 acceptance block.

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

Also, security 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.

- **Termination briefings.** Terminated 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 off-site 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/NNSA should be notified of the situation.

- **Foreign travel briefings.** For those SSAPs responsible for conducting these briefings, some sites fail to maintain up-to-date travel advisories disseminated by the U.S. Department of State (via their website) and other government agencies. Failure to maintain the current status of foreign country activity could jeopardize both travelers and sensitive information.

Planning Activities

- Review program procedures to determine organizational responsibilities, how briefings are developed and updated, and how completion is recorded.

- Determine when and where comprehensive security briefings are conducted to understand how the program ensures that this briefing is conducted before individuals receive a badge, or have access to classified matter and/or SNM.

- Determine whether all contractors, subcontractors, and consultants are included in the SSAP and, if so, how they receive the required briefings and who monitors the process.

- Review briefings to determine the adequacy of the content of initial, comprehensive, refresher, termination, and foreign travel security briefings.

- Examine samples of supplemental awareness materials used in support of the SSAP.

- Review listings of all employees' grant dates, comprehensive security briefing attendees, and refresher briefing attendees for the past 18 months.

- Review a sample of documentation notifying employees of the requirement to attend specific briefings.

- When applicable, review a list of personnel who have traveled to sensitive countries on official or unofficial travel during the past 18 months and the foreign travel briefings they have received.

Data Collection Activities

Documentation

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

Initial Briefing

B. Inspectors should review the initial security briefing to determine whether all required subjects are included and whether the information is accurate and current. Inspectors may also want to compare the dates of when newly hired employees were issued badges to the property protection area and the dates of receipt of the initial briefing to ensure that initial briefings were given before badges were issued.

Comprehensive Briefing

C. Inspectors should review a random sample of records to determine the interval between the date of the comprehensive briefing—the date the SF-312 was signed—and the date of notification that the clearance was granted.

D. Inspectors should determine whether an SF-312, or some other appropriate form, has been completed by all individuals.

E. Inspectors should review all materials (briefing plans and supplemental awareness materials) to ensure that they adequately support the comprehensive briefing.

Refresher Briefing

F. 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.

G. Inspectors should review records to determine the interval between the initial and refresher briefings to determine whether refresher briefings are provided at least every 12 months, as required, and whether attendance is documented.

Termination Briefing

H. Inspectors should review termination briefing content to ensure that briefings 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, badges are returned, and a DOE Form 5631.29 is signed and forwarded to the servicing DOE/NNSA personnel security organization. PSFs of recently terminated employees should be reviewed to determine whether a termination statement exists, and whether it has been completed, signed, and dated.

I. For off-site personnel, inspectors should contact the security representative or the subcontracting technical representative (often the designated Facility Security Officer) to determine whether termination briefings are being given, badges are being returned, and a DOE Form 5631.29 is signed and returned to the servicing DOE/NNSA personnel security organization. Briefing materials should be examined for content. The contract should stipulate that SSAP briefings are required.

J. Inspectors should reconcile the actual dates of termination of DOE access authorizations with CPCI data to ensure clearance terminations were entered into CPCI within 24 hours.

Foreign Travel Briefing

K. When applicable, 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.

L. 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.

M. Inspectors should review a sample of DOE Forms 1512.2, which are 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.

Performance Tests

N. 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, visual aids, knowledge and enthusiasm of the instructor, and quality of supplemental awareness materials. The inspector should determine whether feedback mechanisms (question-and-answer sessions, tests, etc.) are being employed.

O. Inspectors should determine whether the SF-312s are being maintained as required.

This page intentionally left blank.

Section 4.3

Supplemental Awareness Materials

Contents

General Information

Supplemental awareness materials are maintained to provide continuing reminders to employees of the need to protect classified matter and of other safeguards and security-related employee responsibilities. Supplemental awareness material programs are designed to strengthen employee safeguards and security awareness between annual refresher briefings.

Supplemental awareness materials include: web-based security updates and notifications, facility security newsletters, posters, and various materials (pens, coffee mugs, coasters, etc.) that convey a security message.

Common Deficiencies/ Potential Concerns

A common problem with supplemental awareness materials is that the quality may obscure the content. It is important that these materials be presented prominently, that they be applicable to local safeguards and security-related problems, that they reinforce safeguards and security briefings, and that they be consistent with DOE policies.

Planning Activities

Review existing materials and local procedures to determine how they are developed, updated, and disseminated.

Data Collection Activities

Policies, Procedures, and Files

A. Inspectors should review the procedures for supplemental awareness materials to determine whether they are adequate and meet DOE/NNSA standards. All programs should be reviewed for content, organization, effectiveness, and currency. For example, it is helpful to have a schedule or method in place for changing poster themes. Newsletter files should be examined to determine how often they are distributed, and whether their content is appropriate.

Supplemental Awareness Materials

B. Inspectors should examine posters, videos, handouts, newsletters, and booklets to determine whether they are current, support safeguards and security awareness, and are consistent with briefing content and DOE policy. Inspectors should also determine whether themes relate to safeguards and security problems and agree with DOE policy.

This page intentionally left blank.

Section 5

HUMAN RELIABILITY PROGRAM

Contents

References

DOE Order 3792.3, Chg. 1, *Drug-Free Federal Workplace Testing Implementation Program*
10 CFR 707, *Workplace Substance Abuse Programs at DOE Sites*
10 CFR 709, *Polygraph Examination Regulations*
10 CFR 710, Subpart H, *General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material*
10 CFR 712, *Human Reliability Program*
49 CFR 40, Subparts J – N, *Procedures for Transportation Workplace Drug and Alcohol Testing Programs*

General Information

Pursuant to the Atomic Energy Act of 1954, DOE/NNSA 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 national security.

DOE/NNSA—and the nation—have the highest interest in protecting these facilities and activities from 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, 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, nuclear explosives, facilities, and programs meet the highest standards of reliability and physical and mental suitability.

The HRP is designed to meet this objective through a system of continuous evaluation that identifies those individuals whose judgment and reliability may be impaired by physical, mental/personality disorders, alcohol abuse, use of illegal drugs, the abuse of legal drugs or other substances, or any other condition or circumstance that may be a security or safety concern.

The Human Reliability Program

The HRP applies to all applicants for, or current employees of, DOE/NNSA or a DOE/NNSA contractor or subcontractor, in a position defined or designated under 10 CFR 712 as an HRP position.

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

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

(2) Involves nuclear explosives duties or has responsibility for 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; or

(4) Is not included in paragraphs 1 through 3 above, but affords the potential to significantly impact national security or cause unacceptable damage and is approved pursuant to 10 CFR 712.10 (b).

The certification requirements for enrollment in HRP are accomplished through initial reviews, assessments and evaluations, daily interactions between the employee and supervisor, and recurring annual re-certification reviews, assessments, and evaluations consisting of:

- Supervisory review
- Medical assessment (to include psychological evaluations)
- Management evaluation (to include random drug and alcohol testing, drug and alcohol testing following an occurrence, incident, or unsafe work practice, and for reasonable suspicion.
- DOE security review.

An individual in the HRP must have a "Q" access authorization, which includes an initial special background investigation and a reinvestigation every five years. The AAAP may be used only for security police officers.

Personnel enrolled in HRP are evaluated through a process of continuous observation 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.

Alcohol testing for HRP enrolled employees will be based on the provisions of 49 CFR 40, Subparts J – N, *Procedures for Transportation Workplace Drug and Alcohol Testing Programs.* Drug testing for contractor HRP employees will remain under the provisions of 10 CFR 707, *Workplace Substance Abuse Programs at DOE Sites*. DOE Order 3792.3, Chg. 1, addresses drug testing of Federal employees. Drug and alcohol testing will be random, following an incident, unsafe work practice, for occurrence, and for reasonable suspicion.

Common Deficiencies/ Potential Concerns

Inadequate Communication/Coordination

Communication and coordination between nuclear explosive safety, worker safety, the Site Occupational Medical Director (SOMD), security organizations, and HRP officials 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 PSFs by personnel security specialists. It is important that these files be reviewed to determine whether any security concerns are present that need resolution, and if such information has been forwarded to the SOMD and HRP Certifying Official, as is equally important how those concerns 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 712. This may result from the lack of a systematic method for identifying HRP positions. In other cases this results from pressures either to not delay work by waiting for workers to be

enrolled in HRP or to reduce costs associated with the program.

Another potential concern is failing to enroll individuals who are routinely working in areas that require enrollment. Though sites have protocols that are designed to initiate the enrollment process after a certain number of visits, these protocols are not always followed and individuals continue to have unescorted access without being under HRP continuous monitoring.

A potential problem may exist when an HRP position is vacated then temporarily filled by a person who does not meet HRP requirements but has the required clearance. In some cases, action is not taken to enroll these individuals. This can be a particular problem for physical security systems and material control and accountability positions.

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. In addition, it may result in unidentified HRP positions. 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 or positions within that organization.

Outdated HRP Implementation Plans

The HRP plans are to be updated unless the manager states that there have been no substantial changes to the program and that the manager accepts (extends) the current plan.

Inadequate HRP Drug Testing Program

In carrying out the drug and alcohol testing program, sites might not have a methodology that ensures random selection and testing, and provides effective detection and deterrence. For example, some organizations select individuals to be tested two or more weeks in advance of testing. This allows the passage of a significant amount of time between selection and testing, which could result in either an intended or inadvertent disclosure of who had been selected and when the test is scheduled to take place. With this information, an individual could make himself/herself unavailable on the test date or provide a substitute/adulterated sample to avoid detection of drug or alcohol use. The best method for providing the maximum capability to detect and deter is selection and testing on the same day. Individuals working the evening and night shifts must have an equal probability to be selected as individuals working during the day shifts.

Another concern is that some sites have developed selection algorithms that significantly reduce the probability of selecting individuals who have already been tested to meet the annual testing requirement. In other cases, individuals who have been tested multiple times are being removed from the testing pool until after re-certification. In either case, individuals might become aware of these practices, thus impacting the detection of illegal drug use or the abuse of alcohol. Such practices continue because of the temptation to reduce the cost of the drug and alcohol testing program or to reduce the impact on work schedules due to multiple tests for HRP certified employees. This temptation must be resisted, otherwise the site drug and alcohol testing program will not be effective and will not provide the intended benefits to the site protection program.

Inspectors might find that some sites may not have a process for conducting tests for reasonable suspicion, following an occurrence, incident, or an unsafe work practice. This may be a result of inadequate training of supervisors and employees. More often, the problem exists because the sites have not developed lines of communication among safety and security organizations, and/or sites may not have developed specific criteria that would help individuals determine when testing should occur. Regardless, HRP training programs must emphasize the need to test whenever a suspicion arises regarding drug use or

alcohol abuse for HRP personnel both off duty and on the job.

Inadequate HRP Medical Assessment

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

HRP medical officials may not have been trained to properly identify and report security concerns. In some cases, HRP medical officials are not reporting or recommending temporary removal to the HRP Management Official when a medical restriction has been placed on a HRP-certified employee or when security concerns are developed as a part of the medical assessment. This may result in HRP employees having access to the material access area and SNM while no longer being suitable to perform HRP duties. These security concerns are often not reported to the HRP Management Official or to the DOE/NNSA personnel security organization.

Sometimes diagnosing alcohol abuse can be complex, depending on the circumstances and the evidence that is available to medical officials. Therefore, medical examinations must be thorough and consistent, especially in cases when test results indicate elevated liver enzymes. Specific actions should be taken to rule out an alcohol problem when there is no other medical reason for the elevated liver enzymes. Failure to treat each case in the same manner could lead to perceptions of favoritism or unfairness. Equally important is that inconsistent or inadequate examinations could allow individuals who abuse alcohol to perform HRP duties while they do not meet the required reliability standards.

The medical staff at some sites does not always refer to the job/task analysis (JTA) when assessing employees who are seeking HRP certification or recertification. If the medical staff is not familiar with the JTA, then the impact of a medical or mental condition may not be adequately considered concerning an individual's ability to perform HRP duties. The JTA should be readily available to the medical personnel or psychologist or be placed in the files to ensure its availability each time the individual is seen.

Inadequate Implementation of the 8-hour Alcohol Abstinence Requirement

Individuals performing nuclear explosive duties and other positions designated by the Manager are prohibited from consuming alcohol within an eight-hour period preceding any unscheduled tour of work and during the normally scheduled period of work. Consequently, management is required to develop procedures to ensure the fitness of persons called in to perform an unscheduled working tour that involves nuclear explosives. In addition, management must implement a process to ensure that all nuclear explosive duty positions are identified. Failure to develop these procedures could potentially allow an unfit individual to perform nuclear explosives duties.

Inadequate HRP Training Program

Training is one of the most important ingredients in a successful HRP. Persons in HRP positions are required to receive initial and annual instruction and must fully understand their program responsibilities. Supervisors must be trained to identify aberrant behavior and to take appropriate action. In addition, medical officials must be trained to understand the impact of medical and mental conditions on the performance of HRP duties and report these conditions to the HRP Management Official. At some facilities, some first-line supervisors, HRP personnel, and medical officials have not received adequate training and do not fully understand their responsibilities.

Improperly Conducted HRP Reviews, Assessments, and Evaluations

If managers, supervisors, 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.

Supervisors might not have sufficient interaction with employees or may supervise too many employees so they can not realistically complete the annual supervisory review and/or report each observed safety or security concern to the HRP Management Official.

Another potential concern is that some sites may not share derogatory information with the SOMD or HRP Certifying Official, even though this exchange is now authorized. Not sharing all information with the SOMD or the certifying official may affect the analysis and ultimate resolution of a potential concern. Therefore, individuals may not be temporary removed from performing HRP duties when warranted.

Inadequate System for Documenting and Maintaining HRP Data

Some facilities lack a system for documenting or maintaining appropriate data on HRP employees, such as evaluations, medical restrictions, reporting of prescribed medications, certification, 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 and Documenting of Medical Issues

Some sites may not have established adequate lines of communication between the medical officials and the HRP Management Official that ensure timely reporting of medical restrictions that may impact the performance of HRP duties. Further, medical officials may not have documented their concerns to clearly indicate to the HRP Management Official how a medical condition can impact the performance of HRP duties. In other cases, the medical officials might not have recommended to the HRP Management Official that an individual needs to be removed.

Frequently, sites do not enforce established mechanisms for reporting prescribed medications. The medical staff might not always be determining the affects of prescribed medications on the cognitive ability of HRP employees. Many opiate-based medications do affect cognitive ability and individuals taking such medications should be assessed for potential temporary removal from HRP. Sites must also take care that their reporting mechanisms include the reporting of prescription medication use during off-shift hours.

Inadequate Reporting of HRP Concerns

Because 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 reported to the SOMD, HRP management, or certifying official. In some instances, the concern may overlap and there could be a security concern that might go unreported. The implementation plan should clearly stipulate the procedures that are in place to accomplish the exchange of information between safety, security, and HRP program officials.

Planning Activities

- Determine the status of the facility HRP program, including a review of all current HRP positions (and the associated job task analyses), how long personnel have been in these positions, and all personnel pending initial certification.

- Determine whether the facility has a random drug and alcohol-testing program, and, if the program includes testing for reasonable suspicion, following an occurrence, incident, and unsafe work practice, chain-of-custody procedures, unannounced selection and testing procedures, how employees are notified for testing and how this is documented, procedures and documentation for employees selected for testing, but not tested, and availability of all materials required to effectively conduct the tests.

- Determine if the site has a process in place for the immediate removal of individuals who test positive for illegal drugs or alcohol use.

- Determine whether the enrollment process ensures the identification of all individuals who have used any hallucinogens during the last five years or any HRP-certified employees who have experienced a flashback from the use of any hallucinogens.

- Determine whether the facility has an alcohol testing program, whether the technicians are certified, whether their equipment is approved by the Department of Transportation, whether materials are in place for an effective program, whether procedures are in place to ensure that all who test 0.02 or greater are sent home, and if concentrations are above 0.04, whether additional actions are taken to determine whether the consumption occurred on the job.

- Review the list of individuals designated as having to abstain from alcohol consumption for the eight hours prior to reporting for work and determine whether all required individuals have been designated.

- Review training materials (including instructor guides and student handouts), and determine whether a training program is in place for instructors, managers, supervisors, medical officials, and HRP personnel.

- Determine whether managers, supervisors, and HRP personnel receive awareness training in the recognition of aberrant behavior every 12 months.

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

- Review procedures for immediate or temporary removal and determine whether there are protocols that allow escorted access for individuals who have been removed. In addition, determine if the removed individuals have also been removed from the access control system for the material access area or areas that store or possess nuclear weapons, components, or SNM.

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 a system is in place for identifying all positions. 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 material access area access records to determine if there are individuals who are accessing the material access area frequently, but are not HRP-certified. A list of all individuals entering the MAA who are not HRP certified should be reviewed. This list should also be compared to all individuals who are pending HRP certification.

C. Inspectors should review site plans, policies, and procedures to confirm that they provide for drug testing; alcohol testing; actions

in response to positive drug and/or alcohol test results; supervisory reviews; medical assessments; management evaluations; security reviews; approval authority notification procedures; sharing of information among the SOMD, HRP Management Official, and the HRP Certifying Official; immediate and temporary removal; termination procedures; and an effective program for maintaining appropriate data on HRP positions.

HRP Training Program

D. 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 initial and annual refresher training and are aware of their responsibilities, especially in reporting unusual conduct. Additionally, inspectors should determine whether medical personnel that support HRP have received training concerning program objectives and their roles and responsibilities, and are knowledgeable of what medical/mental conditions also constitutes a security concern and the requirement to report these conditions to the HRP Management Official.

E. 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 and observe the completion of duties. The testing of staff and personnel supporting the HRP may also be utilized to determine the effectiveness of training.

HRP Drug/Alcohol Testing Program

F. Inspectors should review drug and alcohol testing procedures and inspect the materials used to conduct the tests. It may be helpful to have individuals responsible for conducting drug/ alcohol testing explain the processes step by step. For drug testing, 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.

G. Inspectors should observe both drug and alcohol testing performed 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, unannounced basis, whether individuals selected for testing arrived with two hours of notification, and review the procedures for alcohol testing when individuals are called in for unscheduled work. Inspectors should review a sampling of any positive drug and alcohol tests to ensure appropriate actions were taken, including timely reporting.

H. 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. Inspectors should also review the process for testing employees for reasonable suspicion, following an incident, unsafe practice, or occurrence, including determining how information is communicated among supervisors, and the safety and security organizations. If some employees have not been tested, determine why they were excluded. Inspectors should determine whether there is consistency in testing for these reasons and whether reasons for conducting these types of testing are well known and specified in written procedures.

I. Similarly, records should be reviewed to determine whether individuals in designated positions that prohibit the consumption of alcohol eight hours prior to reporting for work are sent home if they test 0.02 or greater, and whether additional tests are conducted if they test greater than 0.04.

Individuals returning to work after testing positive should be re-tested, with results determined at less than 0.02 before being allowed to perform HRP duties. This should be a part of the reasonable suspicion test procedure.

HRP Reviews and Evaluations

J. Inspectors should examine the HRP evaluations to determine whether all parts have been completed annually, including supervisory review, medical assessment (including if the JTA was used and is adequate), security review, 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. Recertifications must be completed with 12 months of the last certification or recertification date.

K. 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 and whether the action was taken in a timely manner.

Maintaining HRP Records and Files

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

Reporting Requirements

M. Inspectors should determine whether a full understanding exists between the site's HRPmedical officials (psychologists, physicians, and physician's assistants, etc.), the DOE/NNSA site office, and the DOE/NNSA personnel security organization as to what is a reportable HRP concern.

Performance Tests

N. 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.

O. 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.

Section 6

UNCLASSIFIED VISITS AND ASSIGNMENTS BY FOREIGN NATIONALS

Contents

References

DOE Order 142.3, *Unclassified Foreign Visits and Assignments*
DOE Notice 205.2, *Foreign National Access to DOE Cyber Systems*

General Information

In the conduct of DOE/NNSA operations, Federal and contractor facilities often host unclassified visits and assignments by foreign nationals. DOE/NNSA and its international partners benefit from the exchange of information that results from a managed process of unclassified FV&A. However, DOE/NNSA and contractor organizations that host foreign nationals must ensure that the potential threat that these foreign nationals represent to sensitive information, classified matter, and SNM is thoroughly analyzed and mitigated. The analysis must consider whether there is a risk due to the proximity of foreign nationals to these security interests. The analysis should be based on the foreign nationals' ability to observe operations or security measures in addition to the risk of their unauthorized access. It is DOE policy that counterintelligence interests, security interests, and sensitive subject information and technologies be protected in a manner consistent with program requirements, including compliance with export control laws and regulations. DOE has established a set of requirements that if properly implemented will meet these protection requirements. The references above contain these requirements and, in conjunction with approved local procedures, provide direction towards their implementation.

Common Deficiencies/ Potential Concerns

Inadequate Notice

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

Passport, Visa, and Immigration and Naturalization Service Information

In addition to the information required to be collected for DOE/NNSA-sponsored visits, all sites, facilities, and laboratories must collect from all foreign national visitors and assignees sufficient passport, visa, and Immigration and Naturalization Service information for review and documentation in the Foreign Activities Central Tracking System (FACTS). This is being done to verify identify, to verify authority to work, and to ensure that the foreign national is currently eligible to be in the United States.

