

INSPECTORS GUIDE

Personnel Security



Office of Security Evaluations
Office of Independent Oversight
Office of Health, Safety and Security

October 2009

PERSONNEL SECURITY
INSPECTORS GUIDE



October 2009

**U.S. Department of Energy
Office of Security Evaluations
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
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 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

Acronyms	v
Section 1: Introduction	
Purpose	1-1
General Considerations	1-1
Characterization of the Personnel Security Topic	1-1
Organization	1-2
Using the Topic-Specific Tools	1-3
Validation	1-5
Using the Tools in Each Inspection Phase	1-6
Integrated Safeguards and Security Management	1-7
Section 2: Management	
References	2-1
General Information	2-1
Common Deficiencies/Potential Concerns	2-2
Planning Activities	2-4
Data Collection Activities	2-5
Section 3: Personnel Security Clearance Program	
3.1 Types of Clearances	3-3
3.2 Pre-Employment Checks	3-4
3.3 Processing Clearance Requests	3-6
3.4 Screening and Analysis	3-8
3.5 Adjudicating Derogatory Information	3-10
3.6 Reinvestigations	3-12
Section 4: Safeguards and Security Awareness Program	
4.1 Administration and Management	4-1
4.2 Safeguards and Security Awareness Briefings	4-3
4.3 Supplemental Awareness Materials	4-7
Section 5: Human Reliability Program	
References	5-1
General Information	5-1
Common Deficiencies/Potential Concerns	5-2
Planning Activities	5-5
Data Collection Activities	5-6
Section 6: Unclassified Visits and Assignments by Foreign Nationals	
References	6-1
General Information	6-1
Common Deficiencies/Potential Concerns	6-1
Planning Activities	6-3
Data Collection Activities	6-4

Section 7: Interfaces

Integration 7-1
Integration by the Personnel Security Topic Team 7-1

Section 8. Analyzing Data and Interpreting Results

Introduction 8-1
Analysis of Results 8-1
Consideration of Integrated Safeguards and Security Management Concepts 8-4

Appendix A. Data Collection and Analysis Tools A-1

Acronyms

BI	Background Investigation
CAP	Corrective Action Plan
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
D&A	Drug and Alcohol
DEAR	Department of Energy Acquisition Regulation
DHHS	Department of Health and Human Services
DOE	U.S. Department of Energy
DOT	Department of Transportation
EBT	Evidential Breath Test Device
eQIP	Electronic Questionnaire for Investigation Processing
FACTS	Foreign Activities Central Tracking System
FBI	Federal Bureau of Investigation
FV&A	Foreign Visits and Assignments
HRP	Human Reliability Program
HS-61	Office of Security Evaluations
HSS	Office of Health, Safety and Security
IG	DOE Office of the Inspector General
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISSM	Integrated Safeguards and Security Management
IT	Information Technology
JTA	Job Task Analysis
LOI	Letter of Interrogatory
LSPT	Limited-Scope Performance Test
MAA	Material Access Area
NNSA	National Nuclear Security Administration
NSI	National Security Information
ODC	Oversight Document Center
OIO	Office of Independent Oversight
OJT	On-the-Job Training
OPM	Office of Personnel Management
OPSEC	Operations Security
ORPS	Occurrence Reporting and Processing System
PPM	Protection Program Management
PSC	Personnel Security Clearance
PSF	Personnel Security File
PSI	Personnel Security Interview

Acronyms (continued)

PSO	Program Secretarial Officer
QAP	Quality Assurance Plan
QNSP	Questionnaire for National Security Positions
QRB	Quality Review Board
SAP	Special Access Program
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SF	Standard Form
SNM	Special Nuclear Material
SO	Office of Security
SOMD	Site Occupational Medical Director
SSAP	Safeguards and Security Awareness Program
SSD	Safeguards & Security Director
SSSP	Site Safeguards and Security Plan
STS	Security Termination Statement

Section 1: Introduction

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 (OIO) 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 that are not specifically covered in this guide.