Inadequate Security Plans 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 involving foreign nationals from sensitive countries, thereby setting the stage for possible compromise of DOE/NNSA security interests. In some cases, site security plans or SSSPs are used as substitutes for a generic security plan. However, these plans do not provide adequate control measures for foreign initiators and assignees. 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/NNSA site or facility by a foreign national from a sensitive country. Though most sites develop a more detailed security plan, they sometimes do not meet all the generally accepted requirements of a security plan in that all security interests and protection measures are not identified, and actions to address unmitigated potential security concerns are not included. Special care must be taken to consider security interests that are adjacent to the areas to which the foreign national has access. At some sites, foreign nationals can gain visual access of security operations that must take place outside. These types of operations should be taken into consideration and may result in temporary restrictions on the movements of visiting foreign nationals. Specific security plans can also benefit by the inclusion of a diagram depicting the location of security interests along the route on ingress and egress that the foreign national will be using during the visit or assignment. In some cases, there is no record that the applicable security organization has reviewed the security plan.

Inadequate Communications

Ineffective communications between the various site organizations often lead to a lack of control and oversight of foreign nationals. The worst-case scenario is when a visit occurs with no communication or coordination between the host and the FV&A organization. The fact that these "unapproved" visits still occur at DOE/NNSA facilities emphasizes the need for continued efforts by the FV&A organization and line management to ensure that all employees know and understand the requirements for properly hosting foreign national visitors.

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 FV&A 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 national visitors/assignees sometimes lack sufficient detail to ensure that the plans can be implemented. Another potential concern results from the failure to coordinate with the protective force to ensure that after-hours patrols include checks on foreign nationals that are authorized late working hours, and the failure to inform all employees in organizations and offices that are in proximity of foreign nationals.

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 workstations and computer networks, which could allow them to compromise DOE/NNSA security interests. Security awareness on the part of hosts, escorts, and other individuals in the facility must be maintained.

Inadequate Host Actions

Though recent inspection experience has shown that hosts are knowledgeable of applicable requirements and their responsibilities, hosts do

not always 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. Host 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 closed out.

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

Another potential concern can arise if the host is not assigned to the facility or location where the foreign national visit or assignment will occur. In these cases, it is strongly advised that a manager or employee with full knowledge of facility security interests and measures be formally identified as an additional host. This individual can assist in ensuring that adequate control measures are in place throughout the duration of the visit or assignment and can assist in escort training.

Inadequate Computer Access Controls

Determining the implications of allowing foreign national visitors and assignees access to computer systems is a matter for review by the Office of Cyber Security Evaluations (HS-62) cyber security team. However, visitor and assignment requests and security plans may not have considered or identified which computer systems the visitor or assignee will be permitted to access and whether access will be during normal duty hours or after-duty hours. After-hours access presents special concerns when other computer workstations are accessible by the foreign national and are not password protected. A particular problem occurs with foreign personnel who are provided access to computer networks and are not stationed on site. Personnel security inspectors reviewing the FV&A program should ensure that risk assessments and required security plans have been developed and approved. Changes in computer access should also be reviewed to ensure coordination with cyber security. Inspectors should also determine whether the site has a process in place to ensure that cyber access does not extend beyond the term of the visit or assignment or when access is no longer needed, regardless of the reason.

Foreign Access Central Tracking System

Over the past several years, much effort has been placed on ensuring that the information contained in FACTS is current and correct. Recent inspection results have concluded that most DOE/NNSA sites are achieving a greater degree of success in accomplishing this objective. However, some problems have been noted. One of the most common problems is failure to validate that automatic uploads into FACTS have been successful. When validation is not being done, inadequate or incorrect information can reside in FACTS for an extended period of time before discovery. Another persistent problem is that some of the software programs that have been developed to upload information into FACTS from local databases may not ensure that all required information is uploaded. Correction of this problem often requires manpower-intensive solutions until the software can be modified. In many cases the resources to modify the software have not been identified and can cause these manpower intensive solutions to be needed for an extended period.

Jointly Staffed Facilities

There are several DOE/NNSA sites that reside in or share facilities with other government agencies or private companies. Under these circumstances, is it important to establish lines of communications to ensure that when foreign nationals visit either organization, appropriate steps are taken by all parties to protect security interests. Once the lines of communications are established, the DOE/NNSA FV&A program manager should share DOE requirements for hosting foreign visitors and obtain the other party's requirements for hosting foreign nationals. It might be necessary for each party to review and approve requests for foreign visits or

assignments. Another possible procedure to consider between the parties would be a joint FV&A committee.

Planning Activities

- Review local procedures for requesting, processing, and approving visits and assignments by foreign nationals.
- Determine whether adequate controls are in place regarding the issuance of site-specific and DOE security access badges and proximity badges to foreign nationals.
- Review the procedures for escorting foreign nationals.
- Identify all facilities on the site involved in hosting/escorting foreign nationals for the past 18 months.
- Determine the number of visits and assignments by foreign nationals during the past 18 months, including the dates of each visit or assignment and the names of the hosts.
- Review any counterintelligence inspection reports that have been conducted.

Data Collection Activities

Plans and Procedures

A. Inspectors should determine whether the site has a comprehensive and integrated approach to FV&A. This would include review of a sample of request forms and specific and generic security plans to determine whether the elements required by DOE Order 142.3 are covered. A random sample of visit requests should be examined to determine whether they are timely and complete, and have the appropriate level of approval. 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. If deficiencies are noted, it may be prudent to review additional visit requests.

It should be determined whether individual and organizational roles and responsibilities are clearly understood and whether an integrated approach exists to assessing the risks to classified and sensitive information that 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 that an appropriately detailed plan has been developed that incorporates all required security considerations and administrative processing requirements.

Host/Escort Procedures

B. Inspectors should examine host/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 hosts/escorts. Additionally, hosts/escorts should be interviewed to determine their knowledge of and adherence to program requirements. Inspectors may want to determine whether similar interviews are conducted during periodic safeguards and security surveys self-assessments and counterintelligence inspections.

Coordination

C. Inspectors should interview site OPSEC, Counterintelligence, Classification, and Export Control personnel to determine the existence of an effective and integrated approach for assessing risks to classified matter and sensitive information prior to approval of the visit or assignment. Inspectors should also determine whether the results of the coordination are included in the security plans. The cyber security topic team will interview their points of contact concerning the actions taken by the site cyber security organization to assess the risk in authorizing access to site computing assets and

should provide the results of these discussions to the personnel security topic team.

Host Reports

D. Inspectors should review a random sample of host reports to determine whether they were timely, complete, and forwarded to the appropriate program official. If deficiencies are noted, it may be prudent to review additional host reports.

Security Plan Data

E. 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

F. 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

G. Inspectors should conduct a performance test(s) of the unclassified FV&A elements, such as:

- Interview a representative sample of individuals who acted as hosts or escorts for a selection of non-sensitive and sensitive visits and assignments conducted during the past 18 months. Determine each host/escort's knowledge of the specific security plan and the responsibilities pertaining to the visit. Inspectors should conduct a walk-through of the security plan to determine its accuracy and completeness, and review access control procedures into the security area.

- Interview any visiting foreign nationals that are on site to determine their knowledge of authorized access and their responsibilities.

- Conduct walking tours of areas that have or are hosting foreign nationals during normal working hours to determine if other personnel in the area are aware that foreign nationals are present and if the personnel are aware of their responsibilities to protect government information and property.

- Also conduct tours during after hours to determine if the foreign national can gain access to unauthorized areas and if DOE security interests are properly secured.

This page intentionally left blank.

Section 7

INTERFACES

Contents

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 inspection.

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 HS-60 inspection report. This strengthens the overall HS-61 capacity to provide significant value-added contributions to the safeguards and security community as well as to the DOE/NNSA 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.

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. Early and continuing integration helps 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, other topic teams may assist in the identification of individuals who are performing duties that require enrollment in the HRP. Also, inspection teams from all other topic areas can be asked to check for, and report on, supplemental awareness material in areas that the personnel security topic 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.

Consequently, 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.

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 topic team may be able to elicit and provide information on 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.

The PPM topic team's review of the survey and self-assessment programs may provide data relative to the status of personnel security program effectiveness as viewed by the inspected site's security organizations. Conversely, the personnel security topic team may be able to provide information on the status of corrective actions taken to address survey or self-assessment findings.

The PPM topic team should be consulted concerning insider analysis that is part of the vulnerability assessment process. Of special interest is validation that all HRP positions are being appropriately modeled and analyzed.

Operations Security and Cyber Security

At many sites, SSAPs incorporate OPSEC, cyber security, communications security, and other security components into their safeguards and security awareness briefings. Inspection teams evaluating these areas can provide information on briefings' effectiveness, thereby assisting in the overall evaluation of safeguards and security awareness. Additionally, the cyber security topic team can address foreign nationals' access to computer systems, especially networked systems. Such assistance should be coordinated during the planning meeting.

Classified Matter Protection and Control

The CMPC topic team can provide information relative to a site's administration of the incidents of security concern program. Using incident data, the personnel security topic team can assure that reports of incidents are filed in an individual's PSF and, when appropriate, considered in the determination of an individual's continued eligibility for access. Identified incidents 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 topic team) can be used to identify potential access to this data by foreign national visitors and assignees.

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

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 national visitors and assignees, are permitted access only to approved areas.

Visitor access control procedures typically include issuing and retrieving 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.

The DOE visitor control program addresses security concerns raised by visits and technical exchanges by universities, private industry, other governmental agencies, and foreign governments. Cleared and uncleared visitors gain access on a daily basis to some of the nation's most sensitive facilities engaged in various activities. Visitors may be conducting unclassified work or working on classified projects with an 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 concerns.

Careful planning is also advised when classified areas have been redefined, since the end result may increase rather than decrease the need for access authorizations.

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 or SNM. 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.

Protective Force

The protective force topic team may be useful in assisting the personnel security topic team in determining whether protective force post orders contain current and accurate information relative to foreign nationals in a particular area.

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

This page intentionally left blank.

Section 8

ANALYZING DATA AND INTERPRETING RESULTS

Contents

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, action on suspending clearances, and 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.

Personnel Security Clearances

Requests for clearances are certified at the DOE office or contractor facility (that is, certified to ensure that the duties of a position require access to classified matter or 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 clearance is terminated when the need for it no longer exists.

Because the security clearance process is a costly, resource-intensive effort, significant deficiencies in handling initial requests 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 pre-employment check program that does not assure proper completion of all paperwork submitted with requests for access authorizations may prevent or significantly delay processing. This process should be carefully examined as a potential root cause, since the time consumed by personnel security specialists in rectifying errors in pre-employment checks has a considerable impact on budget and personnel resources.

If pre-employment checks do not meet the requirements of the DEAR, there is no assurance that available derogatory information will be forwarded to the DOE/NNSA personnel security organization to alert or assist the investigative agency in scoping its investigation.

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

Failure to screen and analyze results of personnel security investigations in a timely manner can also have serious impacts on organizations requiring cleared personnel, and on the quality of the process of granting clearances. 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 clearances to unreliable individuals, or the denial of access to reliable and valuable individuals.

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

Safeguards and Security Awareness

Management support and adequate documentation are essential to the success of the SSAP and should weigh heavily in evaluating the overall program. An inadequate SSAP can increase the potential for inadvertent compromise of classified matter. Deficiencies are particularly significant if the information security or physical security systems topic teams find that classified matter is not being adequately protected. If the SSAP 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.

Security briefings are the heart of the SSAP. 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 receipt of such information is acknowledged and documented.

Supplemental awareness materials 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 matter, and maintaining safeguards and security awareness between annual refresher briefings.

A lack of experienced, skilled coordinators can degrade the effectiveness of the SSAP, thereby affecting safeguards and security awareness and the overall security posture of the facility.

Unclassified Visits and Assignments by Foreign Nationals

DOE/NNSA 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 security interests if the procedures in DOE directives are effectively implemented and enforced. Otherwise, foreign nationals may gain unauthorized access to classified matter or sensitive information.

Human Reliability Program

A facility may cite enrollment of certain staff in the HRP as the primary factor for mitigating the potential insider threat and, therefore, consider existing risks 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 physical security system, protective force, or procedural measure 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.

When evaluating the facility's implementation of the HRP, all program elements must be in place and effectively implemented for the residual insider threat to be mitigated. The benefits of an active enrollment process can be rendered useless if all required individuals have not been identified and enrolled. Drug and alcohol testing programs are important for the success of an HRP; however, if testing is neither random nor adequately controlled, then overall program effectiveness is impacted. 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.

Consideration of Integrated Safeguards and Security Management Concepts

As discussed in Section 1, ISSM 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, HS-60 inspectors should review the results (both positive aspects and weaknesses/findings) of the review of the protective security topic in the context of the ISSM 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 safeguards and security awareness could occur if line management had not placed sufficient priority on safeguards and security awareness functions and has not provided adequate resources to implement an effective SSAP. 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.

Appendix A

DATA COLLECTION AND ANALYSIS TOOLS

Contents

The following tools and forms may help inspectors systematically plan and schedule topic activities, request site personnel security program documentation, and record and evaluate the effectiveness of individual elements of the personnel security program. These tools and forms can be used at the inspector's discretion. However, it must be remembered that use of these tools and forms will have to be tailored for each inspection, and some tools and forms may require revision in response to new or modified U.S. Department

of Energy (DOE) direction. The tools and forms are arranged to support an inspector through all phases of the inspection process.

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.

PERSONNEL SECURITY PROGRAM PERFORMANCE MEASURES

PROGRAM MANAGEMENT

Management commitment and support is evidenced by:

1. All elements of the personnel security program are effectively implemented as indicated by the results of self-assessments, surveys, independent oversight inspections and other DOE or external agency reviews (e.g., Inspector General [IG] and Government Accounting Office).

2. Self-assessment and survey programs are identifying and correcting program weaknesses.

PERSONNEL SECURITY CLEARANCE PROGRAM

Protection of classified matter and special nuclear material is assured by:

1. Pre-employment checks have been completed for all employees requiring a security clearance.

2. All potentially disqualifying/derogatory information (identified by pre-employment checks, investigatory agencies, self-reporting, reports of security infractions and violations, results of IG and employee concerns program investigations, other independent sources [supervisors, fellow employees, local law enforcement agencies, etc.]) has been reported to the applicable DOE/National Nuclear Security Administration (NNSA) personnel security organization.

3. All potentially disqualifying/derogatory information has been appropriately adjudicated (and the rationale for all adjudicative recommendations and decisions is fully documented).

4. Clearance termination/suspension actions, to include coordination with applicable DOE/NNSA line managers and contractor managers, are completed in a timely manner (days) so as to prevent unauthorized access to classified matter and special nuclear material by the return of all security badges and appropriate data entry in the local access control/badge databases and the Central Personnel Clearance Index (CPCI).

5. The accuracy of information contained in CPCI and local personnel security and access control/badge databases prevents unauthorized access.

HUMAN RELIABILTY PROGRAM

The insider threat has been mitigated by:

1. All positions meeting the requirement for enrollment have been identified and communicated to applicable mangers and supervisors.

2. All individuals filling Human Reliability Program (HRP) positions have received all required evaluations, approvals, and training prior to performing duties.

3. The HRP Certifying Official and/or the HRP Management Official have been notified of all potentially disqualifying concerns (security infractions, results of drug and alcohol tests, prescription of medications, results of IG or employee concerns investigations, observations of supervisors and fellow employees, safety, etc.) and have taken appropriate action to continue, temporarily remove, or remove the individual from the HRP. (If notification of concerns is not occurring, evaluate training for supervisors and incumbents.)

4. The HRP Certifying Official and/or the HRP Management Official ensure that timely action is taken to prohibit unauthorized access when an individual has been temporarily removed or removed from HRP, to include the return of all security badges, and appropriate data entry in the local access control/badge databases and CPCI.

5. All HRP individuals are re-certified every 12 months and have been randomly selected and tested for drugs and alcohol at least once every 12 months.

6. All individuals performing nuclear explosive duties and those individuals selected by either the Manager or the NNSA Administrator have been formally designated, and these designations have been communicated to the individuals and applicable managers and supervisors.

7. Managers and supervisors prevent (through adherence to formal procedures) designated individuals from performing unscheduled work when they have been asked and indicate that they have consumed alcohol within the preceding eight-hour period.

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

Employees have been fully prepared to support an effective protection program by:

1. Cleared employees and support contractors demonstrate that they are knowledgeable of their individual security duties and responsibilities by achieving at least a score of 85 percent on the independent oversight questionnaire.

2. All awareness program briefings and supplemental materials are accurate and up to date.

3. Access to classified matter or special nuclear material is not authorized prior to completion of all program requirements (initial and comprehensive briefings).

4. For all of those no longer requiring access to classified matter or special nuclear material, termination briefings are conducted, badges are retrieved, and appropriate data entries are made in the local access control/badge databases.

UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS

Potential risks represented by foreign national visitors and assignees have been minimized by:

1. There has been no unauthorized access/unintentional disclosure of classified matter, special nuclear material, and/or sensitive unclassified information/technology (including Cooperative Research and Development Agreements and export control information).

2. All required reviews and approvals have been completed (i.e., security, counterintelligence, export control, cyber, Operations Security [OPSEC], classification, others), and security plans have been developed and communicated prior to the start of the visit or assignment.

3. All incidents of security concern related to the hosting of a foreign national have been reported to DOE/NNSA, which indicates that hosts and escorts are knowledgeable of their duties and responsibilities.

PERSONNEL SECURITY DETAILED INSPECTION PLAN

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
MANAGEMENT: Does management ensure that the personnel security program represents a logical and cost-effective approach to protecting against the insider threat? Is senior management support evidenced by proper funding and personnel security program resources, and by support for recommendation to suspend or revoke clearances? **IMPACT:** Since the human element may represent the weakest link in any protection program and the greatest threat, it is important that management recognizes the significance of an effective personnel security program. This threat is realized through an insider who has authorized access that effectively bypasses some elements of protection systems and who may have extensive knowledge of a facility.			
Management: Line management responsibility for safeguards and security is exhibited by management's recognition of the significance of an effective personnel security program.	1. Have self-assessments, surveys, and/or inspections identified systemic deficiencies concerning delays resulting from processing unnecessary access authorization requests, minimal participation in the security awareness briefings, and lack of proper visitor control? 2. Are there sufficient personnel to avoid an excessive workload for the personnel security specialists? 3. Is the assignment of secondary duties impacting the performance of the personnel security program? 4. Have the number of assess authorizations been reduced to the least possible number to still meet operational requirements? 5. Are there sufficient funds in the budget to support retention of adequate staff and for training?	1. Review corrective action plans to determine the time required to address identified program weaknesses. 2. Conduct interviews and review records to determine the extent of any backlogs impacting program implementation. 3. Review records to determine the number and type of additional duties. 4. Interview managers to identify budgetary impacts on program implementation, especially the granting of initial access or to conduct reinvestigations. Also determine the amount of paid and unpaid overtime granted during the past year. 5. Obtain information to determine the number of program actions processed each month and how the organization would be able to respond to surge situations 6. Review records to determine the number of personnel assigned against the number authorized. 7. Interview and review records to determine whether	pre-planning pre-planning and on-site pre-planning on-site pre-planning pre-planning

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		an action plan exists for the review and elimination of access authorizations.	on-site
Management: Personal competence and training is maintained by management making adequate resources available to perform all personnel security program functions.	1. Is the basis used by the Safeguards & Security Director to assert that individuals performing personnel security functions are technically competent sufficient? 2. Has the level of turnover of personnel security specialists impacted the program? 3. Is there a structured program (on-the-job training [OJT] program, desk-side procedures, mentoring, etc.) for preparing new personnel for duties as a personnel security specialist?	1. Interview the Safeguards & Security Director or person responsible for the training of the personnel security professionals to determine whether the program has been formalized, if it is based on a needs and job task analysis, and whether lesson plans have been developed to support locally developed training. 2. Interview personnel security program managers or professionals to determine their satisfaction with the training program (continuing and new hire). 3. Review position descriptions to verify that responsibilities are actually reflected at the individual's level. 4. Interview/review records to determine the turnover in personnel security professionals, and what program is in place for new hires.	on-site on-site pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Management: Program direction, plans, and records are supported by personnel security program representatives' involvement in the development of plans to analyze and mitigate the risk represented by insiders, and/or to determine the level of assumed risk. Management ensures that personnel security plans, policies, and priorities are adjusted to meet changing threat situations.	1. Are personnel security concerns adequately addressed in the site operational and security planning processes? 2. Does personnel security professionals' participation in threat analysis studies, management-level meetings, and budget allocation deliberations lead to personnel security program issues not being identified, analyzed, and addressed? 3. Are personnel security program plans and procedures sufficient (accurate and comprehensive) to support the successful implementation of all elements of the personnel security program?	1. Interview managers and personnel security professionals to determine the extent personnel security professionals participate in planning meetings, budget discussions, and management-level decisions. 2. Review the Site Safety and Security Plan (SSSP), and other security and operational planning documents to determine the manner in which personnel security concerns are addressed. 3. Review site policies to determine whether personnel security program officials are in a position to ensure compliance. 4. Interview/review records to determine whether any program weaknesses are due to a lack of authority over operational elements to implement requirements (including corrective action plans). 5. Review site personnel security program procedures to determine whether they are accurate and comprehensive. 6. Interview managers to determine what incentives are used to encourage good performance.	on-site pre-planning pre-planning on-site pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Management: Feedback and improvement is supported by effective self-assessment and corrective action programs.	1. Has the self-assessment program identified significant program weaknesses that when addressed would materially enhance program implementation? 2. Does the corrective action process include all the required elements (analyze root cause and prioritize actions, establish corrective action schedule that will allow monitoring progress, assign responsibility for each action to a specific individual, continually update the plan, and ensure adequate resources are applied) to ensure that identified weaknesses are addressed in the most effective and efficient manner?	1. Review past self-assessments to determine whether they reflect thorough coverage of the personnel security program, and are conducted on a regular basis. 2. Review records to determine who conducts the self-assessments and their qualifications. 3. Review records to determine whether concerns identified during self-assessments are entered into a central tracking system. 4. Review procedures to determine whether the corrective action process contains all the required elements. 5. Review records to determine whether some form of independent verification of closure of findings is in place.	pre-planning pre-planning pre-planning pre-planning pre-planning
PERSONNEL SECURITY CLEARANCE: Are only the most demonstrably reliable and trustworthy (free of un-adjudicated derogatory information) individuals determined to be eligible and therefore granted access to classified matter and/or special nuclear material? Is the process used to determine eligibility credible and timely? **IMPACT:** Flaws in the process to determine reliability and trustworthiness undermine the first line of defense against the insider threat.			

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Clearance: Request process (type of access authorization) ensures that the type of access authorization is appropriate.	1. Is the system in place sufficient to ensure the proper and timely review of access authorization requests? 2. Are all of the key elements in place to process requests? • Certification that the request is justified? • Adequate procedures to ensure that the requested type of access authorization is appropriate? • A tracking system to ensure that access is terminated when it is no longer needed? 3. Is management support for this process evident? 4. Does the overall number of clearances indicate a lack of control and scrutiny?	1. Review site procedures and interview program personnel to determine how the process is conducted. 2. Review a sample of security files to evaluate whether local criteria for justifications are being used consistently. 3. Interview program personnel on how they make a determination of the appropriateness of the requested type of access authorization. 4. Compare positions requiring access to the number of individuals currently holding authorizations to determine whether all are justified. 5. Review a list of terminated contractor and subcontractor personnel to determine whether timely action (updating of CPCI and retrieval of badges) was taken. 6. Interview supervisors to determine whether they understand the relationship between duty positions and clearances.	pre-planning and on-site on-site on-site on-site pre-planning on-site
Clearance: The contractor pre-screening program provides DOE all identified derogatory information.	1. Does the contractor pre-screening program ensure that all paper work is complete? 2. Does the contractor pre-screening program eliminate all errors? 3. Does the contractor forward all identified derogatory information to DOE?	1. Compare recent access authorization requests with the personnel security files associated with these requests to determine whether they are consistent. 2. Through interviews and document reviews determine how many access authorization requests were not forwarded due to the identification of derogatory information by the contractor. 3. Review records to determine how many requests were returned to the contractor for correction or for additional information.	on-site pre-planning and on-site pre-planning

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Clearance: DOE screening and analysis support the action taken (grant, disapprove, or send to Office of Personnel Security) concerning a request for access authorization. The contractor badge program ensures that badges are issued only after a clearance is granted and awareness requirements have been completed.	1. Are the results of investigations screened and analyzed in a timely manner? 2. Are individuals charged with the task to complete the screenings and analyses trained? 3. Is the screening and analysis function supported by local procedures, and do these procedures ensure that these activities are completed accurately, efficiently, and in a timely manner? 4. Is all derogatory information and are all discrepancies identified during screening and analysis? 5. Is sufficient data documented to support all adjudicative recommendations and procedures? 6. Does the contractor organization inform DOE of changes in status, additional information, or cancellation of access authorization requests? 7. Is there an active quality assurance process? 8. Are PSFs organized in a consistent manner, accurate, and complete? 9. Are there procedures in place to ensure that badges are only issued to properly cleared individuals?	1. Review local procedures, interview personnel to determine their understanding of DOE directives and local procedures, and identify any training they may have received. 2. Interview the head of the DOE personnel security organization to determine the amount of overtime routinely required of the personnel security specialists. 3. Examine a random sample of Personnel Security Files (PSFs) from the last 12 to 18 months to determine the following: • The timeliness (within 7 days of receipt of completed investigations for clear cases and 30 days for cases with derogatory information) of screening/analysis activities • The scheduling of Personnel Security Interviews (PSIs) within 30 days of determination to interview • Peer and supervisory reviews are completed and documented as necessary • Five-percent reviews of clear cases are completed and documented • Information is arranged in a uniform manner, and is accurate and complete • Establish that the DOE investigation requirements have been met • The existence of errors and omissions on Questionnaire for National Security Positions (QNSPs) and fingerprint cards	pre-planning and on-site on-site on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		• Case reference sheets document the resolution or mitigation of all identified derogatory information • All derogatory information has been identified 4. Review documentation that supports the quality assurance process to determine its effectiveness. 5. Review the CPCI database to determine whether timely entries are made. 6. Review a sample of clearances during the past 12-18 months against badge records to determine whether any badges were issued prior to the granting of the clearance.	 on-site on-site
Clearance: The identification and resolution of derogatory information is thorough and timely.	1. Is all derogatory information resolved prior to granting or continuing a clearance? 2. Does a significant backlog of cases (initial and reinvestigations) requiring resolution exist? 3. Are there any systemic deficiencies in the Administrative Review process? 4. Are adjudication criteria and procedures consistently applied? 5. Is the appropriate denial of access (including retrieval of badges) initiated upon notification of suspension of a clearance or notification that a clearance is no longer needed?	1. Interview the individuals responsible for Letters of Interrogatory (LOIs) and PSIs to evaluate their competence. 2. Review any local procedures to determine whether they are consistent with policy/ 3. Review a sample of PSFs (including cases that involved LOIs, PSIs, and psychiatric referral) from the past 12 to 18 months to determine the following: • That local procedures are being followed • That all derogatory information was reviewed, evaluated, and adjudicated in a timely manner • That case results are supported by the information provided by LOI and interviews • Decisions to refer for additional investigation are justified • Decisions to grant an access authorization that have been made without a referral are justifiable	on-site pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		• In cases where access was suspended, that all procedures were followed and appropriate documentation exists to justify suspension • Evidence of a consistent application of adjudicative criteria and procedures 4. Review clearances that have been suspended during the past 12 to 18 months against badge and CPCI records to ensure timely denial of access.	on-site
Clearance: DOE is responsible for the timely submission and completion of reinvestigations.	1. Is there a system in place for the selection of individuals for reinvestigation and the completion of these reinvestigations?	1. Review local procedures supporting the reinvestigation program (including contractor procedures). 2. Interview individuals responsible for the reinvestigation program to determine whether the process is accurately identifying all individuals due to be reinvestigated. 3. Review records to determine whether reinvestigations are being requested in accordance with DOE requirements.	on-site on-site on-site
HUMAN RELIABILITY PROGRAM (HRP): Is the program identifying and enrolling all positions identified in the SSSP to mitigate threat represented by insiders and therefore providing all the intended benefits of an enhanced safeguards and security reliability program? Does the system of continuous evaluation identify those individuals that may represent a reliability, safety, and/or security concern? **IMPACT:** Weaknesses in this program could lead to unacceptable damage to specific national security interests.			

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Human Reliability Program: Plans, policies, and procedures are complete and up to date.	1. Is there a systematic process for identifying HRP positions that is consistent with policy, and are these positions reflected in the SSSP? 2. Does the site HRP ensure that individuals thrust into an HRP position meet all HRP requirements? 3. Have program responsibilities been formally assigned? 4. Has a comprehensive implementation plan and/or schedule for implementation been developed?	1. Review site implementation plans and procedures to determine whether all program elements have been implemented and all HRP positions have been identified. 2. Review the SSSP and coordinate with the other inspection topic teams to determine whether personnel serving in critical positions are enrolled in the HRP. 3. Interview program officials, heads of support organizations, and supervisors to determine how roles and responsibilities have been communicated and whether they are understood.	pre-planning pre-planning on-site
Human Reliability Program: Reviews and evaluations are completed as required and are comprehensive.	1. Are all required reviews and evaluations completed before enrolling an individual into the HRP? 2. Is there a process that ensures that all of the annual evaluations, assessments, and determinations are completed for each individual enrolled in the HRP?	1. Interview supervisors, medical personnel, personnel security specialists, HRP certifying officials, and individuals serving in HRP positions to determine whether required evaluations and assessments are being completed. 2. Review HRP forms, QNSPs, and other parts of evaluations and assessments to determine whether they are complete, and if they were completed in a timely manner.	on-site on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Human Reliability Program: Drug and alcohol testing effectively identifies safety and security concerns.	1. Does the drug and alcohol testing program ensure that all individuals in HRP positions are tested annually? 2. Are appropriate security measures in place concerning selection for drug testing, and is there a continuous chain of custody for samples? 3. Is there a procedure that ensures that persons called in to perform unscheduled work are fit to perform the task assigned? 4. Are there sufficient numbers of trained medical staff to implement the testing program?	1. Review testing procedures to determine the following: • The overall process • How specimens are to be handled • The selection process 2. Interview personnel responsible for conducting the test to determine whether they understand and implement the procedures. 3. Interview individuals that have been recently tested to verify that testing was according to procedures. 4. Review test records to determine whether all personnel in HRP positions have been tested.	pre-planning on-site on-site on-site
Human Reliability Program: The training program adequately prepares supervisors.	1. How does the HRP approving official ensure that supervisors understand their responsibility of being able to identify aberrant behavior and take appropriate action (immediate removal/reporting)? 2. Are supervisors aware of their responsibility to report any security concerns to the appropriate officials, and if necessary, take immediate action?	1. Review the process used to train supervisors. 2. Interview supervisors to evaluate the effectiveness of training. 3. Examine any materials used in the training program for usefulness.	pre-planning on-site pre-planning
Human Reliability Program: Reporting requirements are met.	1. Is there sufficient coordination between nuclear explosive safety, contractor, and HRP officials to ensure that information about any concerns is being shared?	1. Review any reports of unusual conduct or aberrant behavior to determine who made the report, how it was recorded, and what action was taken. 2. Interview safety officials and supervisors to determine whether they understand the security impact of observed safety concerns.	pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Human Reliability Program: Records and files are complete.	1. Is there an adequate system to maintain appropriate data on HRP positions? 2. Are the required release forms, waivers, and certifications being filed in the PSF? 3. Does this system make data readily available to program officials? 4. Does the system ensure that vacated HRP positions are filled in a timely manner and that supervisors are notified when positions become vacant?	1. Review HRP records and PSFs to verify that they are complete and adequate to support the program.	on-site
SAFEGUARDS AND SECURITY AWARENESS PROGRAM: Are all personnel (on- and off-site) informed of their security responsibilities upon employment and prior to being granted access to classified matter and SNM, and are personnel informed of actual and potential threats to the extent that inadvertent compromises of classified and sensitive unclassified information are effectively eliminated? Has a method been developed to measure the effectiveness of the program? **IMPACT:** The ultimate effectiveness of the site protection program depends on the actions of all employees. As such, a poorly designed and implemented safeguards and security awareness program can have a serious impact.			
Safeguards and Security Awareness Program: Administration and management supports program implementation.	1. Do program procedures and documentation support full implementation? 2. Do the parameters of the program include coverage for subcontractors?	1. Review policies and procedures to determine whether a structured safeguards and security awareness program has been implemented for on-site personnel and off-site support contractors, adequate records are kept, and briefing materials are reviewed and updated by a responsible individual. 2. Review documentation to determine whether the coordinator has been formally appointed. 3. Interview/review records to determine whether the Operations Office has delegated the authority for oversight/implementation of contractor and subcontractor safeguards and security awareness programs.	pre-planning and on-site pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Safeguards and Security Awareness Program: Briefings are comprehensive and are conducted as a precondition to initial and continuing access.	1. Is the comprehensive briefing conducted after the clearance has been granted? 2. Is a security badge permitting unescorted access to a security area issued only after attendance at the comprehensive briefing? 3. Do briefings contain all required subjects and/or site-specific information, and is the briefing material accurate? 4. Do all on-site and off-site personnel complete annual refresher briefings? 5. Are required briefings given to personnel traveling abroad?	1. Review a sample of SF-312 forms to determine whether the date of the comprehensive briefing preceded the date clearance was granted. 2. Compare badging dates with dates of initial briefings to ensure that the briefings were conducted prior to badging. 3. Review documentation and/or attend briefings to determine whether all required topics, and site-specific information when applicable, is included for each type of briefing. 4. Review records to determine whether there is a system for scheduling and presenting refresher briefings. 5. Review DOE Forms 1512.2 and 1512.3 and DOE authorization letters associated with foreign travel to determine whether the forms were submitted in a timely manner, and whether associated briefings were presented.	on-site on-site pre-planning or on-site on-site on-site
Safeguards and Security Awareness Program: Termination briefings are conducted.	1. Do all individuals receive a termination briefing when a clearance is no longer required? 2. Are the appropriate forms executed after the completion of the termination briefing? 3. Are all badges retrieved once the termination briefing has been administered?	1. Interview to determine whether there are procedures in place to ensure that termination briefings are conducted, DOE Form 5631.9 is properly executed, and badges are retrieved. 2. Review records to determine whether termination briefings are conducted, a DOE Form 5631.9 is properly executed, and badges are retrieved.	on-site on-site
Safeguards and Security Awareness Program: Visual aids and other materials support the program.	1. Are posters, newsletters, booklets, and other media accurate? 2. Do visual aids effectively provide security-related information to employees and support/emphasize the content of briefings?	1. Review records to determine the accuracy and adequacy of instructional aids and other materials. 2. Review the results of the Safeguards and Security Awareness Program (SSAP) questionnaire to determine effectiveness of aids and other materials.	on-site on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Safeguards and Security Awareness Program: Coordinator training is evident in the quality of the briefings.	1. Do the individuals assigned the responsibility to coordinate and present safeguards and security awareness briefings possess the proper skills and knowledge?	1. Review records to determine whether the coordinator has attended the DOE-required training. 2. Review records that substantiate the qualifications of other personnel responsible for the development and presentation of the briefings. 3. Attend briefings to evaluate the presenter's skill and knowledge.	pre-planning pre-planning on-site
Safeguards and Security Awareness Program (SSAP): Feedback is continuous and leads to program enhancements.	1. Does employee knowledge reflect an effective safeguards and security awareness program? 2. Which feedback mechanisms (surveys, self-assessments, OPSEC programs, questionnaires, tests, etc.) provide data (written or verbal) to the program manager? 3. Are the results of these mechanisms analyzed to identify lessons learned or potential enhancements?	1. Review the results of the SSAP questionnaire. 2. Interview the coordinator to determine what type of feedback mechanism is used, if any, how the data is used. 3. Incidents of security concern records should be reviewed for any trends that are relative to the effectiveness of the safeguards and security awareness program.	on-site on-site on-site
UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS: Does the program prevent or mitigate unauthorized access to or unintentional disclosure of classified information, sensitive unclassified information, and/or special nuclear material? **IMPACT:** The lack of a comprehensive visits and assignments program could assist the efforts of hostile intelligence services to obtain key information. It must be recognized that all returning foreign national visitors are debriefed and would be obliged to divulge any information they may have gained, even if it was gained unintentionally.			
Unclassified Foreign Visits and Assignments: Procedures provide a basis for an integrated approach.	1. Does management support of site procedures ensure that visits and assignments are requested in sufficient time to allow for all precautions to be taken? 2. Are local policies clear and unambiguous about roles and responsibilities and ensure proper integration and communications between all parties?	1. Review records to determine whether the site has developed a comprehensive and integrated approach to visits and assignments. 2. Review records to determine whether requests are submitted in a timely manner. 3. Interview personnel to determine whether they understand their roles and responsibilities.	pre-planning on-site on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	3. Are hosts and escorts fully knowledgeable of their responsibilities concerning requesting a visit or assignment, reporting changes during the conduct of a visit or assignment, and reporting any unusual occurrences during a visit or assignment?	4. Review records to determine whether approval is held by either the Operations Office Manager or Laboratory Director (delineation to only one level down permitted). 5. Review records to determine whether all reviews are conducted (line management, OPSEC, export control, security, cyber security, etc.). 6. Review past self-assessments and surveys to determine whether the Foreign Visits and Assignments (FV&A) program is periodically assessed to identify and correct program weaknesses.	pre-planning pre-planning and on-site
Unclassified Foreign Visits and Assignments: Indices checks are used to identify potential risks.	1. Are indices checks completed prior to all visits and assignments that involve foreign nationals from sensitive countries or terrorists countries, that are concerned with sensitive subjects, and/or that include access to security areas? 2. Are counterintelligence consultations used appropriately in lieu of indices checks?	1. Review files to determine whether indices checks were completed prior to applicable visits or assignments. 2. Interview to determine whether results are being received by the requesting Operations Office and what actions are taken when derogatory information has been identified.	on-site on-site
Unclassified Foreign Visits and Assignments: Security plans and coordination ensure the consideration of all security factors.	1. Are all security plans (especially generic security plans) sufficiently detailed to ensure that inadvertent compromises of security interests do not occur? 2. Does the approach to assessing risks include the identification of all classified and sensitive unclassified information and activities, determine the reason the information is sensitive, determine mechanisms for compromise, and develop actions to mitigate any residual risks? 3. Do security plans adequately address and	1. Review records to develop an understanding of the site's approach to assessing risk (including coordination with OPSEC, counterintelligence [CI], and export control program officials). 2. Interview subject matter experts to determine whether they are qualified. 3. Review the Sensitive Subjects List and determine whether it is current and whether it includes a site-specific addendum for identifying additional subjects. 4. Review a selection of specific and generic security	pre-planning on-site on-site pre-planning

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	control remote access to site computing assets? 4. Do FV&A officials coordinate requests with OPSEC, CI, and export control program officials/subject matter experts? 5. Are foreign nationals permitted access to or use of computing assets? 6. Are foreign nationals appropriately badged?	plans to determine whether they are sufficiently detailed to make decisions concerning their adequacy and comprehensiveness. 5. Conduct a walk-through of locations where visits or assignments are ongoing or had occurred to determine whether the measures contained in the security plans were adequate and whether they were followed. 6. Interview/review records to determine the level of coordination with cyber security program managers regarding on and off-site utilization of computing assets. 7. Interview to determine how the site conducts performance tests to ensure only appropriate and approved access to computing assets. 8. Review badging records to confirm that foreign national visitors are badged, and tour areas hosting foreign national visitors to determine whether they are in possession of their badges.	and on-site pre-planning and on-site
Unclassified Foreign Visits and Assignments: Escort procedures and training ensure that escorts can effectively meet their responsibilities.	1. Are escorts sufficiently indoctrinated in their responsibilities, and is there a mechanism to remind them of these responsibilities, especially for long-term assignments? 2. Is there a specific training program for escorts (and hosts)? 3. Is there a quality assurance process?	1. Review records to determine the adequacy of escort training/instructions. 2. Examine escort training materials to determine whether they are adequate. 3. Interview escorts to determine whether they were periodically reminded of their responsibilities.	pre-planning pre-planning on-site

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
Unclassified Foreign Visits and Assignments: Host reports support enhancements to the program.	1. Are hosts fully knowledgeable of their responsibilities concerning submitting a host report at the end of a visit or assignment? 2. Do host reports provide sufficient information to detect program weaknesses and take appropriate action (i.e., identify enhancements, conduct investigations, issue infractions, etc)? 3. Are incidents of security infractions reported?	1. Interview hosts to determine whether they are knowledgeable of their responsibilities. 2. Review a sample of host reports to determine whether they were timely, complete, and forwarded to the appropriate distribution. 3. Is the host report formatted in such a manner to elicit information on how well the request process worked, whether any unexpected changes in security procedures or the location of security interests occurred, and whether the visitor/assignee did anything unusual. 4. Interview/review records to determine whether host reports are analyzed to identify program weaknesses and lessons learned. 5. Review records and conduct interviews to determine how lessons learned are shared. 6. Review security incident files to determine whether any incidents have occurred and what action was taken to preclude a recurrence.	on-site on-site pre-planning and on-site on-site pre-planning and on-site