The information contained within this guide does not repeat all of the detailed information presented in DOE directives (including policies, orders, and manuals); rather, it is intended to provide practical guidance for planning independent oversight activities and for collecting and analyzing inspection data.

One significant consideration in developing the inspectors guides is to provide a repository for the collective knowledge of OIO's inspectors that can be enhanced and updated as inspection methods improve and OIO inspector experience accumulates. Every attempt has been made to develop specific guidelines that 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, OIO has included the personnel security clearance 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) is granted only after it has been determined that such access will not endanger security and that the approved access 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 inspection planning, data collection, analysis of results, and report preparation.

The personnel security program's functions include the appropriate justification and grant of security clearances, assuring that program officials and employees are aware of their security responsibilities, and the control of foreign national visitors within the DOE complex. Additionally, the personnel security program 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 management and protection of the nation's nuclear weapons complex, and individuals with a clearance (and a commensurate 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 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 that are designed 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 (PPM), and protective force programs. The section emphasizes techniques that can be used by inspectors to improve data collection by coordinating with other teams and identifies data that inspectors on other teams can collect that may be relevant 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. These guidelines also incorporate statements on the relative significance of potential deficiencies, as well as suggestions for conducting additional activities 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 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:** By determining the eligibility of individuals for access to classified matter and SNM, the program addresses appropriate types of clearances, pre-employment checks, adjudication of cases, and reinvestigations.
- **Safeguards and security awareness program:** This program is maintained through the presentation of initial, comprehensive, annual security refresher, and termination security briefings that are supplemented by additional materials (e.g., posters, e-mail messages, newsletter articles, etc.).
- **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 and maintain the highest standards of personal 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 foreign visits and assignments by foreign nationals program:** This program is concerned with the proper approval and control of foreign visitors 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, 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 and includes a short discussion detailing each potential deficiency. However, the identified deficiencies are not necessarily evident at every facility, but have been noted often enough to warrant special attention during inspections. 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 efforts. By reviewing the section before collecting data, inspectors can be alerted to commonly identified deficiencies and potential concerns that may exist at the inspected facility.

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.

Although 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 defining 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. The Data Collection Activities section includes activities that are most often conducted and that reflect as much OIO 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 OIO inspectors use to verify the accuracy of the information obtained during data collection activities. The process for performing validations of inspection results with site representatives is discussed in detail in the HS-61 Safeguards and Security Appraisal Process Guide and includes a discussion of on-the-spot validations, daily validations, and summary validations.

Inspectors should ensure that they are validating facts, conclusions, and impact, not their own conjecture. Facts (data points) noted during the inspection of the personnel security program should be validated with facility representatives as they become apparent (on-the-spot), if representatives accompany the inspection team. If facility representatives do not accompany the inspection team, the data points should be validated during 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 and affects a number of protection activities, it is particularly important that team members keep track of significant information to ensure that the information is recapped and that the facts are reconfirmed during the daily and summary validations.

Using the Tools in Each Inspection Phase

The inspection tools are intended to be used throughout all inspection phases. 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 their currency.

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 additional activities should be conducted to further distinguish the deficiency or aid in identifying potential root causes.
- 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 analyze the collected data and to discuss the potential impacts of identified deficiencies.

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

- Review comments received on the final draft report.
- Review and comment on the 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, OIO 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.

Section 2: Management

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 broad scope of the personnel security program not only provides for the justification and the determination of an individual's 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 clearance. The personnel security program is the only program that focuses on individual eligibility for access throughout the life of the clearance—from grant to termination. In addition, in today's environment of increased information exchange, added emphasis is now being placed on foreign 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 can be effectively exploited to bypass some elements of protection systems. Further, insiders may have extensive knowledge of an inspected facility. Therefore, individuals should only be granted a security clearance when their work requires access to classified information or SNM. Since the human element is 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 phases of 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.