PERSONNEL SECURITY INSPECTION PROCESS MATRIX

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
PRE-PLANNING		
Develop an overview of past personnel security program issues and concerns by reviewing past inspection results and discussing them with team members.		Team Leader. ***Throughout pre-planning, the team leader will consult with other team members as appropriate and in accordance with security requirements to identify and analyze past and current site-specific or complex-wide personnel security program issues.***
Review site protection strategy, VAs/SSSP, security plan, Classified Matter Protection and Control (CMPC) team data or cyber security team data to develop a list of potential adversary targets/facilities and personnel positions critical to the protection of special nuclear material (SNM), and review classified and sensitive unclassified information on which to base data collection activities/sampling. Examples: • Facilities processing, handling, and storing SNM • Sensitive compartmented information facilities (SCIFS) • Facilities with sampling and analysis plans (SAPs) • Facilities/vaults that require enrollment in an HRP		Team Leader
Contact Deputy Inspection Chief and obtain the name of the operations office and contractor personnel security program points of contact.		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
After the completion of the above, complete the following: • Confirm topic and sub-topic objectives and scope • Assign personnel/resources to support data collection activities • Develop expectations regarding the completion of data collection tasks.		Team Leader
Discuss proposed topic objectives and scope with Office Director and Deputy Office Director.		Team Leader
Refine topic objectives and scope, and tailor the document request list.		Team Leader
Develop the personnel security input for the inspection plan (topic focus [topic elements and/or issues that will have the most bearing on determining the effectiveness of the topic], performance testing, management interviews, potential issues, and data collection assignments).		Team Leader
Develop topic team schedule. (The schedule is a general forecast of activities and not a precise description of each day's activities.)		Team Leader
Contact field points of contact; provide (via email) topic objectives, data collection activities/schedule, and the document request list, which identifies items that need to be sent to Germantown in advance of on-site activities and those items that we will need at the site. Of special importance is that the document request list identifies the lists for personnel security file reviews, and site sensitive locations and operations to focus foreign visits and assignments data collection activities.		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Coordinate the development of a safeguards and security awareness questionnaire (performance test) with the site point of contact (the questionnaire will be completed prior to the start of the final on-site data collection phase).		Team Leader or SSAP lead inspector
Meet with Headquarters topic points of contact to gather information and to discuss data collection activities.		Team Leader
Identify items to be sent to the site to the Oversight Document Center.		Team Leader
Prepare a list of additional documentation needed from the site for use before or during the planning meeting and provide to Deputy Inspection Chief; email the request to points of contact.		Team Leader
Receive and review requested documentation in preparation of the planning meeting.		Team Leader
Verify initial schedule with team and points of contact.		Team Leader
CONDUCT ON-SITE PLANNING AND INITIAL DATA COLLECTION (ONE WEEK)		
Assemble at badge office, **Monday afternoon**		Team
Attend site security and safety training, **Monday afternoon**		Team
Attend In-Briefing, **Monday afternoon**		Team
Meet field points of contact, confirm/refine schedule, **Monday afternoon**		Team
Assemble at work space to conduct topic team meeting to discuss matters as appropriate before the initiation of planning/data collection activities, **Monday afternoon**		Team
Sign copies of the computer security plan, and post the plan, **Monday afternoon**		Team
Participate in tour of the material access areas (MAAs) with the systems team. note: this activity can occur **Monday afternoon** or on **Tuesday**		HRP sub-topic lead

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Verify receipt of all requested documents and provide to Admin Support Manager, **Tuesday or Wednesday**		Team Leader
Collect data, **Tuesday through Thursday** • FV&A, Interviews, file reviews and tours • SSAP: Interviews, file reviews, reconciliation with CPCI • HRP: Interviews of officials Validate data (as team will be split, each team member will validate data as it is collected and then summarized with attending field points of contact when a data collection activity is completed).		Team Team
Must keep Team Leader informed of location and phone number (may be done via admin support personnel).		Team
Daily, prepare data collection forms (personal preference: either complete before the daily team meeting, after the meeting, but not later than the initiation of the next day's data collection activities). Data collected on the forms should represent a roll-up and **not a verbatim transcription** of an individual's notes. In this way, the analysis process will be initiated and it should ease preparation of issues forms (when required) and the inspection report. Distribute to Deputy Inspection Chief and Admin Coordinator.		Team Team Leader
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Topic team discusses results of data collection, leading to drafting of evening bullets, and confirms/revises schedule (should occur briefly before the daily meeting, over the phone if necessary). *The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: • Topic team has reached agreement on the importance of the issue • Integration with other topic teams has been completed • Inspection team management has been informed off-line (no surprises). **Assign a team member the responsibility to capture on an Issue Form those issues that could impact the rating.** (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response.)		Team Leader
Attend daily team meeting (as necessary, the Team Leader may coordinate the absent team members)		Team
Finalize evening bullets and provide to Deputy Inspection Chief during the evening meeting.		Team Leader
Conduct end-of-the-day security checks.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Throughout this phase of the inspection the team works to: • Identify the key results to date • Determine the facts that support the key results, and **capture these facts on an Issue Form for rating impacting issues** *(initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response).* • Revise data collection plan and adjust resources to collect this data. • Revise topic annex/sub-topical report submissions/bulletized outlines (intro, background, and conduct, and results if possible).		Team
Meet with field points of contact to provide summary of initial results, and to schedule future data collection activities for HRP, safeguards and security awareness, and unclassified FV&A, **Thursday**		Team
Identify and destroy unwanted papers, return pagers, keys and dosimeters to administrative support personnel, **Thursday**		Team
POST PLANNING ACTIVITIES		
Conduct Headquarters interviews (Program Secretarial Officers [PSOs], NNSA, etc.).		Team Leader
Review additional documentation.		Team Leader and Team
Collect and validate data.		Team Leader
Analyze data collection results to date.		Team
Refine inspection focus and topic assignments.		Team Leader
Coordinate inspection activities with field points-of-contact.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
When required, prepare data collection forms, and distribute to Deputy Inspection Chief and Admin Coordinator.		Team Leader
When required, prepare Issue Forms, review Issue Forms, and provide to Deputy Inspection Chief; resolve site comments on Issues Forms.		Team Leader
DATA COLLECTION (ONE WEEK)		
New team members report to badge office, attend training, and sign computer security plans, **Monday**		Team Member (s)
Conduct topic team meeting on first day of data collection to confirm/refine schedule, **Monday**		Team Leader

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Collect data, **Monday through Thursday** • Interview personnel security clearance program officials and specialists. • Complete PSF reviews and record results on file review form.		Team
Validate data (as team will be split, each team member will validate data as it is collected and then summarized with the attending field points of contact when a data collection activity is completed).		Team
*The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved.		Team Leader
*Issues that could impact the topic rating should normally be discussed in the evening meeting only after: • Topic team has reached agreement on the importance of the issue • Integration with other topic teams has been completed • Inspection team management has been informed off-line (no surprises).		

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
A team member should take the responsibility to capture on an Issue Form those issues that could impact the topic rating ***as soon as such an issue has been identified.*** (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response) ***Must keep Team Leader informed of location and phone number (may be done via admin support personnel).***		Team
Daily, prepare data collection forms (personal preference: complete either before the daily team meeting or after the meeting, but not later than the initiation of the next day's data collection activities). Distribute to Deputy Inspection Chief and Admin Coordinator.		Team Team Leader
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member
Conduct limited scope performance tests (LSPTs), as required.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Conduct brief topic discussion before daily team meeting on the results of data collection, leading to drafting the evening bullets, and confirm/revise schedule. *The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: • Topic team has reached agreement on the importance of the issue • Integration with other topic teams has been completed • Inspection team management has been informed off-line (no surprises). **Assign a team member the responsibility to capture on an Issue Form those issues that could impact the topic rating.** (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response.)		Team Leader
Attend daily team meeting (as before, team members may be absent with approval).		Team
Finalize evening bullet points for HSS Management.		Team Leader
Conduct end-of-the-day security checks.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
FINAL DATA COLLECTION ACTIVITIES, DRAFT REPORT TOPIC APPENDIX PREPARATION AND CLOSEOUT (TWO WEEKS)		
Collect data, **Monday through Thursday** • Conduct file of HRP and medical files. • Observe drug and alcohol testing and administer tests to all technicians • Administer the safeguards and security awareness questionnaire and analyze results. Validate data (as team will be split, each team member will validate data as it is collected and then summarized with the attending field points of contact when a data collection activity is completed). *The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: • Topic team has reached agreement on the importance of the issue • Integration with other topic teams has been completed • Inspection team management has been informed off-line (no surprises).		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
A team member should take the responsibility to capture on an Issue Form those issues that could impact the topic rating ***as soon as such an issue has been identified.*** (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response)		
Must keep Team Leader informed of location and phone number (may be done via admin support personnel).		Principal Writer
Daily, prepare data collection forms (personal preference: complete either before the daily team meeting or after the meeting, but not later than the initiation of the next day's data collection activities). Distribute to Deputy Inspection Chief and Administrative Coordinator.		Team Team Leader
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member
Conduct LSPTs, as required.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Conduct brief topic discussion before daily team meeting on the results of data collection, leading to drafting the evening bullets, and confirm/revise schedule. *The topic team leader is responsible for deciding when an issue will be raised during the evening meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved. *Issues that could impact the topic rating should normally be discussed in the evening meeting only after: • Topic team has reached agreement on the importance of the issue • Integration with other topic teams has been completed • Inspection team management has been informed off-line (no surprises). **Assign a team member the responsibility to capture on an Issue Form those issues that could impact the topic rating.** (Initially this will assist internal topic and inspection team discussions of the issue, and may lead to formulation of an issue paper for site response.)		Team Leader
Attend daily team meeting (as before, team members may be absent with approval).		Team
Finalize evening bullets for HSS Management.		Team Leader
Conduct end-of-the-day security checks.		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Sub-topic inspectors turn in all data collection forms and/or draft sub-sections of the appendix to the principal writer by **Friday close of business**		Team
When required, conduct discussion with team members on **Friday afternoon** to prepare the Inspection Chief focus briefing, to include: • Finalize the key points (conclusions) to be made in the inspection report • List the facts that support each key point • Do not over emphasize lesser strengths or weaknesses that might obscure the presentation of the key points • Findings • Policy issues • Proposed rating		Team
When required, present Inspection Chief focus briefing, **Saturday**		Team Leader
Finalize draft topic appendix, **Saturday**		Principal Writer
Conduct reviews of the draft appendix for content and readability, provide comments to principal writer, **Saturday and Monday morning**		Team
Conduct technical edit of draft appendix and provide input to principal writer**, Monday afternoon**		Team
Turn in draft inspection report to the Quality Review Board (QRB), **Monday or Tuesday morning**		Team Leader
Provide list of acronyms, interviews, and references to Admin Support Manager, **Tuesday**		Team
Address QRB /HSS-1/site comments (inform QRB of actions) **Tuesday or Wednesday**		Team Leader
Meet with site personnel to discuss the disposition of comments on the draft inspection report appendix, **Tuesday or Wednesday**		Team
Prepare briefing bullets and notes, **Tuesday**		Team

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
Participate in Roundtable, **Wednesday or Thursday**		Team
Identify documents for return to Germantown; return room keys, dosimeters, and pagers; destroy unwanted documents; return supplies; return site documents, **Wednesday and Thursday**		Team Leader
Conduct topic team lessons-learned meeting, **Thursday**		Team Leader
POST-INSPECTION ACTIVITIES		
Review 10-day site comments and incorporate as appropriate.		Team Leader
Review and respond to initial and final corrective actions and provide to Deputy Inspection Chief.		Team Leader
Revise Topic Inspection Process Matrix and distribute.		Team Leader

Document Request List (DOE Site)
Personnel Security Topic Team
XXXXX Inspection 200X

The below information is requested to support the personnel security topic (personnel security clearance program, human reliability program, safeguards and security awareness program, and foreign visits and assignments program) team. Responsibility for each action or item is identified as bolded and in parentheses.

The preferred method of transmission of any unclassified items is an attached file to an email message to the identified Office of Security Evaluations (HS-61) point of contact**. The alternative method of transmission is in hardcopy sent to** DOE Headquarters – Germantown Building (Attention HS-61 point of contact)**. Any classified information must be sent to HS-61 according to DOE directives for mailing classified information.**

Questions should be addressed to (HS-61 point of contact at (301) 903-XXXX).

The following documents and/or information are requested to be provided by [Month], [Date], 200X:

GENERAL INFORMATION:

- An organization chart(s) or other means of describing the structure supporting the overall personnel security program that supports the overall XXX protection program. The description is needed to understand where all key program officials and support staff reside organizationally, and to see the chain of command to each key program official and support staff.

- A copy of the personnel security clearance program, HRP, awareness program, and foreign visits and assignments program portion of the last two self-assessments and surveys.

PERSONNEL SECURITY CLEARANCE PROGRAM

Servicing DOE Personnel Security Organization

- Provide the following **separate, line-numbered alphabetized lists (last name first)** of personnel security cases for XXX personnel with a **"Q" access authorization** to assist in the random selection of PSF for review (the timeframe for all lists is [18 months]):

    - Cases for individuals who have completed an initial or periodic report of investigation and have required the use of any additional adjudicative action (LOI, PSI, psychiatric evaluation, etc.) to resolve derogatory information

    - Cases for personnel who have completed an initial or periodic report of investigation and have resulted in a clear case file determination that required no additional adjudicative actions required prior to granting or continuing a clearance

- All initial background investigation reports that are pending screening
- All re-investigation reports that are pending screening

- Reinstatements that have been completed

- Individuals who have any derogatory information reported; this includes all such potential sources for the derogatory information as investigations of security incidents, infraction reports, the Occurrence Reporting and Processing System (ORPS), job-related disciplinary action, self-reporting, Employee Equal Opportunity program (e.g., sexual harassment)

- All suspension actions related to the initiation of administrative review

- All grant cases with drug use identified and requiring adjudicative action to resolve.

Contractor Personnel Security Organization

- Provide the following **separate, alphabetized (last name first) lists** for personnel with a **"Q"** access authorization (the timeframe for all lists is [18 months]):

  - All completed pre-employment checks for individuals with "L" or "Q" access authorizations

  - All individuals with "L" or "Q" access authorizations who had **absences of 90 days or more**; payroll records should be used to develop this listing.

  - A listing of all contractor/sub-contractor employees for which INL has notified or reported to (the servicing DOE personnel security organization) information of personnel security interest as a result of a disciplinary action (the listing should not include security infraction reports like the one requested by the CMPC topic team). Please include the date reported to (the servicing DOE personnel security organization).

- Provide documents that describe how XXX met the requirement to report information of personnel security interest to DOE as specified in DOE Manual 470.4-5, Contractor Requirements Document (CRD) paragraph 7.(4).

- Provide a **alphabetized (last name first)** listing of individuals who have reported information of personnel security interest to the XXX personnel security organization from (18 months).

- Provide a **alphabetized (last name first)** listing of disciplinary action taken against XXX employees for the period (18 months); include the date the disciplinary action was taken and a description of the issue that prompted the disciplinary action.

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

- Provide a copy of the current procedure or a description of the badge process, including the process for acting upon a lost badge and retrieving badges from individuals who no longer require an access to XXX facilities and/or no longer are doing any work at XXX that requires access to classified information.

- Separate **alphabetized (last name first), line numbered** lists (use Excel, if possible) of all cleared employees. XXX should also provide a separate listing for subcontractor employees and their duty location(s).

- Provide documentation verifying both the completion of required DOE training by the SSAP coordinator and the appointment of the individual as the coordinator.

- Dates and location(s) of all initial and comprehensive briefings being presented during this inspection (to allow HS-61 to attend selected presentations).

- Provide the following **separate, alphabetized (last name first) lists** for personnel **with a "Q" access authorization** (the timeframe for all lists is [18 months]):

    - Access authorization **terminations**; this list should **not** include transfers or any item other than a termination of access authorization

    - All employees (cleared and uncleared) whose **employment** was **terminated**; this data must be from the site Office of Human Resources or employment office

    - All individuals who have been **granted** an initial access authorization, the date action to grant that was taken by DOE**,** and the date a DOE security badge was issued

    - All individuals who have **transferred** from another DOE facility, the date action to transfer that was taken by DOE**,** and the date a DOE security badge was issued

    - All individuals who have had their access authorization **reinstated**, the date action to reinstate that was taken by DOE**,** and the date a DOE security badge was issued.

- Provide a **draft** of three versions of a security awareness questionnaire each consisting of 25 multiple choice and true or false questions.

  (In concert with HS-61, the XXX points of contact will develop the variations of a questionnaire that will be administered either on-line or in person as applicable to randomly selected individuals. Each variation of the questionnaire should have five questions that are not repeated on the other variations. The questionnaire should be based on initial, comprehensive, and annual refresher briefings, and should focus on the most important elements that employees are expected to remember.)

(HS-61 will determine the number of individuals who will be requested to complete the questionnaire, while the XXX points of contact will notify those chosen using a mutually agreed upon, random selection process to complete the questionnaire.)

HUMAN RELIABILITY PROGRAM

- Provide the building/room identifier for each material access area (MAA), and a diagram depicting the location of each MAA.

- Provide the following **separate, alphabetized (last name first) with organization lists** (using site access control logs/databases) for the period (18 months):

  - Names and dates when non-HRP enrolled, "Q" or "L" cleared individuals were granted escorted access into each MAA, and the total number of individuals granted escorted access for the period

  - Names and dates when uncleared individuals were granted escorted access into each MAA, and the total number of individuals granted escorted access for the period.

- Provide documents that describe the process (e.g., risk analysis, a finite number of times escorted into a MAA) used at XXX to determine when the enrollment process should begin for individuals filling duty positions that are not listed in the HRP implementation plan.

- Provide a copy of the HRP implementation plans and documentation of review and approval by the Manager.

- Provide the following **separate, alphabetized (last name first) lists** for XXX enrolled in a **HRP program** (the timeframe for all lists is [18 months]):

  - All individuals enrolled in HRP; include each individual's duty position (as listed in the approved HRP implementation plan), and the name of the person who completes the annual supervisory review for each individual

  - All supervisors and their subordinates who are enrolled in HRP.

  - All individuals pending HRP approval

  - All individuals who have been temporarily removed from HRP or had their HRP certification revoked for any reason (security, safety, medical or changes of position/employment); include the date of removal, reason for removal, and, if applicable, the date of reinstatement

  - All individuals who have been involved in an accident that was reported as an occurrence to DOE

  - All personnel who have been designated as individuals that are prohibited from consuming alcohol for eight hours preceding scheduled work.

- Provide a copy of the initial and annual unannounced drug and alcohol testing procedures and/or protocols.

- Provide a copy of procedures that describe the actions that will be taken for positive drug and alcohol test results.
- Provide a copy of all HRP instructional materials for supervisors, HRP-certified individuals, and site occupational medical providers.

- Provide a description of process used to evaluate and designate HRP positions.

- Assemble letters of designation/certification for the SOMD, Designated Physician, Designated Psychiatrist, breath analysis technicians, and drug testing technicians.

- Provide a list of breath alcohol and drug testing technicians.

- Provide copies of the letters that give the Designated Physician or Designated Psychiatrist authority to sign for the SOMD.

- Provide a list of equipment used for alcohol testing.

- Provide a list of positions and job titles for which JTAs have been developed and provided to medical personnel.

UNCLASSIFIED FOREIGN VISITS & ASSIGNMENTS

- Provide the total number of foreign national visits and assignments that have occurred at XXX between (a period of 18 months). Please also provide the number of foreign national visitors and assignees that are from a sensitive country or a terrorist country, and foreign visits and assignments that involved sensitive subjects and/or access to security areas (protected, limited, exclusion, and property protection areas).

- Assemble separate, **alphabetized (last name first)** listings or computer printouts of visits and assignments that have occurred between (18 months) for each of the following:

    - FV&As involving foreign nationals from sensitive countries

    - FV&As involving sensitive subjects

    - FV&As involving access to security areas (protected, limited- and property-protection areas)

    - FV&As involving foreign nationals from terrorist countries

    - Any foreign nationals who have approval for unescorted access to any XXX security area

    - All visiting foreign nationals who have been granted access to XXX computing assets, with a termination date for access to the computing assets

    - All foreign nationals visitors and assignees who have been granted remote access to XXX

computing assets, with a termination date for remote access

- All visiting foreign nationals who have bee granted after-duty-hours access to XXX facilities
- All foreign nationals who are related to incidents and inquiries of incidents of security concern
- All of the most frequently visited site facilities and programs.

Each of these lists should provide the following information: name and nationality of visitor/assignee, date of visit/assignment, name of host/escorts, facilities included in the scope of the visit/assignment, and, when applicable, approval for remote or on-site access to computing systems.

- Provide a diagram that depicts all site security areas (protected, limited, exclusion, and property protection areas, including building numbers). (Please provide a separate diagram from those provided in response to other topic team requests.)
- Provide procedures and/or protocols used to process and approve all FV&As.
- Provide an example of both a generic security plan and a specific security plan.
- Obtain a copy of host/escort guidance or training materials.
- Provide a procedure or description of how lessons learned are shared with other hosts/escorts.

REQUIRED DOCUMENTS / INFORMATION

Access to the following documents and/or information items will be required during the on-site phases of the inspection:

- Personnel Security Clearance Program
  - Pre-employment check files
  - 90-day absences files
  - Information of personnel security interest files
  - Personnel security files.
- SSAP
  - Initial, comprehensive, annual refresher, and termination briefings and any supporting materials/handouts
  - Records (e.g., attendance rosters, SF 312, *Classified Information Nondisclosure Agreement*, DOE F 5631.29) of completion of initial, comprehensive, refresher, and termination briefings.

- HRP

  - Records that document the completion of HRP initial and annual instruction
  - HRP records and HRP-associated medical and psychological files
  - JTAs that have been developed and provided to the Designated Physician(s) and Psychologist(s).

- FV&A

  - Requests for FV&As
  - Records of reviews and approvals of FV&As
  - Specific and generic security plans
  - Local Foreign Activities Central Tracking System (FACTS) terminal.

Document Request List (NNSA Site)
Personnel Security Topic Team
XXXXX Inspection 200X

The below information is requested to support the personnel security topic (personnel security clearance program, human reliability program, safeguards and security awareness program, and foreign visits and assignments program) team. Responsibility for each action or item is identified as bolded and in parentheses.

The preferred method of transmission of any unclassified items is an attached file to an email message to the identified HS-61 point of contact**. The alternative method of transmission is in hardcopy sent to** DOE Headquarters – Germantown Building (Attention HS-61 point of contact)**. Any classified information must be sent to HS-61 according to DOE directives for mailing classified information.**

Questions should be addressed to (HS-61 point of contact at (301) 903-XXXX).

The following documents and/or information are requested to be provided by [Month], [Date], 200X:

GENERAL INFORMATION

- An organization chart(s) or other means of describing the structure supporting the overall personnel security program that supports the overall XXX protection program. The description is needed to understand where all key program officials and support staff reside organizationally, and to see the chain of command to each key program official and support staff.

- A copy of the personnel security, including clearance program, human reliability program, awareness program, and foreign visits and assignments program portion of the last two self-assessments and surveys.

PERSONNEL SECURITY CLEARANCE PROGRAM

Contractor Personnel Security Organization

- Provide the following **separate, alphabetized (last name first) lists** for personnel **with a "Q" access authorization** (the timeframe for all lists is [18 months]):

    - All completed pre-employment checks for individuals with "L" or "Q" access authorizations

    - All individuals with "L" or "Q" access authorizations who had **absences of 90 days or more**; payroll records should be used to develop this listing.

- A listing of all contractor/sub-contractor employees for which INL has notified or reported to (the servicing DOE personnel security organization) information of personnel security interest as a result of a disciplinary action (the listing should not include security infraction reports like the one requested by the CMPC topic team). Please include the date reported to (the servicing DOE personnel security organization).

SAFEGUARDS AND SECURITY AWARENESS PROGRAM

- Provide a copy of the current procedure or a description of the badge process, including the process for acting upon a lost badge and retrieving badges from individuals who no longer require an access to XXX facilities and/or no longer are doing any work at XXX that requires access to classified information.

- Separate **alphabetized (last name first), line numbered** lists (use Excel, if possible) of all cleared employees. XXX should also provide a separate listing for subcontractor employees and their duty location(s).

- Provide documentation verifying both the completion of required DOE training by the SSAP coordinator and the appointment of the individual as the coordinator.

- Set dates and location(s) of all initial and comprehensive briefings being presented during this inspection (to allow HS-61 to attend selected presentations).

- Provide the following **separate, alphabetized (last name first) lists** for personnel **with a "Q" access authorization** (the timeframe for all lists is [18 months]):

  - Access authorization **terminations**; this list should **not** include transfers or any item other than a termination of access authorization

  - All employees (cleared and uncleared) whose **employment** was **terminated**; this data must be from the site Office of Human Resources or employment office

  - All individuals who have been **granted** an initial access authorization, the date action to grant that was taken by DOE**,** and the date a DOE security badge was issued

  - All individuals who have **transferred** from another DOE facility, the date action to transfer that was taken by DOE**,** and the date a DOE security badge was issued

  - All individuals who have had their access authorization **reinstated**, the date action to reinstate that was taken by DOE**,** and the date a DOE security badge was issued.

- Provide a **draft** of three versions of a security awareness questionnaire each consisting of 25 multiple choice and true or false questions.

  (In concert with HS-61, the XXX points of contact will develop the variations of a questionnaire that will be administered either on-line or in-person as applicable to randomly selected individuals. Each variation of the questionnaire should have five questions that are not repeated on the other variations.

The questionnaire should be based on initial, comprehensive, and annual refresher briefings, and should focus on the most important elements that employees are expected to remember.)

(HS-61 will determine the number of individuals who will be requested to complete the questionnaire, while the XXX points of contact will notify those chosen using a mutually agreed upon, random selection process to complete the questionnaire.)

HUMAN RELIABILITY PROGRAM

- Provide copy of the HRP implementation plans and documentation of review and approval by the Manager.

- Provide the following **separate, alphabetized (last name first) lists** for XXX enrolled in a **HRP program** (the timeframe for all lists is [18 months]):

    - All individuals enrolled in HRP; include each individual's duty position (as listed in the approved HRP implementation plan), and the name of the person who completes the annual supervisory review for each individual

    - All supervisors and their subordinates who are enrolled in HRP

    - All individuals pending HRP approval

    - All individuals who have been temporarily removed from HRP or had their HRP certification revoked for any reason (security, safety, medical or changes of position/employment); include the date of removal, reason for removal, and, if applicable, the date of reinstatement

    - All individuals who have been involved in an accident that was reported as an occurrence to DOE

    - All personnel who have been designated as individuals that are prohibited from consuming alcohol for eight hours preceding scheduled work.

- Provide a copy of the initial and annual unannounced drug and alcohol testing procedures and/or protocols.

- Provide a copy of procedures that describe the actions that will be taken for positive drug and alcohol test results.

- Provide a copy of all HRP instructional materials for supervisors, HRP-certified individuals, and site occupational medical providers.

- Provide a description of process used to evaluate and designate HRP positions.

- Assemble letters of designation/certification for the SOMD, Designated Physician, Designated Psychiatrist, breath analysis technicians, and drug testing technicians.

- Provide a list of breath alcohol and drug testing technicians.

- Provide copies of the letters that give the Designated Physician or Designated Psychiatrist authority to sign for the SOMD.

- Provide a list of equipment used for alcohol testing.

- Provide a list of positions and job titles for which JTAs have been developed and provided to medical personnel.

UNCLASSIFIED FOREIGN VISITS & ASSIGNMENTS

- Provide the total number of foreign national visits and assignments that have occurred at XXX between (a period of 18 months). Please also provide the number of foreign national visitors and assignees that are from a sensitive country or a terrorist country, and foreign visits and assignments that involved sensitive subjects and/or access to security areas (protected, limited, exclusion, and property protection areas).

- Assemble separate, **alphabetized (last name first)** listings or computer printouts of visits and assignments that have occurred between (18 months) for each of the following:

    - FV&As involving foreign nationals from sensitive countries

    - FV&As involving sensitive subjects

    - FV&As involving access to security areas (protected, limited- and property-protection areas)

    - FV&As involving foreign nationals from terrorist countries

    - Any foreign nationals who have approval for unescorted access to any XXX security area

    - All visiting foreign nationals who have been granted access to XXX computing assets, with a termination date for access to the computing assets

    - All foreign nationals visitors and assignees who have been granted remote access to XXX computing assets, with a termination date for remote access

    - All visiting foreign nationals who have been granted after-duty-hours access to XXX facilities

    - All foreign nationals who are related to incidents and inquiries of incidents of security concern

    - All of the most frequently visited site facilities and programs.

  Each of these lists should provide the following information: name and nationality of visitor/assignee, date of visit/assignment, name of host/escorts, facilities included in the scope of the visit/assignment, and, when applicable, approval for remote or on-site access to computing systems.

- Provide a diagram that depicts all site security areas (protected, limited, exclusion, and property protection areas, including building numbers). (Please provide a separate diagram from those provided in response to other topic team requests.)

- Provide procedures and/or protocols used to process and approve all FV&As.

- Provide an example of both a generic security plan and a specific security plan.

- Obtain a copy of host/escort guidance or training materials.

- Provide a procedure or description of how lessons learned are shared with other hosts/escorts.

REQUIRED DOCUMENTS / INFORMATION

Access to the following documents and/or information items will be required during the on-site phases of the inspection:

- Personnel Security Clearance Program
    - Pre-employment check files.
- SSAP
    - Initial, comprehensive, annual refresher, and termination briefings and any supporting materials/handouts
    - Records (e.g., attendance rosters, SF 312, *Classified Information Nondisclosure Agreement*, DOE F 5631.29) of completion of initial, comprehensive, refresher, and termination briefings.
- HRP
    - Records that document the completion of HRP initial and annual instruction
    - HRP records and HRP-associated medical and psychological files
    - JTAs that have been developed and provided to the Designated Physician(s) and Psychologist(s).
- FV&A
    - Requests for FV&As
    - Records of reviews and approvals of FV&As
    - Specific and generic security plans
    - Local Foreign Activities Central Tracking System (FACTS) terminal.

Methodology for Reviewing
Personnel Security Files

Block 1: Copy the name and DOE number from the file jacket.

Blocks 2, 3, 5 to 7: Review the clearance/access authorization request form on the left side (use information on the most recent form).

Block 4: Review the file summary sheet.

Block 8: Use the most recent background investigation (BI) on right side (first volume) of the file; use the date stamped on first page by the investigation agency.

Block 9: Insert the first case evaluation sheet (CES) after the most recent BI, on right side of the file.

Block 10: Use this section to evaluate how the most current issue(s) was adjudicated. The entries begin with the CES that first documented the issue(s) and continue until the issue(s) is adjudicated or the access authorization is denied or suspended, as follows:

- Initial Row, Column 1: **Analyst** and **Date** are taken from the CES that first documented the issue(s)
- Initial Row, Column 2 (Criteria): Found on the CES (↑ indicates more serious and ↓ indicates less serious)
- Initial Row, Column 3 (Resolution): Found on the CES; ensure that the analyst's recommendation is concurred upon by the peer/supervisor, when required
- Succeeding Rows: Same as Column 3 for each additional adjudication action until resolution or denial/suspension of access authorization.

Block 11: Derive information from the review of the CESs.

Block 12: Ensure that Office of Personnel Management (OPM) 79A was removed and returned after completion of clearance actions related to a background investigation for Federal employees.

PERSONNEL SECURITY FILE DATA COLLECTION FORM: DEROGATORY INFORMATION

PSF REVIEW FORM FOR DEROG FILES	**1. Name/File Number**	**2. Site/Employer & Work Location**	**3. Job Title/Position**	**4. AA Status** ☐ Initial/Applicant ☐ Incumbent ☐ Reinstate ☐ Other	**5. High-risk Program Status** ☐ Yes ☐ HRP ☐ SCI ☐ No	**6. Pre-employment Check Documented** ☐ Yes Date: ☐ No ☐ NA (if employment began more than 5 years ago)	**7. AA Justification Adequate** ☐ Yes Date: ☐ No ☐ NA	**8. Date Most Recent BI or partial BI (if last investigation) received:** **9. Most Recent BI Screened** Analyst: Date:

10. Identification and Resolution of Derogatory Information [beginning with the <u>most recent</u> issue(s)]

	CRITERIA OF ALL DEROGATORY INFORMATION	**RESOLUTION METHOD(s) TO RESOLVE DEROGATORY INFORMATION**
CASE EVALUATION SHEET (CES) **IDENTIFYING** the <u>MOST RECENT</u> issue(s) Analyst: Date:	Criteria: ____ Criteria:____ ↑ (major) or ↓ (minor) ↑ or ↓ ≤ 5 years or ≥ 5 years ≤ 5 years or ≥ 5 years Criteria: ____ Criteria:____ ↑ or ↓ ↑ or ↓ ≤ 5 years or ≥ 5 years ≤ 5 years or ≥ 5 years	**Initial** Additional Adjudicative Action: ☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed: **ACTION TAKEN AND DATE OF ACTION** ☐ G ☐ C ☐ S ☐ D ☐ N Date:
Complete for **each** additional CES develop as a result of the adjudicative actions that were required to resolve this issue.	**Second** Additional Adjudicative Action CES date:_____ Analyst:_____ ☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed: **ACTION TAKEN AND DATE OF ACTION** ☐ G ☐ C ☐ S ☐ D ☐ N Date::	**Third** Additional Adjudicative Action CES date:_____ Analyst:_____ ☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed: **ACTION TAKEN AND DATE OF ACTION** ☐ G ☐ C ☐ S ☐ D ☐ N Date::
	Fourth Additional Adjudicative Action CES date:_____ Analyst:_____ ☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved:	**Fifth** Additional Adjudicative Action CES date:_____ Analyst:_____ ☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved:

	Date Completed: **ACTION TAKEN AND DATE OF ACTION** ☐ G ☐ C ☐ S ☐ D ☐ N Date:	Date Completed: **ACTION TAKEN AND DATE OF ACTION** ☐ G ☐ C ☐ S ☐ D ☐ N Date:

CRITERIA:
A: Acts of Treason
B: Association
C: Membership
D: Overthrow of Government
E: Foreign Influence
F: Falsification

RESOLUTION METHOD:
G: Violation of Security Requirements
H: Emotional, Mental Disorders
I: Refusal to Testify
J: Alcohol Consumption
K: Use of or Trafficking in Illegal Drugs
L: Personal Conduct/Finance

LOI: Letter of Interrogatory
PSI: Personnel Security Interview
PE: Psychiatric Evaluation
CI: Counterintelligence Review (when applicable)
AR: Administrative Review

ACTION TAKEN:
G: Grant
C: Continue
S: Suspend
D: Deny
N: None Taken

11. Was consideration of applicable mitigating factors documented*? ☐ Yes ☐ No *Generic Mitigating Factors: Nature, extent and seriousness of the conduct Knowledgeable participation Age and maturity Presence or absence of behavioral changes Frequency and recency of the conduct Motivation Future intentions Potential for coercion	**12. For a Federal employee, was OPM Form 79A returned after completion of the security clearance determination?** ☐ Yes ☐ No

PERSONNEL SECURITY FILE DATA COLLECTION FORM: REINSTATEMENTS

1. Name & File Number	2. Site/Employer & Work Location	3a. Date of most recent QNSP: 3b. Date of the most recent Investigation:	4a. Date Access Authorization was last Terminated: 4b. Date Reinstatement Requested:	5. Was a QNSP, Parts I/II completed when 6 months elapsed since termination **and** more that 1 year elapsed since the date of the most recent QNSP? Yes ___ No ___	6. If over 5 years since the most recent investigation, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:
7. If the access authorization was terminated for more than 24 months and the individual was not employed by the same employer, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	8. If new derogatory information identified since termination, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	9. If the reason for termination concerned eligibility for an access authorization, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No ___ Date Submitted:	10. If last investigation was more than 10 years old, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	11. Date of reinstatement: Was Personnel Security File documented to reflect rationale for reinstatement action? Yes ___ No ___	12. Was a new DOE F 5631.18, "Security Acknowledgement" obtained? Yes ___ No ___ Date signed:

13. Summary of Inspector's Concerns:

1. Name & File Number	2. Site/Employer & Work Location	3a. Date of most recent QNSP: 3b. Date of the most recent Investigation:	4a. Date Access Authorization was last Terminated: 4b. Date Reinstatement Requested:	5. Was a QNSP, Parts I/II completed when 6 months elapsed since termination **and** more that 1 year elapsed since the date of the most recent QNSP? Yes ___ No ___	6. If over 5 years since the most recent investigation, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:
7. If the access authorization was terminated for more than 24 months and the individual was not employed by the same employer, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	8. If new derogatory information identified since termination, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	9. If the reason for termination concerned eligibility for an access authorization, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No ___ Date Submitted:	10. If last investigation was more than 10 years old, was a Supplemental Investigation submitted prior to or concurrent with the reinstatement? Yes ___ No___ Date Submitted:	11. Date of reinstatement: Was Personnel Security File documented to reflect rationale for reinstatement action? Yes ___ No ___	12. Was a new DOE F 5631.18, "Security Acknowledgement" obtained? Yes ___ No ___ Date signed:

13. Summary of Inspector's Concerns:

PERSONNEL SECURITY FILE DATA COLLECTION FORM: TERMINATIONS

PSF Review Form	1. File Number	2. Site/Employer & Work Location	3. Effective Date of Termination	4. Date Terminated in CPCI	5. Date AA Terminated in Site Database	6. Reason for Termination Documented? Yes___ No____	7. Did Individual Sign Security Termination Statement (STS)? Yes___ No___	8. Date Badge Retrieved

9. Summary of Inspector's Concern:

10. Site Response:

PSF Review Form	1. File Number	2. Site/Employer & Work Location	3. Effective Date of Termination	4. Date Terminated in CPCI	5. Date AA Terminated in Site Database	6. Reason for Termination Documented? Yes___ No____	7. Did Individual Sign STS? Yes___ No___	8. Date Badge Retrieved

9. Summary of Inspector's Concern:

10. Site Response:

PSF Review Form	1. File Number	2. Site/Employer & Work Location	3. Effective Date of Termination	4. Date Terminated in CPCI:	5. Date AA Terminated in Site Database	6. Reason for Termination Documented? Yes___ No____	7. Did Individual Sign STS? Yes___ No___	8. Date Badge Retrieved

9. Summary of Inspector's Concern:

10. Site Response:

PSF Review Form	1. File Number	2. Site/Employer & Work Location	3. Effective Date of Termination	4. Date AA Terminated in CPCI	5. Date AA Terminated in Site Database	6. Reason for Termination Documented? Yes___ No____	7. Did Individual Sign STS? Yes___ No___	8. Date Badge Retrieved

9. Summary of Inspector's Concern:

10. Site Response:

PERSONNEL SECURITY FILE DATA COLLECTION FORM: CLEAR CASES

PSF REVIEW FORM FOR CLEAR FILES	1. File Number	2. Site/Employer & Work Location	3. Job Title/Position	4. AA Status ☐ Initial/ Applicant ☐ Incumbent ☐ Reinstate ☐ Other	5. Pre-employment Check Documented ☐ Yes ☐ Date: ☐ No ☐ NA (if employment began more than 5 years ago)	6. AA Justification Adequate ☐ Yes ☐ No ☐ Date: ☐ NA	7. High-risk Program Status ☐ Yes ☐ No ☐ HRP ☐ SCI	8. Date Most Recent BI or partial BI (if last investigation) received: 9. Date Most Recent BI or partial BI screened: Analyst: Date:

10. No derogatory information ever identified.

11. Derogatory information identified, but determined to be insignificant and/or previously adjudicated. (Circle the applicable derogatory information type and the number of times each type of derogatory information had been identified; indicate if major [↑] or minor [↓], and recent [≤ 5 years] or old [≥ 5 years]; and circle the action taken)

Criteria of Derogatory Information		Action Taken
Acts of Treason	Violation of Security Requirements	Grant
Association	Emotional, Mental Disorders	Continue
Membership	Refusal to Testify	None Taken
Overthrow of Government	Alcohol Consumption	
Foreign Influence	Use of or Trafficking in Illegal Drugs	
Falsification	Personal Conduct/Finance	

12. Was consideration of applicable mitigating factors documented*?

☐ Yes ☐ No

*Generic Mitigating Factors:

-Nature, extent and seriousness of the conduct	-Frequency and recency of the conduct
-Knowledgeable participation	-Motivation
-Age and maturity	-Future intentions
-Presence or absence of behavioral changes	-Potential for coercion

13. For Federal employee, was OPM Form 79A returned after completion of the security clearance determination?

☐ Yes ☐ No

PERSONNEL SECURITY FILE DATA COLLECTION FORM: PENDING RE-INVESTIGATIONS

PSF REVIEW FORM FOR PENDING RE-INVESTIGATIONS **Rev-8/15/07**	**1. File Number**	**2. Site/Employer & Work Location**	**3. Job Title/Position**	**4. Pre-employment Check Documented?** ☐ Yes Date: ☐ No ☐ NA (if employment began more than 5 years ago)	**5. AA Justification** **Adequate** ☐ Yes ☐ No Date: ☐ NA	**6. High-risk Program Status** ☐Yes ☐ No ☐ HRP ☐ SCI	**7. Date Reinvestigation Submitted** **Received**	**8. Date of HS-61 File Review** **9. Date Nest Most Recent Previous BI Screened** Analyst: Date:

10. No derogatory information ever identified.

11. Derogatory information identified, but previously adjudicated. (circle the applicable derogatory information type and the number of times each type of derogatory information had been identified; indicate if major [↑] or minor [↓], and/or if recent [≤ 5 years] or old [≥ 5 years]

Criteria of Derogatory Information

Acts of Treason	Violation of Security Requirements
Association	Emotional, Mental, and Personality Disorders
Membership	Refusal to Testify
Overthrow of Government	Alcohol Consumption
Foreign Influence	Use of or Trafficking in Illegal Drugs
Falsification	Personal Conduct/Finance

12. Did the investigation report identify any new derogatory information?

☐ Yes ☐ No

If so, . (circle the applicable derogatory information type and the number of times each type of derogatory information had been identified; indicate if major [↑] or minor [↓], and recent [≤ 5 years] or old [≥ 5 years]indicate the applicable criteria:

Acts of Treason	Violation of Security Requirements
Association	Emotional, Mental and Personality Disorders
Membership	Refusal to Testify
Overthrow of Government	Alcohol Consumption
Foreign Influence	Use of or Trafficking in Illegal Drugs
Falsification	Personal Conduct/Finance

13. Site's subsequent review (after identifying pending status in the data call) of the reinvestigation report:

Date Reviewed: **Analyst:**
Adjudicative Action Taken: ☐ **LOI** ☐ **PSI** ☐ **PE** ☐ **Adjudicate on Record** **Date Action Recommended:** **Date Approved:** **Date Initiated:**
Final Action Taken: ☐ **Grant** ☐ **Continue** ☐ **Recommend Suspension** ☐ **None/Pending** **Date Final Action Taken:**

14. Summary of Inspector's Concerns

PERSONNEL SECURITY FILE DATA COLLECTION FORM: UNSCREENED FILES

PSF REVIEW FORM FOR UNSCREENED FILES	**1. Name & File Number**	**2. Site/ Employer & Work Location**	**3. Job Title/ Position**	**4. AA Status** ☐ Initial/ Applicant ☐ Incumbent ☐ Reinstate ☐ Other	**5. High-risk Program Status**? ☐ Yes ☐ No ☐ HRP ☐ SCI	**6. Pre-employment Check Documented?** ☐ Yes/date: ☐ No ☐ NA (if employment began more than 5 years ago)	**7. AA Justification Adequate?** ☐ Yes Date: ☐ No ☐ NA	**8. Date Unscreened Report Received** Personnel Security Organization: Adjudicative Analyst:	**9. When Applicable, Date Report Screened by Site after Receipt of Data Call** Analyst: Date: (See Block 10 B)