An effective management provides adequate resources 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 re-certification of individuals enrolled in HRP, conduct and documentation of awareness briefings, and analysis and mitigation of the threat represented by foreign national visitors. Adequate staffing levels should be maintained, and individuals who perform critical personnel security tasks should be properly trained. This is especially important because personnel security organizations are frequently tasked with the performance of additional responsibilities (e.g., activities associated with the implementation of Homeland Security Presidential Directive-12).

Finally, line management support is essential to ensure the success of all elements 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 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. Although site awareness coordinators and supervisors have employed a variety of techniques to remind employees of the need to complete these briefings, responsibility ultimately falls on the individual to ensure that they are aware of all security requirements.

Incidents of Security Concern. Similarly, DOE/NNSA organizations that are experiencing recurring incidents of security concern probably have deficient SSAPs. Although not the only measure of program effectiveness, casual analysis of these incidents often indicates that individuals either do not understand their safeguards and security responsibilities or awareness briefings are not effectively communicating employee responsibilities. 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 online FV&A request and approval systems now support a number of DOE/NNSA programs. Even though these programs offer the potential to better control approved foreign visitors and assignees, when employees fail to utilize these programs and host a foreign visitor prior to or without formal approval, the unanalyzed and unmitigated risks are being accepted by facility managers. It is essential that employees realize that they are the most important link in the protection program involving the mitigation of 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 overall program or elements of the program are deficient.

Inadequate Resources. The 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 personnel security case management systems are available to effectively implement the personnel security program and efficiently handle all critical personnel security functions. Without adequate resources, clearances cannot be processed efficiently and within prescribed timeframes, 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 the effective control of foreign visitors cannot be assured.

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 inadequately justified and/or unnecessary security clearance requests, minimal participation in the security awareness briefings, improper badging of approved foreign visitors, and foreign visits that take place without formal approval). When an accumulation of deficiencies exist, 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 additional management commitment and support are needed. Also, many personnel security specialists are assigned secondary duties and thus have insufficient time to dedicate to the performance of 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, especially with regard to 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 containing derogatory information and, when necessary, the preparation of cases for administrative review. Another example is the need for training of all hosts and escorts of foreign visitors and assignees. The lack of proper host and escort 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/or 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 accrual of additional expenses associated with requesting and granting security clearances for employees for the sole

purpose of accessing the facility to reach their place of work, the failure to enroll individuals in HRP prior to the conduct of work, or major problems in processing and escorting uncleared foreign visitors.

Feedback and Continuous Improvement

Inadequate Self-Assessment Process. Not all facilities have implemented a comprehensive self-assessment program. Consequently, 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 may not be identified.

Inadequate Surveys. Organizations charged with the responsibility to conduct surveys rarely have the appropriate staff to perform comprehensive evaluations of the personnel security program, which often results in surveys that lack the necessary scope and 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 adequate numbers of competent personnel are assigned to effectively evaluate the personnel security program. In some cases, the appropriate resolution of the staffing shortfalls requires obtaining assistance from other organizations or from support contractors to ensure that proper surveys are conducted.

Inadequate Corrective Action Plans. The creation of inadequate corrective action plans 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 that resources can be used to correct the most serious issues first; 2) establish a corrective action schedule with milestones so that 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 correct 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 focusing on 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 causes of deficiencies, which usually results in the recurrence of the same deficiencies. Often, 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 performs a root cause analysis of identified deficiencies, it is likely that similar deficiencies will reoccur.

Planning Activities

- 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 overall performance.
- Determine if the site contractor or DOE/NNSA field organization has established a program of reviews that is designed to periodically validate the need for security clearances held by contractor and Federal employees.
- Review the results of recent surveys and self-assessments to determine if feedback programs are producing comprehensive evaluations of the personnel security program, and review applicable corrective action plans to determine if program deficiencies are being appropriately addressed.

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, workflow bottlenecks, 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 overall site protection system.

B. Although DOE orders do not define the number of positions required to efficiently 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 clearances, screening investigation reports, additional adjudicative actions, and HRP enrollment and re-certifications
- Determining the extent of any temporary or short-term use of overtime or other resources to assist in the reduction of backlogs
- Determining the personnel security clearance organization’s ability to effectively respond to “surge” situations.