10. Identification of Derogatory Information Contained in Unscreened Report

A. RESULTS OF *HS-61* REVIEW OF AN UNSCREENED REPORT	**CRITERIA OF <u>NEW/UNRESOLVED</u> DEROGATORY INFORMATION CONTAINED IN THE UNSCREENED REPORT**	**CRITERIA OF <u>PREVIOUSLY IDENTIFIED</u> DEROGATORY INFORMATION CONTAINED IN THE UNSCREENED REPORT**	**RESOLUTION METHOD**(s)	**ACTION TAKEN AND DATE OF ACTION**
	☐ Criteria A, Acts of Treason ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria A, Acts of Treason ↑ or ↓ ≤ 5 years or ≥ 5 years A:	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria B, Association ↑ or ↓ ≤ 5 years or ≥ 5 years ☐ B:	☐ Criteria B, Association ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria C, Membership ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria C, Membership ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria D, Overthrow of Government ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria D, Overthrow of Government ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria E, Foreign Influence ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria E, Foreign Influence ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:

	☐ Criteria F, Falsification ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria F, Falsification ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria H, Emotional, Mental Disorders ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria H, Emotional, Mental Disorders ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria I, Refusal to Testify ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria I, Refusal to Testify ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria J, Alcohol Consumption ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria J, Alcohol Consumption ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria K, Use of or Trafficking in Illegal Drugs ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria K, Use of or Trafficking in Illegal Drugs ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:
	☐ Criteria L, Personal Conduct/Finances ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ Criteria L, Personal Conduct/Finances ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Rec: Date Approved: Date Completed:	☐ G ☐ C ☐ S ☐ R ☐ N Date:

	CRITERIA OF <u>NEW</u> DEROGATORY INFORMATION CONTAINED IN THE PREVIOUSLY UNSCREENED REORT	**RESOLUTION METHOD**(s)	**ACTION TAKEN AND DATE OF ACTION**
B. NEW DEROGATORY INFORMATION IDENTIFIED DURING *SITE* REVIEW OF A PREVIOUSLY UNSCREENED REPORT	☐ Criteria A, Acts of Treason ↑ or ↓ ≤ 5 years or ≥ 5 years :	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria B, Association ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria C, Membership ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria D, Overthrow of Government ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:

	☐ Criteria E, Foreign Influence ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria F, Falsification ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria H, Emotional, Mental Disorders ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria I, Refusal to Testify ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria J, Alcohol Consumption ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria K, Use of or Trafficking in Illegal Drugs ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:
	☐ Criteria L, Personal Conduct/Finances ↑ or ↓ ≤ 5 years or ≥ 5 years	☐ LOI ☐ PSI ☐ PE ☐ CI ☐ AR Date Recommended: Date Approved: Date Completed:	☐ G ☐ C ☐ R ☐ N Date:

RESOLUTION METHODS:
LOI: Letter of Interrogatory
PSI: Personnel Security Interview
PE: Psychiatric Evaluation
CI: Counterintelligence Review
AR: Administrative Review

ACTION TAKEN:
G: Grant
C: Continue
S: Suspend
R: Revoke
N: None/Pending

INTERVIEW QUESTIONS: PERSONNEL SECURITY ORGANIZATION MANAGER

1. Provide an overview of your organization (number of Federal and contractor analysts, other contractor support, reporting chain, number of clearances supported for each site, etc.).

2. Describe roles and responsibilities for you (5 percent reviews, supervisor approval of psychiatric evaluations, etc.) and your organization.

3. Are you currently operating under any deviations?

4. Describe the tenure and skill of your staff.

5. Describe in-house training activities.

6. How often does your staff attend external training?

7. Describe the manner in which internal procedures are provided to the staff?

8. How is work assigned (cradle-to-grave or random)?

9. How is work prioritized?

10. How do you maintain consistency of operations (action to resolve derogatory information, determination of clear files, seriousness of potentially disqualifying information, etc.)?

11. Do you have a backlog in requesting or completing reinvestigations? If so, what actions are being taken?

12. How is your program periodically assessed/surveyed? Who conducts these assessments?

13. What are your responsibilities to Safety System Oversight (in accordance with the Memorandum of Understanding)?

HRP INTERVIEW QUESTIONS: HRP OFFICIALS (CERTIFYING OFFICIAL, MANAGEMENT OFFICIAL/ADMINISTRATOR)

(Use the questions below as applicable to the role of the individual.)

1. **What are your HRP responsibilities?** (Certifying Official certifies, recertifies, temporarily removes, and/or reinstates. Management Official has programmatic responsibility for HRP positions, receives information from a wide variety of sources, and makes a determination whether an individual should be temporarily removed from HRP duties; conducts the annual management evaluation of the supervisor, medical, and drug and alcohol test results; notifies personnel security office of security concerns; oversees drug and alcohol testing; and ensures the initial and annual training of HRP supervisors, employees, and medical personnel.)

2. **Who supports you in your role?** (Include the experience level of those responsible for HRP – e.g., SOMD, HRP administrators/coordinators, support contractors.)

3. **What process did you utilize for determining which positions should be designated as HRP?**

4. **How do you (and what site procedures) ensure that no individual performs HRP duties prior to certification?** (Access control system?)

5. **How many times are individuals allowed to be escorted into a MAA or allowed access to nuclear explosives or nuclear weapon components to train/observe HRP operations prior to being certified?**

6. **How do you ensure that supervisors of record** (those who signed the 470.3) **have enough interaction with their HRP employees to perform the supervisory review?**

7. **How do you ensure that the annual recertifications are completed on time?** (Do you utilize a report from an automated database or do you start the HRP process *X* months prior to the anniversary date?)

8. **How do you ensure that HRP individuals are reporting prescription medication or other medication that could cause cognitive impairment?** (What do you do if they do not report their medication? How do you ensure that your medical personnel are asking if the HRP patient is taking any prescription medication or other medication that could cause cognitive impairment?)

9. **What processes and protocols are used to ensure that information is shared between HRP officials, medical personnel, and security officials?** (Describe each example.)

10. **Have there been any HRP immediate removals, temporary removals, or medical restrictions during the last 18 months?** (Ask for specific examples first and then names for each type of removal.)

11. **How often do you meet with or interact** (telephone or e-mail) **with the HRP Certifying Official?**

12. Concerning drug and alcohol testing:

- Are people selected and tested on the same day?
- Do you have any maximum number of random tests before chances of selection decrease?
- What are considered reasonable excuses for not reporting for testing?
- How is this conveyed to the employees and supervisors?
- How is this enforced?

13. How do you ensure that individuals who have been removed by supervisors are denied access to MAAs, nuclear weapons, or nuclear weapon components? (How do you ensure timeliness in their removal from access control systems and that they are prohibited from performing HRP duties?)

HRP INTERVIEW QUESTIONS: MEDICAL OFFICIALS (SOMD, DESIGNATED PHYSICIANS, AND DESIGNATED PSYCHOLOGISTS)

1. **What is the name of your HRP Management Official and the HRP Certifying Official?**

2. **How do you know that you are evaluating/interviewing an HRP person?** (File color? Engraved plate?)

3. **What medical conditions or behaviors that would cause you to recommend removing an individual from HRP?** (When security concerns are found as a result of your evaluations? To whom do you report your concerns? Have you ever reported any security concerns [name these individuals]? How are security concerns documented in the medical or psychological file?)

4. **What medications do you believe could cause cognitive impairment?** (When notified that an HRP employee is taking such medication, have you recommended to the HRP Management/Certifying Official that the individual be temporarily removed?)

5. **What actions do you take when you believe that someone has an alcohol problem?** (What follow-up would be conducted to confirm a problem? Would there be evidence of these actions in the medical or psychological file? If appropriate: In the last 18 months have you had any such case [names these cases]?)

6. **After your decision to recommend temporary removal of someone, how soon must you notify DOE?** (Answer should be: Immediately, but no greater than 24 hours.)

7. **Have you been HRP trained? If so, how, what, when? If not, why not? Where is it documented?** (Training should include a detailed explanation of HRP duties and responsibilities, designated physician and psychologist reporting responsibilities, and the process for temporary removal recommendation and returning to work.)

8. **Have you placed medical restrictions on any HRP employee(s)?** If so, who do you notify and how is it documented?

9. **Have you ever recommended that anyone be temporarily removed from HRP? If so, for what reasons?** (Prescription medications, over-the-counter [OTC] drugs, illnesses, conditions that do not meet the standards of the JTA.) (Provide names of these individuals.)

10. **Have you read 10 CFR 712?**

SITE OCCUPATIONAL MEDICAL DIRECTOR

1. **What are your primary responsibilities under HRP?**
   (Answer should include:
   - Make a recommendation based on the HRP assessment.
   - Submit annual report on the HRP medical activity to the DOE Deputy Assistant Secretary for Health or his/her designee.
   - Take responsibility for the medical assessment of HRP candidates and HRP-certified individuals.

- Nominate an HRP physician and psychologist and re-nominate them biennially.
- Investigate reports of performance issues regarding the Designated Physician/Psychologist.)

2. **Do you review all recommendations for HRP eligibility?** (Does the Designated Physician sign the 470.3 for you? If so, where is the Letter of Authority delegating that responsibility?)

3. **Who is the Medical Review Officer (MRO)?**
(Answer: MRO is the medical official who certifies that drug tests are positive and/or negative.)

4. **How have you ensured that the results of the physical and the psychological assessments are reviewed in their entirety before completing an HRP eligibility recommendation and signing the 470.3?** (How do you ensure that the JTA has been reviewed prior to an assessment and subsequent HRP determination?)

DESIGNATED PHYSICIAN

1. **What are your primary responsibilities under HRP?**
(Answer: To evaluate whether an HRP or HRP-certified individual, the Designated Physician should determine whether the individual:
   - Represents a security concern
   - Has a condition that may prevent the individual from performing HRP duties in a reliable and safe manner
   - Is subject to the existence or nature of any of the following:
     - Physical or medical disabilities, such as a lack of visual acuity, defective color vision, impaired hearing, muscular skeletal deformities, and neuromuscular impairment
     - Use of illegal drugs or the abuse of legal drugs or other substances as identified by self-reporting or medical/psychological evaluation or testing
     - Medical conditions such as cardiovascular disease, endocrine disease, cerebrovascular or other neurological disease
     - Conditions that are treated by drugs that may adversely affect the individual's judgment or ability to perform assigned duties in a reliable and safe manner.)

2. **What information do you consider before determining HRP eligibility? (**Is the psychological assessment considered? JTA?)

3. **Have you been provided a JTA for each of the HRP positions?** (Where are the JTAs kept? How do you ensure that the JTA is reviewed prior to an assessment and subsequent HRP determination?)

4. **Do you utilize physician assistants, nurse practitioners, or other (**non-HRP designated**) physicians to perform the HRP medical assessment? (**Do you review and approve their assessments prior to signing the 470.3 form? How is this documented?)
(Answer: Yes, CFR 712.32, (c) (1-6) and CFR 712.36, (f).)

DESIGNATED PSYCHOLOGIST

1. **What are your primary responsibilities under HRP?**

(Answer: To evaluate whether an HRP or HRP certified individual, the Designated Psychologist should determine whether the individual:

- Represents a security concern
- Has a condition that may prevent the individual from performing HRP duties in a reliable and safe manner
- Has a mental or personality disorder or behavior problem, including alcohol and other substance use, disorders as described in the Diagnostic and Statistical Manual of Mental Disorders
- Uses illegal drugs or abuses legal drugs or other substances as identified by self-reporting or medical/psychological evaluation or testing
- Is a threat for suicide, homicide, or physical harm?)

2. **How often is the Minnesota Multiphasic Personality Inventory (MMPI) used as a part of the psychological assessment given to HRP personnel?**
   (Answer: Every third year.)

3. **What information do you consider before determining HRP eligibility?** (Is the psychological assessment considered? JTA?)

4. **Have you been provided a JTA for each of the HRP positions?** (Where are the JTAs kept? How do you ensure that the JTA is reviewed prior to an assessment and subsequent HRP determination?)

5. **Does the SOMD/Designated Physician review your recommendation for HRP eligibility prior to signing the 470.3 form?**
   (Answer: Yes, CFR 712.33, (a) and CFR 712.36, (f).)

INTERVIEW QUESTIONS: FV&A PROGRAM MANAGER

Name: _____

Phone Number:_____

1. Describe responsibilities of the coordinator/administrator.

   _____
   _____
   _____

2. Describe FV&A organization (e.g., number of staff, qualifications).

   _____
   _____
   _____

3. Describe the FV&A process (e.g., request to closeout, who is authorized to approve). (You might need to interview specific subject matter experts to determine the elements of their review.)

   _____
   _____
   _____

4. If used, how often are counterintelligence consultations used in lieu of completion of indices checks (as a possible indication of late submission of requests)?

   _____
   _____
   _____

5. Describe how security plans are developed. Does the review of security plans indicate that they are adequate to control the foreign national?

   _____
   _____
   _____

6. Describe the local FV&A database.

   _____
   _____
   _____

7. How is information on the local FV&A database uploaded onto FACTS?

   _____
   _____
   _____

8. How is visa/Immigration and Naturalization Service information obtained and documented?

   _____
   _____
   _____

9. How are badges issued and retrieved from foreign nationals?

   _____
   _____
   _____

10. When was the last self-assessment of the FV&A program? What were the results of this self-assessment?

    _____
    _____
    _____

11. Is the host report used as a feedback mechanism or just to meet the base requirement? (If the report is not used, you might want to recommend that the coordinator consider expanding the use of the host report to obtain feedback on how well the FV&A process is working.)

    _____
    _____
    _____

12. Are there any foreign national visitors/assignees from a terrorist state? If so, who approved these visits or assignments?

    _____
    _____
    _____

13. How are hosts/escorts/foreign nationals informed/trained on their responsibilities?

    _____
    _____
    _____

14. Review 20 to 40 files (randomly select from the lists provided in the document call, usually focus on sensitive area visits, but pick some from the entire sensitive group) to determine whether all elements of the request process were completed prior to the start of a visit/assignment.

    _____
    _____
    _____

15. During the Item 14 (immediately above) review associated security plans to determine whether all hosts and escorts have been identified, whether all authorized locations have been identified, and whether all restrictions are included.

    _____
    _____
    _____

INTERVIEW QUESTIONS: FV&A HOSTS AND ESCORTS

Name: _____

Phone Number:_____

1. What are your responsibilities?

_____
_____
_____

2. How were you informed of your responsibilities?

_____
_____
_____

3. What control measures are/were in place for this visit/assignment?

_____
_____
_____

4. What is the location of the nearest security interests/classified repositories?

_____
_____
_____

5. Explain the request process.

_____
_____
_____

6. Describe the process you used to develop the security plan (if applicable).

_____
_____
_____

7. Tour of the area during which the host/escort can explain how the foreign national was controlled.

_____
_____
_____

INTERVIEW QUESTIONS: SSAP COORDINATOR

Name: _____

Phone Number:_____

1. How long have you been the coordinator?_____
2. Describe your responsibilities concerning the SSAP and what staff has been assigned to assist you.

_____
_____
_____

3. Do you have a copy of DOE Manual 470.1-1?_____
4. What training have you received to complete your coordinator responsibilities?

_____
_____
_____

5. Have you been formally appointed?
6. ☐ Yes ☐ No
7. How are awareness briefings developed and updated?

_____
_____
_____

8. What processes are in place to ensure that individuals attend all required briefings?

_____
_____
_____

9. Describe the measures that are in place to ensure that an individual does not have access to classified matter or SNM prior to completion of the comprehensive briefing (to include badge issuance).

_____
_____
_____

10. How is attendance at briefings or completion of awareness activities documented?

_____
_____
_____

11. What materials (e.g., posters, newsletters, online reminders) are used to supplement the awareness briefings?

_____
_____
_____

12. What steps are taken when an individual fails to attend/complete the annual refresher briefing?

_____
_____
_____

HRP INCUMBENT QUESTIONNAIRE

Organization:_____ Date:_____

1. Check **all** responses that you believe apply to you for completing the following sentence.

   My current position

   ☐ Affords me unescorted access to Category I SNM or I have the responsibility for transporting or protecting Category I quantities of SNM.

   ☐ Involves nuclear explosives duties (i.e., work assignments that allow custody of a nuclear explosive or access to a nuclear explosive device or area) or has responsibility for working with , protecting, or transporting nuclear explosives, nuclear devices, or selected components.

   ☐ Affords me access to information concerning vulnerabilities in protective systems when transporting nuclear explosives, nuclear devices, selected nuclear weapons components, or Category I quantities of SNM.

   ☐ Affords me the potential to significantly impact national security or cause unacceptable damage (i.e., an incident that could result in a nuclear detonation; high-explosive detonation or deflagration from a nuclear explosive; the diversion, misuse or removal of Category I SNM; or an interruption of nuclear explosive operations with a significant impact on national security).

2. Check **all** responses that you believe apply to you for completing the following sentence.

   Prior to being certified in the HRP

   ☐ I received HRP specific training.
   ☐ I had unescorted access to and in the material access area.
   ☐ I was tested for drugs and alcohol.
   ☐ I had access to a Category I quantity of SNM.
   ☐ I had to undergo a counterintelligence polygraph test.

3. What is the objective of the HRP? (Check the **one** response that you think is **best.**)

   ☐ To ensure appropriate levels of protection against unauthorized access, theft, diversion, loss of custody, or destruction of nuclear weapons; espionage; loss or theft of classified matter or Government property; and other hostile acts.

   ☐ To ensure that individuals with access to Category I quantities of SNM, and/or nuclear explosives meet the highest standards of reliability and physical and mental suitability.

   ☐ To ensure that individuals are processed for, granted, and retain a DOE access authorization only when their official duties require such access.

4. Which of the following are **your** responsibilities under the HRP? (Check **all** responses that you believe apply.)

   ☐ Read, sign, and submit releases, acknowledgments, and waivers.
   ☐ Complete and submit an annual financial statement.
   ☐ Provide full, frank, and truthful answers to questions and supply information that DOE requires to reach a certification determination.

5. Which of the following are required steps for initial certification or recertification in HRP? (Check **all** responses that you believe apply.)

   ☐ Possess a DOE "Q" access authorization (clearance).
   ☐ Participate in an annual force-on-force performance test.
   ☐ Undergo an initial CI evaluation, including a polygraph.
   ☐ Participate in a peer review (initial and annually).
   ☐ Undergo an initial and annual medical and psychological examination, management evaluation, supervisor review, and DOE security review.
   ☐ Receive an annual inoculation for the flu.
   ☐ Participate in initial and annual random drug and alcohol testing.

6. Prior to HRP certification and receiving your "Q" access authorization, were you ever escorted into the material access area? If you answered yes, how many times were you escorted into an MAA? (Check the **most** accurate response.)

   ☐ One to five times
   ☐ Six to 20 times
   ☐ More than 20 times

7. In addition to reporting requirements related to your holding a "Q" access authorization (e.g., bankruptcies, cohabitation, fines over $250), which of the following concerns do you believe you are **specifically** required to report about yourself or other HRP employees? (Check **all** responses that you believe apply.)

   ☐ Injury that could affect performance of duties (e.g., ability to operate a machine, vehicle, or weapon)
   ☐ Attempted or threatened destruction of property or life
   ☐ Change in address
   ☐ Driver's license expiration
   ☐ Failure to comply with work directives and safety or security procedures
   ☐ Significant behavior changes, moodiness, or depression.

8. How often are you required to be recertified in HRP? (Check only **one** response.)

   ☐ 6 months
   ☐ 12 months
   ☐ 24 months (2 years).

9. While you have been a HRP certified employee, have you ever been restricted from having unescorted access to the material access area?

   ☐ Yes ☐ No

10. If you answered Yes to question 9, for which of the following reasons were you restricted from having unrestricted access to the material access area?. (Check **all** responses that apply.)

    ☐ Taking of prescription medications
    ☐ Disciplinary action
    ☐ Not being certified prior to your anniversary date
    ☐ Security issue
    ☐ Other: _____

11. Have you ever been immediately or temporarily removed from HRP?

    ☐ Yes ☐ No

12. What are the requirements for returning to work after an absence due to illness of five or more days? (Check only **one** response.)

    ☐ Call your supervisor the day before returning to work.
    ☐ Report to the site medical organization and be evaluated by a doctor for clearance to return to work.
    ☐ Arrive at your duty location at the normal start time.

13. Have you undergone drug and alcohol testing during the last 12 months?

    ☐ Yes ☐ No

14. What is the **maximum** amount of time allowed for you to report to the drug/alcohol testing station after being notified of being selected for random testing? (Check only **one** response.)

    ☐ 30 minutes
    ☐ 1 hour
    ☐ 2 hours
    ☐ No time limit is in effect at my site

15. HRP includes provisions for due process (legal proceedings to protect your rights) if you are notified of the decision to deny (applicant) or revoke (incumbent) your HRP certification.

    ☐ True ☐ False

16. If you have been temporarily removed from HRP, were you allowed to enter the material access area under the escort of another HRP-certified employee?

    ☐ Yes ☐ No

17. Which of the following behaviors or circumstances could likely compromise an individual's judgment or reliability, and represent insider risk issues? (Check **all** responses that you believe apply.)

    ☐ Use of illegal drugs
    ☐ Playing practical jokes
    ☐ Habitual excessive use of alcohol
    ☐ Psychological disorders
    ☐ Excessive number of outgoing private phone calls

18. Which of the following are conducted as part of the annual recertification? (Check **all** responses that you believe apply.)

    ☐ Random drug and alcohol tests
    ☐ Supervisory reviews
    ☐ Annual filing of income tax returns with the Internal Revenue Service
    ☐ DOE personnel security reviews
    ☐ Medical evaluations

HRP SUPERVISOR QUESTIONNAIRE

Organization:_____ Date:_____

1. What is the objective of the HRP? (Check the **one** response that you think is **best.**)

   ☐ To ensure appropriate levels of protection against unauthorized access, theft, diversion, loss of custody, or destruction of nuclear weapons; espionage; loss or theft of classified matter or Government property; and other hostile acts.

   ☐ To ensure that individuals with access to Category I quantities of special nuclear material, and/or nuclear explosives meet the highest standards of reliability and physical and mental suitability.

   ☐ To ensure that individuals are processed for, granted, and retain a DOE access authorization only when their official duties require such access.

2. Which of the following are your **supervisory** responsibilities under the HRP? (Check **all** responses that you believe apply.)

   ☐ Ensure HRP candidates under your supervision have executed appropriate HRP releases, acknowledgments, and waivers.

   ☐ Immediately remove an HRP employee under your supervision from performing HRP duties when warranted.

   ☐ Report to the HRP Management Official any behavior or conditions that causes you any concerns about an HRP employee's ability to perform his/her HRP duties.

   ☐ Ensure that an HRP-certified employee under your supervision is sent home and not allowed to perform HRP duties for 24 hours when notified that the employee has tested positive for alcohol use (concentration greater than 0.02 percent).

3. How often do you have face-to-face contact with your HRP-certified employees?

   ☐ Once a day
   ☐ More than once a day
   ☐ All day long (for example, frequent contact due to working in the same area or office)
   ☐ Never or rarely on a daily basis.

4. If you do have daily contact with your HRP-certified employees, which of the following actions do you take when completing the annual supervisory review? (Check **all** responses that you believe apply.)

   ☐ Interview the employee at the time of the annual review.
   ☐ Contact intermediate supervisors to discuss the employee's performance of HRP duties.

- ☐ Base the annual supervisory review solely on information officially reported to me by Human Resources, Employee Relations, Internal Inquiries, etc.
- ☐ Not required to obtain additional information at my site.
- ☐ Not applicable (I do not have daily contact with my HRP-certified employees).

5. Prior to HRP certification, were any of your HRP employees ever escorted into a material access area?

   ☐ Yes ☐ No

6. If you answered Yes to question 5, what was the reason(s) for the escorted access? (Check **all** responses that you believe apply.)

   - ☐ On-the-job training
   - ☐ Familiarization tour(s)
   - ☐ Other: _____

7. Which of the following are **required** steps for initial certification or recertification in HRP? (Check **all** responses that you believe apply.)

   - ☐ Possess a DOE "Q" access authorization (clearance).
   - ☐ Participate in an annual force on force performance test.
   - ☐ Undergo an initial CI evaluation, including a polygraph.
   - ☐ Participate in a peer review (initial and annually).
   - ☐ Undergo an initial and annual medical and psychological examination, management evaluation, supervisor review, and DOE security review.
   - ☐ Receive an annual inoculation for the flu.
   - ☐ Participate in initial and annual random drug and alcohol testing.

8. In addition to reporting requirements related to your holding a "Q" access authorization (e.g., bankruptcies, cohabitation, fines over $250), which of the following concerns about your HRP employees do you believe **you** are **specifically** required to report to the HRP Management Official? (Check **all** responses that you believe apply.)

   - ☐ Injury that could affect performance of duties (e.g., ability to operate a machine, vehicle or weapon)
   - ☐ Attempted or threatened destruction of property or life
   - ☐ Change in address
   - ☐ Driver's license expiration
   - ☐ Failure to comply with work directives and safety or security procedures
   - ☐ Significant behavior changes, moodiness, or depression.

9. How often is an HRP-certified employee required to be recertified in HRP? (Check only **one** response.)

   - ☐ 6 months
   - ☐ 12 months

☐ 24 months (2 years).

10. If you immediately remove one of your employees from performing your HRP duties, you must provide a written reason to the HRP Management Official within 24 hours.

    ☐ True ☐ False

11. HRP includes provisions for due process (i.e., legal proceedings to protect an employee's rights) if an employee is notified of the decision to revoke his/her HRP certification.

    ☐ True ☐ False

12. What are the HRP requirements for an employee to return to work after an absence due to illness of five or more days? (Check only **one** response.)

    ☐ Call the supervisor the day before returning to work.
    ☐ Report to the site medical organization and be evaluated by a physician and/or psychologist for clearance to return to work.
    ☐ Arrive at the duty location at the normal start time.

13. How long does an HRP-certified individual have to report to the drug/alcohol testing station after being notified of being selected for random testing?

    ☐ 30 minutes
    ☐ 1 hour
    ☐ 2 hours
    ☐ No time limit is in effect at my site.

14. Which of the following behaviors or circumstances could likely compromise an individual's judgment or reliability, and represent insider risk issues? (Check **all** responses that you believe apply.) (Some respondents might check all five answers and this would be acceptable, although not optimal.)

    ☐ Use of illegal drugs
    ☐ Playing practical jokes
    ☐ Habitual excessive use of alcohol
    ☐ Psychological disorders
    ☐ Excessive numbers of outgoing private phone calls.

15. Which of the following **annually** conducted activities are included in the system of continuous evaluation that has been put into place to identify insider risks posed by HRP-certified individuals? (Check **all** responses that you believe apply.)

    ☐ Random drug and alcohol tests
    ☐ Supervisory reviews
    ☐ Counterintelligence polygraph tests
    ☐ Annual filing review of income tax returns with the Internal Revenue Service

☐ DOE personnel security reviews
☐ Medical evaluations.

16. After an employee has been temporarily removed from their HRP position, is he/she allowed to enter the material access are under escort?

☐ Yes ☐ No

17. If you answered Yes to question 16, what was the reason(s) for the escorted access? (Check **all** the responses that you believe apply.)

☐ Complete normal HRP duties.
☐ Complete other non-HRP duties.
☐ Other: _____

DRUG COLLECTION TECHNICIAN TEST

Name:_____ Date:_____

Position Title:_____ Number of years in position:_____

Are your training and certifications current? _____ Yes _____No _____ Not Certain

1. If an employee refuses to cooperate with the urine collection, he/she will be treated as if he/she had a positive test result.

   ☐ True
   ☐ False

2. Which government regulation(s) contain specific rules or guidance to be followed when collecting urine samples? (Select **two** responses that you believe are correct.)

   ☐ DOE 10 CFR, Part 710 – "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material"
   ☐ DOE 10 CFR, Part 707 – "Workplace Substance Abuse Programs at DOE Sites"
   ☐ DOT 49 CFR, Part 40 – "Procedures for Transportation Workplace Drug and Alcohol Testing Programs"
   ☐ Department of Health and Human Services Mandatory Guidelines for Federal Workplace Drug Testing Programs
   ☐ DOE Order 3428.3b – "Drug and Alcohol Testing Procedures"

3. From the time of notification, how much time is allowed for an HRP employee to reach the collection site? (Select **one** response.)

   ☐ 3 hours
   ☐ 4 hours
   ☐ 2 hours
   ☐ No time limit required at my site

4. Which of the following unusual behaviors or appearances would you be required to list on the specimen chain of custody form? (Select **three** responses that you believe are correct.)

   ☐ Did not want to wash hands
   ☐ Smoked 15 minutes prior to entry of testing site
   ☐ Showed erratic behavior
   ☐ Showed drowsiness.

5. The employee and the collection technician must keep the specimen in view at all times.

   ☐ True
   ☐ False

6. If a donor refuses to show the drug collection technician the items in his or her pockets, this is considered a refusal to test.

   ☐ True
   ☐ False

7. An employee is to be instructed to wash and dry his/her hands prior to urination.

   ☐ True
   ☐ False

8. After collection, how much time does the technician have to measure the temperature of the urine? (Select **one** response.)

   ☐ Not to exceed 3 minutes
   ☐ Not to exceed 5 minutes
   ☐ Not to exceed 4 minutes

9. If a technician suspects a specimen has been adulterated or diluted, the specimen is: (Select **one** response.)

   ☐ Discarded and a new specimen obtained
   ☐ Forwarded for testing and a new specimen obtained
   ☐ Discarded and treated as a positive test result
   ☐ Forwarded for testing and suspicions noted on chain of custody form.

10. If the collected urine volume is less than required and the temperature is within acceptable range, the specimen is discarded and a second specimen is collected.

    ☐ True
    ☐ False

11. When using a split specimen, what is the least amount of urine that can be collected? (Select **one** response.)

    ☐ 45 ml
    ☐ 15 ml
    ☐ 36 ml
    ☐ 30 ml

12. If necessary, bleach may be used as a substitute for bluing.

    ☐ True
    ☐ False

13. The employee must initial the label on the specimen bottle certifying it was collected from him/her.

    ☐ True
    ☐ False

14. What is the appropriate temperature range of the urine? (Select **one** response.)

    ☐ 86 to 98 degrees F
    ☐ 90 to 100 degrees F
    ☐ 90 to 96 degrees F

15. If the collected urine volume is less than required and the temperature is outside the acceptable range, the employee must be tested under direct observation.

    ☐ True
    ☐ False

NOTE: If your Site uses a different procedure that is not listed or contradicts a statement, please use the back of this form to provide any additional information you feel necessary.

DRUG COLLECTION TECHNICIAN
ANSWER SHEET

1. If an employee refuses to cooperate with the urine collection, he/she will be treated as if he/she had a positive test result.

   ■ **True (707.12(b)(1))**
   ☐ False

2. Which government regulation(s) contain specific rules or guidance to be followed when collecting urine samples? (Select **two** responses that you believe are correct.)

   ☐ DOE 10 CFR, Part 710 – "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material"
   ■ **DOE 10 CFR, Part 707 – "Workplace Substance Abuse Programs at DOE Sites"**
   ☐ DOT 49 CFR, Part 40 – "Procedures for Transportation Workplace Drug and Alcohol Testing Programs"
   ■ **Department of Health and Human Services Mandatory Guidelines for Federal Workplace Drug Testing Programs**
   ☐ DOE Order 3428.3b – "Drug and Alcohol Testing Procedures"

3. From the time of notification, how much time is allowed for an HRP employee to reach the collection site? (Select **one** response.)

   ☐ 3 hours
   ☐ 4 hours
   ■ **2 hours (712.15(b))**
   ☐ No time limit required at my site

4. Which of the following unusual behaviors or appearances would you be required to list on the specimen chain of custody form? (Select **three** responses that you believe are correct.) **(HHS, Section 2.2(f)(8))**

   ■ **Did not want to wash hands**
   ☐ Smoked 15 minutes prior to entry of testing site
   ■ **Showed erratic behavior**
   ■ **Showed drowsiness**

5. The employee and the collection technician must keep the specimen in view at all times.

   ■ **True (707.12(2) and HHS 2.2(f)(17))**
   ☐ False

6. If a donor refuses to show the drug collection technician the items in his or her pockets, this is considered a refusal to test.

   ■ **True (HHS 2.2(f)(4))**
   ☐ False

7. An employee is to be instructed to wash and dry his/her hands prior to urination.

   ■ **True (HHS 2.2(f)(5))**
   ☐ False

8. After collection, how much time does the technician have to measure the temperature of the urine? (Select **one** response.)

   ☐ Not to exceed 3 minutes
   ☐ Not to exceed 5 minutes
   ■ **Not to exceed 4 minutes (HHS 2.2(f)(12))**

9. If a technician suspects a specimen has been adulterated or diluted, the specimen is: (Select **one** response.)

   ☐ Discarded and a new specimen obtained
   ■ **Forwarded for testing and a new specimen obtained (HHS 2.2(f)(15)(16))**
   ☐ Discarded and treated as a positive test result
   ☐ Forwarded for testing and suspicions noted on chain of custody form

10. If the collected urine volume is less than required and the temperature is within acceptable range, the specimen is discarded and a second specimen is collected.

    ■ **True (HHS 2.2(f)(10)(ii))**
    ☐ False

11. When using a split specimen, what is the least amount of urine that can be collected? (Select **one** response.)

    ■ **45 ml (HHS 2.2(h)(1))**
    ☐ 15 ml
    ☐ 36 ml
    ☐ 30 ml

12. If necessary, bleach may be used as a substitute for bluing.

    ☐ True
    ■ **False (HHS 2.2(f)(1))**

13. The employee must initial the label on the specimen bottle certifying it was collected from him/her.

    ■ **True (HHS 2.2(f)(20))**
    ☐ False

14. What is the appropriate temperature range of the urine? (Select **one** response.)

    ☐ 86 to 98 degrees F
    ■ **90 to 100 degrees F (HHS 2.2(f)(13))**
    ☐ 90 to 96 degrees F

15. If the collected urine volume is less than required and the temperature is outside the acceptable range, the employee must be tested under direct observation.

    ■ **True (HHS 2.2(f)(13))**
    ☐ False

NOTE: If your Site uses a different procedure that is not listed or contradicts a statement, please use the back of this form to provide any additional information you feel necessary.

TABLE FOR GRADING RESULTS – VALUE IS ASSIGNED TO *CORRECT* ANSWERS.

+18 = 100%		+ 9 = 50%
+17 = 94%		+ 8 = 44%
+16 = 89%		+ 7 = 39%
+15 = 83%		+ 6 = 33%
+14 = 78%		+ 5 = 28%
+13 = 72%	**14 or fewer correct answers**	+ 4 = 22%
+12 = 67%	**(less than 80%) would be a fail.**	+ 3 = 17%
+11 = 61%		+ 3 = 11%
+10 = 56%		+ 1 = 6%
		0 = 0%

DRUG TEST OBSERVATION CHECKLIST

(In accordance with the Department of Health and Human Services Mandatory Guidelines, 4/13/04)

1. Is there a bluing agent in the toilet? (2.2(f)(1))

   Yes_____No_____

2. Is there any other source of water in urination area? (2.2(f)(1))

   Yes_____No_____

3. Was a photo ID presented? (2.2(f)(2))

   Yes_____No_____

4. Did the donor arrive within 2 hours? (712.15(b))

   Yes_____No_____

5. Was the donor asked to remove unnecessary outer garments? (2.2(f)(4))

   Yes_____No_____

6. Was the donor asked to empty pockets and/or contents checked? (same)

   Yes_____No_____

7. Did the donor's purse/briefcase remains with outer garments? (2.2(f)(4))

   Yes_____No_____

8. Was donor instructed to wash/dry hands prior to urination? (2.2(f)(5))

   Yes_____No_____

9. After washing hands, did the donor remain in the presence of the collection site person and away from access to any water fountain, faucet, soap dispenser, cleaning agent, or any other materials that might be used to adulterate the specimen? (2.2(f)(6))

   Yes_____No_____

10. Was the donor provided with a clean bottle/container? (2.2(f)(7))

    Yes_____No_____

11. Following urination and receipt of specimen, did the collection site person determine the volume of urine in the container? (2.2(f)(10))

    Yes_____No_____

12. If less than 30ml of urine collected and the temperature is in acceptable range, was the specimen is discarded and a second specimen collected?

    Yes_____No_____

    Give donor a reasonable amount of liquid (8 oz glass of water every 30 minutes - not to exceed 24 oz). If the donor fails for any reason to provide 30ml of urine for the second collection, the collection site personnel must contact the HRP Management Official for assistance.

    NOTE: Normally, a medical examination should be performed to determine if a medical condition exists. If none exists, record the situation as a lack of cooperation or a refusal to test under 10 CFR 707.12(b)(2).

    If the volume is less than 30ml and the temperature is outside the acceptable range specified, collect a second specimen under direct observation (acceptable range: 32 to 38 degrees C or 90 to 100 degrees F) under (2.2(f)(10)-(13)).

13. After a good specimen has been provided and submitted, was the donor instructed to wash hands? (2.2(f)(11))

    Yes_____No_____

14. Was the temperature of the specimen measured within 4 minutes. (2.2(f)(12))

    Yes_____No_____

15. Did the donor and the collection site person keep the specimen bottle in view at all times prior to it being sealed and labeled? (2.2(f)(17))

    Yes_____No_____

16. Did the collection site person securely place a dated, tamper-evident seal/label on the specimen bottle? (2.2(f)(19))

    Yes_____No_____

17. Did the donor initial the tamper-evident seal/label on specimen bottle for purpose of certifying that the specimen was collected from him/her? (2.2(f)(20))

    Yes_____No_____

18. Did the collection site person ensure that the required information was entered on the Federal chain-of-custody form? (2.2(f)(21))

    Yes_____No_____

19. Was the donor asked to read and sign the statement on the Federal chain-of-custody form, certifying that the specimen identified as having been collected from him/her is in fact that specimen he/she provided? (2.2(f)(22))

    Yes_____No_____

20. Did the collection site person complete the specimen chain-of-custody form? (2.2(f)(24))

    Yes_____No_____

BREATH ALCOHOL TECHNICIAN TEST

Name:_____ Date:_____

Position Title:_____ Number of years in position:_____

Are your training and certifications current? _____ Yes _____No _____ Not Certain

1. Which government regulation(s) contain specific rules or guidance to be followed when conducting a breath alcohol test? (Select **two** responses that you believe are correct.)

   ☐ DOE 10 CFR, Part 710 – "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material"
   ☐ DOE 10 CFR, Part 712 – "Human Reliability Program"
   ☐ DOT 49 CFR, Part 40 – "Procedures for Transportation Workplace Drug and Alcohol Testing Programs"
   ☐ DOE Order 3428.3b – "Drug and Alcohol Testing Procedures"

2. In addition to the breath alcohol technician, who is allowed to actually **witness** the testing process? (Select **one** response.)

   ☐ The employee
   ☐ DOE/DOT agency representative
   ☐ Union steward
   ☐ The employee and the DOE/DOT representative
   ☐ All of the above

3. What must you do if an individual refuses to sign the Alcohol Testing Form Step 2? (Select **one** response.)

   ☐ Document refusal on the alcohol testing form remarks line.
   ☐ Immediately notify designated employer representative.
   ☐ Immediately notify the SOMD.
   ☐ Document refusal on the alcohol testing form remarks line *and* immediately notify designated employer representative.
   ☐ Document refusal on the alcohol testing form remarks line *and* immediately notify the SOMD.

4. What are the privacy requirements pertinent to breath alcohol testing? (Select **one** response.)

   ☐ Visual
   ☐ Aural
   ☐ Written
   ☐ Visual *and* aural
   ☐ Visual *and* written

5. If an initial breath alcohol test result is equal to or greater than 0.02, which of the following steps

must a breath alcohol technician take? (Select **five** responses that you believe are correct.)

☐ Ensure that the waiting period for the confirmation test lasts at least 15 minutes.
☐ Instruct the employee to notify his/her supervisor of an initial positive test result.
☐ Instruct the employee not to put anything in mouth or belch during the waiting period.
☐ Observe employee during the waiting period.
☐ Note any noncompliance with the waiting period in alcohol testing form remarks line.
☐ Complete confirmation test using the same mouthpiece.
☐ Immediately notify the designated employer representative of confirmed results that exceed 0.02.

6. If a confirmation breath test is required, the breath alcohol technician must tell the tested employee that following instructions concerning the waiting period is to his/her benefit.

☐ True
☐ False

7. Which of the following is considered a "fatal flaw"? (Select **three** responses that you believe are correct.)

☐ Displayed alcohol concentration number and printed alcohol concentration number are exactly the same
☐ Confirmation test started before 15-minute wait
☐ No air blank used before confirmation test
☐ Air blank used before confirmation test was not 0.00
☐ Employee slept during waiting period.

8. Which of the following is considered a "correctable flaw"? (Select **two** responses that you believe are correct.)

☐ Breath alcohol technician did not sign the alcohol testing form.
☐ The displayed test number and the printed test number are not the same.
☐ Breath alcohol technician used a non-standard alcohol testing form for the test.

9. The employee may select his/her own wrapped evidential breath testing device mouthpiece.

☐ True
☐ False

10. The employee may unwrap his/her own evidential breath testing device mouthpiece.

☐ True
☐ False

11. The breath alcohol technician may allow the employee up to three chances to provide adequate breath for a test.

    ☐ True
    ☐ False

12. If it becomes necessary to conduct a repeat test, the breath alcohol technician is not limited in the number of attempts to complete the test.

    ☐ True
    ☐ False

13. It is considered a refusal to test if an employee will not sign and date the Alcohol Testing Form Step 4 after a confirmation test of greater than or equal to 0.02.

    ☐ True
    ☐ False

14. It is considered a refusal to test if an employee will not sign and date the Alcohol Testing Form Step 2 prior to a screening test.

    ☐ True
    ☐ False

15. What must happen if a breath alcohol technician begins a confirmation test 14 minutes after a positive screening test? (Select **one** response.)

    ☐ The breath alcohol technician may conduct a second confirmation test after an additional 15-minute wait.
    ☐ The breath alcohol technician must cancel the test.
    ☐ The breath alcohol technician must complete the test and explain in the alcohol testing form remarks line.

16. If the breath alcohol technician is informed an employee was mistakenly or improperly selected for testing, this is a basis for the breath alcohol technician to cancel the test.