Competence Commensurate With Responsibilities

C. It is important that inspectors determine how well the personnel security program staff are 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, as well as lesson plans, should be reviewed. If these tools have not been developed, the effectiveness of the training program will be called into question. Time permitting, inspectors may also elect to attend a training session to determine whether or not the training covers all relevant information and is appropriately tailored to the needs of the audience.

Identification of Safeguards and Security Requirements

E. 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, training deficiencies, and failures to meet DOE requirements.

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

G. Inspectors should determine whether the persons responsible for the personnel security program are in the positions to ensure compliance and whether or not they are receiving adequate management support. This is especially important for the 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. Reviews of self-assessments and survey findings and corrective action plans may also be necessary 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 appropriate action.

Feedback and Continuous Improvement

H. Inspectors should coordinate with the PPM team concerning the reviews of the self-assessment and survey programs. Additionally, inspectors should determine whether surveys and self-assessments are performed regularly and whether all aspects of the personnel security program are reviewed. It is helpful to compare the results of the facility surveys and self-assessments to inspection findings or other audit results to learn whether performed self-assessments are equally effective.

I. 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 the implementation of corrective actions.

J. Inspectors should review the role of DOE/NNSA oversight by reviewing recent survey reports to determine if they are comprehensive, 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 during 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 review all deficiencies indicated as closed and collect data, as necessary, to verify that the prior deficiency has in fact been adequately corrected.

This page intentionally left blank.

Section 3: Personnel Security Clearance Program

References

- Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (50 U.S.C. 435b)
Public Law 110-181, *National Defense Authorization Act for Fiscal Year 2008*, January 28, 2008, Section 1072, *Security Clearances; Limitations*, (amends the Intelligence Reform and Terrorism Prevention Act of 2004, and is referred to as the Bond Amendment)
DOE Manual 470.4-5, *Personnel Security*
Department of Energy Acquisition Regulation 48 CFR 970.2201-1-2(a)(1)(ii), *Labor Relations*
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)
Secretary of Energy Memorandum, *Decisions Regarding Drug Testing for Department of Energy Positions That Require Access Authorizations (Security Clearances)*, September 14, 2007
Chief Health, Safety and Security Officer Memorandum, *Drug Testing*, December 3, 2007

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. DOE/NNSA personnel security organizations and contractor personnel security organizations are responsible for the 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 and drug tests are required of contractor and Federal employees being hired for positions requiring such access.

The Federal Bureau of Investigation and the Office of Personnel Management (OPM) are the primary providers of security background investigations (BIs) for 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 “Q” clearance must be reinvestigated every five years, and every ten years for individuals possessing an “L” clearance (see Figure 1).