    ☐ True
    ☐ False

17. A cancelled breath alcohol test is neither positive nor negative.

    ☐ True
    ☐ False

18. The evidential breath testing device must be able to perform an external calibration check.

    ☐ True
    ☐ False

19. A breath alcohol technician must instruct the employee to blow steadily and forcefully into the evidential breath testing device mouthpiece for at least 6 seconds.

    ☐ True
    ☐ False

20. If an employee fails to appear for a breath alcohol test, it is considered a/an: (Select **one** response.)

    ☐ Positive test result
    ☐ Refusal to test
    ☐ Invalid test result
    ☐ Canceled test.

NOTE: If your Site uses a different procedure that is not listed or contradicts a statement, please use the space below to provide any additional information that you feel is necessary.

BREATH ALCOHOL TECHNICIAN TEST
ANSWER SHEET

1. Which government regulation(s) contain specific rules or guidance to be followed when conducting a breath alcohol test? (Select **two** responses that you believe are correct.)

   ☐ DOE 10 CFR, Part 710 – "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material"
   ■ **DOE 10 CFR, Part 712 – "Human Reliability Program"**
   ■ **DOT 49 CFR, Part 40 – "Procedures for Transportation Workplace Drug and Alcohol Testing Programs"**
   ☐ DOE Order 3428.3b – "Drug and Alcohol Testing Procedures"

2. In addition to the breath alcohol technician, who is allowed to actually **witness** the testing process? (Select **one** response.)

   ☐ The employee
   ☐ DOE/DOT agency representative
   ☐ Union steward
   ☐ The employee and the DOE/DOT representative
   ■ All of the above

3. What must you do if an individual refuses to sign the Alcohol Testing Form Step 2? (Select **one** response.)

   ☐ Document refusal on the alcohol testing form remarks line.
   ☐ Immediately notify designated employer representative.
   ☐ Immediately notify the SOMD.
   ■ **Document refusal on the alcohol testing form remarks line *and* immediately notify designated employer representative.**
   ☐ Document refusal on the alcohol testing form remarks line *and* immediately notify the SOMD.

4. What are the privacy requirements pertinent to breath alcohol testing? (Select **one** response.)

   ☐ Visual
   ☐ Aural
   ☐ Written
   ■ **Visual *and* aural**
   ☐ Visual *and* written

5. If an initial breath alcohol test result is equal to or greater than 0.02, which of the following steps must a breath alcohol technician take? (Select **five** responses that you believe are correct.) **(DOT 40.251)**

   ■ **Ensure that the waiting period for the confirmation test lasts at least 15 minutes.**
   ☐ Instruct the employee to notify his/her supervisor of an initial positive test result.
   ■ **Instruct the employee not to put anything in mouth or belch during the waiting period.**

■ **Observe employee during the waiting period.**
■ **Note any noncompliance with the waiting period in alcohol testing form remarks line.**
☐ Complete confirmation test using the same mouthpiece.
■ **Immediately notify the designated employer representative of confirmed results that exceed 0.02.**

6. If a confirmation breath test is required, the breath alcohol technician must tell the tested employee that following instructions concerning the waiting period is to his/her benefit.

■ **True (DOT 40.251(a)(2)(iii))**
☐ False

7. Which of the following is considered a "fatal flaw"? (Select **three** responses that you believe are correct.) **(DOT 40.267(b))**

☐ Displayed alcohol concentration number and printed alcohol concentration number are exactly the same
■ **Confirmation test started before 15-minute wait**
■ **No air blank used before confirmation test**
■ **Air blank used before confirmation test was not 0.00**
☐ Employee slept during waiting period.

8. Which of the following is considered a "correctable flaw"? (Select **two** responses that you believe are correct.) **(DOT 40.269)**

■ **Breath alcohol technician does not sign the alcohol testing form.**
☐ The displayed test number and the printed test number are not the same. ***(fatal flaw)***
■ **Breath alcohol technician uses a non-standard alcohol testing form for the test.**

9. The employee may select his/her own wrapped evidential breath testing device mouthpiece.

■ **True (DOT 40.243)**
☐ False

10. The employee may unwrap his/her own evidential breath testing device mouthpiece.

☐ True
■ **False (DOT 40.243)**

11. The breath alcohol technician may allow the employee up to three chances to provide adequate breath for a test.

■ **True (DOT 40.265(b)(2))**
☐ False

12. If it becomes to necessary to conduct a repeat test, the breath alcohol technician is not limited in the number of attempts to complete the test.

■ **True (DOT 40.271(a)(3))**
☐ False

13. It is considered a refusal to test if an employee will not sign and date the Alcohol Testing Form Step 4 after a confirmation test of greater than or equal to 0.02.

☐ True
■ **False (DOT 40.255(a)(3))**

14. It is considered a refusal to test if an employee will not sign and date the Alcohol Testing Form Step 2 prior to a screening test.

■ **True (DOT 40.241(2)(g))**
☐ False

15. What must happen if a breath alcohol technician begins a confirmation test 14 minutes after a positive screening test? (Select **one** response.)

☐ The breath alcohol technician may conduct a second confirmation test after an additional 15-minute wait
■ **The breath alcohol technician must cancel the test (DOT 40.267(c)(1)) (*fatal flaw*)**
☐ The breath alcohol technician must complete the test and explain in the alcohol testing form remarks line

16. If an employee is improperly selected for testing, this is a basis for canceling a test.

☐ True
■ **False (DOT 40.275(b))**

17. A cancelled breath alcohol test is neither positive nor negative.

■ **True (DOT 40.273(a))**
☐ False

18. The evidential breath testing device must be able to perform an external calibration check.

■ **True (DOT 40.231(6) and DOT 40.233(c))**
☐ False

19. A breath alcohol technician must instruct the employee to blow steadily and forcefully into the evidential breath testing device mouthpiece for at least 6 seconds.

■ **True (DOT 40.243(c))**
☐ False

20. If an employee fails to appear for a breath alcohol test, it is considered a/an: (Select **one** response.)

- ☐ Positive test result
- ■ **Refusal to test (DOT 40.261(a)(1))**
- ☐ Invalid test result
- ☐ A canceled test.

NOTE: If your Site uses a different procedure that is not listed or contradicts a statement, please use the space below to provide any additional information that you feel is necessary.

TABLE FOR GRADING RESULTS – VALUE IS ASSIGNED TO *CORRECT* ANSWERS.

+28 = 100%		+13 = 46%
+27 = 96%		+12 = 43%
+26 = 93%		+11 = 39%
+25 = 89%		+10 = 36%
+24 = 86%		+ 9 = 32%
+23 = 82%		+ 8 = 29%
+22 = 79%		+ 7 = 25%
+21 = 75%		+ 6 = 21%
+20 = 71%	**22 or fewer correct answers**	+ 5 = 18%
+19 = 68%	**(less than 80%) would be a fail.**	+ 4 = 14%
+18 = 64%		+ 3 = 11%
+17 = 61%		+ 2 = 7%
+16 = 57%		+ 1 = 4%
+15 = 54%		+ 0 = 0%
+14 = 50%		

Although getting 22 or fewer answers correct is a failure, **not getting all of the correct answers for #5, #8, #9, or #11 would be a serious concern**, because they relate to fatal flaws and potential invalidation of test results.

BREATH ALCOHOL TEST OBSERVATION CHECKLIST
In accordance with U.S. Department of Transportation 49 CFR Part 40

1. Does the device used for testing meet the U.S. Department of Transportation requirements?

   Yes_____ No_____

   (How do you know?)

   Answer: Evidential grade breathalyzer must be listed without "*" on the conforming products list of evidential breath measurement devices.

2. Was the employee verified through positive identification? (40.241(c))

   Yes_____ No_____

3. Was the process explained to the employee along with completing the DOE/Bureau of Alcohol, Tobacco, and Firearms (ATF) Step 1? (40.241(e) & (f))

   Yes_____ No_____

4. Did the employee complete the ATF Step 2 and sign the certification statement? (40.241(g))

   Yes_____ No_____

5. Did the breath alcohol test/site test technician (BAT/STT) unwrap and install a fresh mouthpiece with each test? (yes) (40.243(b))

   Yes_____ No_____

6. Did the BAT/STT instruct the employee to continue blowing until device or operator signaled to stop? (6 sec) (40.243(c))

   Yes_____ No_____

7. Did the BAT/STT show the test result to the employee? (yes) (40.243(c))

   Yes_____ No_____

8. Did the BAT/STT verify that the test number and time did print correctly? (yes) (40.243(e)-(g))

   Yes_____ No_____

   Answer: Three options for the screen include: (either/or)
   - Must print directly on to the ATF
   - Must print to a separate report affixed to the ATF
   - Must be written into Step 3 of the ATF.

9. If the test result is less than 0.02 – were these steps taken?

    - BAT/STT circled "BAT" and "breath" at top of Step 3 on ATF

      Yes_____ No_____

    - BAT/STT signed and dated bottom of Step 3 on ATF

      Yes_____ No_____

    - BAT/STT transmitted ATF original; gave a copy to the employee; and retained a copy (40.247(a)(1)-(2))

      Yes_____ No_____

10. Were the requirements for privacy met?

    Yes_____ No_____

    Answer: Visual and aural (40-221(c))

11. Did the BAT/STT attach the screen test results and any confirmation test results to side or back of ATF with tamper-evident tape? (Unless printed directly on form.) (40.243(f))

    Yes_____ No_____

12. Was a list of fatal flaws readily available to the BAT?

    Yes_____ No_____

    (Not a DOT requirement – this is simply a good business practice.)

13. Were there two evidential breathing test devices (EBTs) available for use? (40.221(d) – not specific)

    Yes_____ No_____

If the breath alcohol test result is **equal to or greater than 0.02**:

Subpart M - Alcohol Confirmation Tests
§ 40.251 What are the first steps in an alcohol confirmation test?

As the BAT for an alcohol confirmation test, you must follow these steps to begin the confirmation test process:

a) You must carry out a requirement for a waiting period before the confirmation test, by taking the following steps:

1) You must ensure that the waiting period lasts at least 15 minutes, starting with the completion of the screening test. After the waiting period has elapsed, you should begin the confirmation test as soon as possible, but not more than 30 minutes after the completion of the screening test.
   i) If the confirmation test is taking place at a different location from the screening test (see §40.247(b)(3)) the time of transit between sites counts toward the waiting period if the STT or BAT who conducted the screening test provided the waiting period instructions.
   ii) If you cannot verify, through review of the ATF, that waiting period instructions were provided, then you must carry out the waiting period requirement.
   iii) You or another BAT or STT, or an employer representative, must observe the employee during the waiting period.

2) Concerning the waiting period, you must tell the employee:
   i) Not to eat, drink, put anything (e.g., cigarette, chewing gum) into his or her mouth, or belch
   ii) The reason for the waiting period (i.e., to prevent an accumulation of mouth alcohol from leading to an artificially high reading)
   iii) That following your instructions concerning the waiting period is to the employee's benefit
   iv) That the confirmation test will be conducted at the end of the waiting period, even if the instructions have not been followed.

3) If you become aware that the employee has not followed the instructions, you must note this on the "Remarks" line of the ATF.

b) If you did not conduct the screening test for the employee, you must require positive identification of the employee, explain the confirmation procedures, and use a new ATF. You must note on the "Remarks" line of the ATF that a different BAT or STT conducted the screening test.

c) Complete Step 1 of the ATF.

d) Direct the employee to complete Step 2 on the ATF and sign the certification. If the employee refuses to sign this certification, you must document this refusal on the "Remarks" line of the ATF and immediately notify the DER. This is a refusal to test.

e) Even if more than 30 minutes have passed since the screening test result was obtained, you must begin the confirmation test procedures in §40.253, not another screening test.

f) You must note on the "Remarks" line of the ATF the time that elapsed between the two events, and if the confirmation test could not begin within 30 minutes of the screening test, the reason why.

g) Beginning the confirmation test procedures after the 30 minutes have elapsed does not invalidate the screening or confirmation tests, but it may constitute a regulatory violation subject to DOT agency sanction.

§ 40.253 What are the procedures for conducting an alcohol confirmation test?

As the BAT conducting an alcohol confirmation test, you must follow these steps in order to complete the confirmation test process:

a) In the presence of the employee, you must conduct an air blank on the EBT you are using before beginning the confirmation test and show the reading to the employee.

   1) If the reading is 0.00, the test may proceed. If the reading is greater than 0.00, you must conduct another air blank.
   2) If the reading on the second air blank is 0.00, the test may proceed. If the reading is greater than 0.00, you must take the EBT out of service.
   3) If you take an EBT out of service for this reason, no one may use it for testing until the EBT is found to be within tolerance limits on an external check of calibration.
   4) You must proceed with the test of the employee using another EBT, if one is available.

b) You must open a new individually wrapped or sealed mouthpiece in view of the employee and insert it into the device in accordance with the manufacturer's instructions.

c) You must ensure that you and the employee read the unique test number displayed on the EBT.

d) You must instruct the employee to blow steadily and forcefully into the mouthpiece for at least six seconds or until the device indicates that an adequate amount of breath has been obtained.

e) You must show the employee the result displayed on the EBT.

f) You must show the employee the result and unique test number that the EBT prints out either directly onto the ATF or onto a separate printout.

g) If the EBT provides a separate printout of the result, you must attach the printout to the designated space on the ATF with tamper-evident tape, or use a self-adhesive label that is tamper-evident. (65 FR 79526, Dec. 19, 2000, as amended at 66 FR 41954, Aug. 9, 2001)

§ 40.255 What happens next after the alcohol confirmation test result?

a) After the EBT has printed the result of an alcohol confirmation test, you must, as the BAT, take the following additional steps:

   1) Sign and date Step 3 of the ATF.
   2) If the alcohol confirmation test result is lower than 0.02, nothing further is required of the employee. As the BAT, you must sign and date Step 3 of the ATF.
   3) If the alcohol confirmation test result is 0.02 or higher, direct the employee to sign and date Step 4 of the ATF. If the employee does not do so, you must note this on the “Remarks” line of the ATF. However, this is not considered a refusal to test.
   4) If the test is invalid, tell the employee the test is cancelled and note the problem on the “Remarks” line of the ATF. If practicable, conduct a re-test. (See §40.271.)
   5) Immediately transmit the result directly to the DER in a confidential manner.

      i) You may transmit the results using Copy 1 of the ATF, in person, by telephone, or by electronic means. In any case, you must immediately notify the DER of any result of 0.02 or greater by any means (e.g., telephone or secure fax machine) that ensures the result is immediately received by the DER. You must not transmit these results through C/TPAs or other service agents.

ii) If you do not make the initial transmission in writing, you must follow up the initial transmission with Copy 1 of the ATF.

b) As an employer, you must take the following steps with respect to the receipt and storage of alcohol test result information:

1) If you receive any test results that are not in writing (e.g., by telephone or electronic means), you must establish a mechanism to establish the identity of the BAT sending you the results.
2) You must store all test result information in a way that protects confidentiality.

HRP FILE REVIEW DATA COLLECTION FORM

Name: **File ID:** **Temporary Removal/Reinstate Dates from Data Call:**
Hallucinogenic Review Date: (ususlly found in either the medical or psychological files)

PSYCH	MEDICAL	HRP
Date of the last Assessment: Evidence of access to JTA? Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals? (dates/info) Security Concerns? Reported?	Date of the last Assessment: Evidence of access to JTA? Evidence of Psych Assessment Integration? Current Prescription Medications: Reported Restrictions/Removals? (dates/info) Notifications made: Unreported Restrictions/Removals? (dates/info) Security Concerns? Reported?	Data from DOE Form 470.3: Last Certification Date: (should be within 12 months of each other) Current Certification Date: Last Drug/Alcohol Test: (should be within 12 months of each other) Current Drug/Alcohol Test: Last Training Date: (should be within 12 months of each other) Current Training Date: Is Section B always signed after the medical and psychological evaluations? ☐ Yes ☐ No Is Section C always signed after drug and alcohol testing? ☐ Yes ☐ No Reported Restrictions/Removals? (dates/info) Notifications made: (<u>who</u>/what/**<u>when</u>**) Unreported Restrictions/Removals? (dates/info)

(OFFICIAL USE ONLY WHEN FILLED IN)

DATA COLLECTION FORM

Though preparation of a data collection form (DCF) may/will begin while various subtopic data collection activities are ongoing, a DCF will not be turned in to the writer **until** all elements of a DCF (as described below) are **FINAL**. An **INTERIM** DCF may be turned into to the administrator with one or more elements of the DCF incomplete with appropriate statements about follow-up activities or additional data collection activities. See example of a DCF on following two pages.

(INTERIM/FINAL)

(U) Date: _____ **(U) Team Member(s):**_____

(U) Site-Year-Topic-Sequence Number:_____
(U) (example: SRS-01-PS-001)

(U) Data Point: Identify the subtopic (Personnel Security Clearance {PSC], SSAP, HRP, or FV&A) or element of the subtopic (i.e., PSC pre-employment checks, HRP supervisor and incumbent questionnaire,), and provide a one-phrase or one-sentence conclusion.

(U) Results: (Bullet statements of strengths and weaknesses.)

Strengths: (U)

Weaknesses: (U)

Narrative: (U) (Briefly summarize **all** of the data collected on a subtopic or on an aspect of a subtopic. This is **not** a verbatim account of data collection results. Identify findings using the standard format and include the appropriate reference(s).

System Description: (U) (Describe the organization [identification of organization(s), number of staff, and training] that has the responsibility to implement this subtopic or subtopical element, and all supporting procedures, including whether the procedures are up-to-date and comprehensive.)

Implementation: (U) (Assessment of effectiveness of **each** major subtopic process/element's effectiveness.)

-(first major sub-topic processes, for example, FV&A request process, or HRP certification process)

-(next major sub-topic process, usually in the sequence in which they are completed during implementation)

(U) Impact: Briefly discuss the impact of any identified weaknesses on implementation of this subtopic and any impact on the overall personnel security program topic.

(U) Need for Additional Information: Briefly state the need to collect additional information and what data collection activity will be conducted to meet this need. If none, then so state. Always state NONE when DCF is **FINAL**.

INSTRUCTIONS FOR COMPLETING AN ISSUE FORM (U)

(U) The purpose of this form is to convey the inspection team's understanding of a concern that could impact the rating, to solicit site management's position on this concern, and to describe actual/proposed mitigating actions. The form may also be used to assist in resolving other communications problems. Issue Forms can be of any length. Portion markings are required when the form contains classified information. Portion markings have been provided but may need to be modified depending on the classification of the text. Topic Team Leaders and applicable site personnel are responsible for ensuring the completion of a classification review by an authorized derivative classifier. The pre-existing portion markings may be lined through when the form contains no classified information.

(U) Date:_____ **(U) Site-Year-Topic-Sequence Number** _____ **(U)**
(example: RL-03-PS-001)

PART A (U)
1. (U) Issue: State in sufficient detail to convey to the site how and why we believe an observed condition is an issue, and state the applicable reference supporting the issue.
2. (U) Impact: Clearly state the immediate or potential impact that exists because of the issue.
(U) Approval: Topic Team Leader_____Date_____ (U) Inspection Chief_____Date_____
PART B (U)
1. (U) Site Response: The response should include the site's position on the issue and its immediate or potential impact. Supporting or additional information should be provided to substantiate this position.
(U) Action Taken, if appropriate: Describe any actions taken to mitigate immediate impacts or actions under consideration for future implementation. Include the rationale for these actions.
(U) Approval: Site Representative_____Date_____
(U) Receipt Acknowledged: (U) HS-61 Representative_____Date_____

REPORT PREPARATION

The following steps will be used in the preparation of the personnel security program topic appendix.

1. Throughout the draft report preparation phase, these objectives will be kept in mind.

   - Make sure the report supports the conclusion, not just a catalog of the results (system description).

   - Issues (positive or negative) that do not support the overall conclusion should be minimized or omitted.

   - Use results-oriented sub-headers to assist the reader.

   - List strengths first and then weaknesses throughout the report.

2. Only the assigned "principal writer" will prepare the appendix.

3. Team members will provide input to the principal writer verbally or in writing, primarily in the form of a data collection sheet(s). In rare occasions, team members may be asked to prepare portions of the appendix.

4. The flow of data collection will dictate the order in which sections of the draft report are prepared. Data for the personnel security clearance program will normally be collected during the planning phase. Data on the human reliability program, SSAP, and FV&A will be collected the first week of the data collection phase. The principal writer will complete data collection for the sup-topic that has been assigned by Wednesday. The other topic team members have until Thursday to complete data collection.

5. Preparation of the draft report will be accomplished in the following manner.

<u>On-Site Planning Phase</u>

- Daily: team meets to identify human reliability, FV&A, and safeguards and security awareness program strengths and weaknesses, and conclusions on overall effectiveness of the personnel security clearance program; this in turn serves as data for the principal writer to use in developing the initial draft

<u>On-Site Data Collection Phase</u>

- Daily: team meets to identify clearance program strengths and weaknesses, and conclusions on overall effectiveness of these programs

- Thursday: using the results of these daily meetings and data collection sheets, the principal writer begins developing introduction section and any sections that have completed data collection activities

Final Data Collection and Report Preparation

- Daily: team meets to identify HRP file, and drug and alcohol testing program strengths and weaknesses, and conclusions on overall effectiveness of these programs
- Friday: the results of the SSAP questionnaire are obtained and analyzed
- Friday: all other subtopical inputs are due to the principal writer by close of business
- Saturday: finalized the draft report, team members review for content and one team member proofreads the report
- Monday: final proofreading and correction prior to submission to the management review board