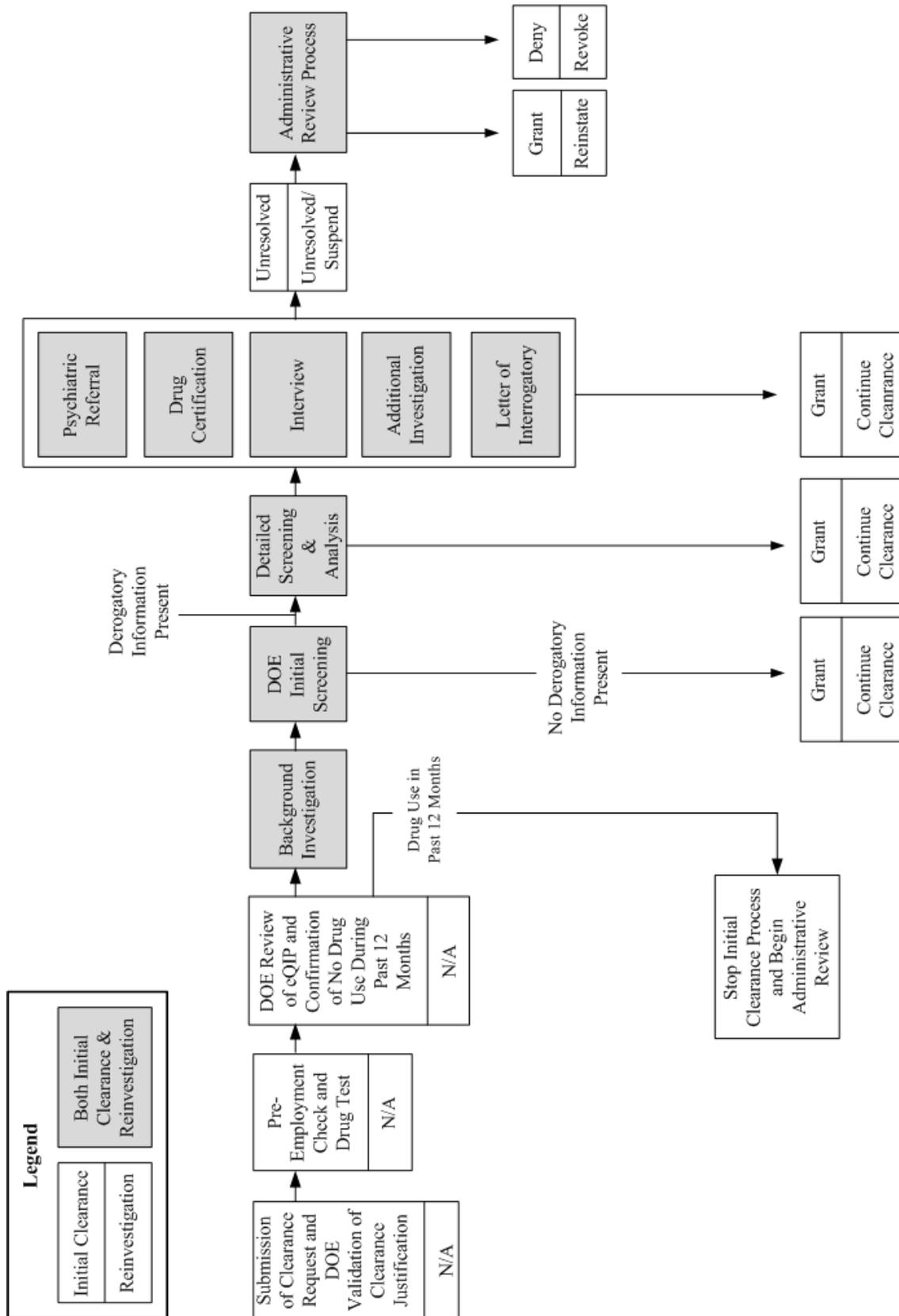


Figure 1. DOE Clearance Process

3.1 Types of Clearances

General Information

Requests for clearances are certified by appropriate personnel at the DOE/NNSA personnel security organization office. The key elements of the process include verifying that clearance requests are justified and that pre-employment checks are completed prior to requesting a clearance (see Section 3.2); ensuring that the type of clearance 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.

IRTPA prescribes timeliness standards for the processing of clearance requests. These standards were developed to reduce clearance processing backlogs and to foster the identification and implementation of government-wide clearance program enhancements.

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

Questionable Clearance Requests

Clearances 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 that do not meet these criteria should not be processed. Further, DOE/NNSA must establish processes that periodically validate that clearance holders actually perform work that requires access to classified information or SNM.

Inappropriate Type of Clearance

In some cases, the requested type of clearance is higher than the position requires. For example, a facility may request a “Q” clearance 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. 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, human resources, labor relations, contracts, medical staff, janitors, and cafeteria workers) for the appropriateness of their clearance types.

Changes in Status

Changes in the status of 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.

Planning Activities

- Review procedures used to determine types of clearances for contractor and subcontractor personnel.
- Obtain a list of personnel with clearances, and for contractors, the associated contract. This list will be used to select files for review to determine if clearance levels meet or exceed work requirements.
- Obtain a list of all inactive classified contracts in order to determine if any current clearance holders are no longer performing work under a classified contract.

Data Collection Activities

Request Procedures

A. Inspectors should interview individuals responsible for handling requests for clearances to determine how the process is conducted and how the need for access is certified. It is important that the justification for the access is based on the duties of the position, that the duties require access to classified matter or SNM, and that the type of clearance is appropriate. Interviews with the responsible individuals provide helpful information including overall explanations, step-by-step procedures, and how the need for access and the type of clearance are determined.

Performance Tests

B. Inspectors should review PSFs to determine whether their duties justify the clearance. Alternatively, inspectors should interview selected cleared personnel (especially human resources, contracts, finance, medical, maintenance professionals) to determine their access requirements.

C. 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.

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

3.2 Pre-employment Checks

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 a clearance, the contractor provides documentation certifying that a pre-employment check has been conducted and supplies the results. Proof of a negative drug test was ostensibly added to the pre-employment process by Secretarial direction promulgated in 2007. 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 all derogatory information revealed during pre-employment checks. In other cases, contractors may not provide sufficient detail regarding derogatory information to ensure that unnecessary requests for clearances are not processed or processing is stopped (denied), current clearances are not continued (suspended), or adjudicative actions can begin as soon as possible. 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.

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 electronic questionnaire for investigation processing (eQIP), and failure to provide proof of drug test completion along with the request for clearance can delay processing of the clearance request.

Planning Activities

- Obtain the names of new hires and hire dates for cleared employees to determine whether or not the pre-employment check and drug test were completed prior to submission of a request for a clearance.
- Review the methods used to determine the accuracy and completeness of pre-employment checks.
- Review local site procedures to determine the requirements levied on contractors regarding their submittal of the results of pre-employment checks, including all derogatory information.
- Determine if DOE/NNSA personnel security organizations have a process to ensure that the results of pre-employment checks and proof of drug testing are provided prior to submission to the investigative agency.

Data Collection Activities

A. Inspectors should review DOE/NNSA survey and site contractor self-assessment reports to determine if they adequately address performance of pre-employment checks and drug testing.

B. Inspectors should interview personnel security managers and review files to determine if DOE/NNSA personnel security organizations have processed clearance requests that did not include pre-employment checks and drug testing results.

Performance Tests

C. 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.

D. Inspectors should obtain a list of contractor new hires and verify that pre-employment checks, drug testing, and proof of citizenship were completed prior to requesting a security clearance.

3.3 Processing Clearance Requests

General Information

In order to effectively process clearance requests, paperwork flows from the initiation of the clearance request, through certification of need, to verification of completeness, and to forwarding of the request to the appropriate investigative agency by the DOE/NNSA personnel security organization. The process 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. IRTPA-related initiatives (electronic fingerprinting and eQIP replacement of Standard Form (SF) 86) have been implemented throughout the Department and have resulted in more timely and accurate submissions of requests for investigation.

Common Deficiencies/Potential Concerns

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 late, incomplete, or inaccurate data entries in the CPCI 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 security clearance or when an individual has terminated employment, the DOE must be notified immediately, and the request for clearance must be canceled/terminated.

Planning Activities

- Review a description of the facility’s personnel security clearance processing system, tracking system, and procedures.
- Determine whether any problems have been encountered by the DOE/NNSA personnel security organization in reviewing eQIP 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 or not 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 clearance process, these quotas can be examined to determine whether or not 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 the eQIP submission.

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 or not 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 or not data is arranged in the files in accordance with DOE requirements or in a similarly uniform manner to facilitate data handling and retrieval.

3.4 Screening and Analysis

General Information

Screening and analysis of the BI reports or other reported information (self-reporting, security infractions, employee concerns programs, Inspector General investigations, pre-employment check results, and other sources) are among 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 eQIP 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. The adoption of IRTPA has facilitated the DOE-wide implementation of electronic receipt of investigation reports and computer hardware upgrades (dual screens) at many personnel security organizations. These enhancements assist the Department in reducing the time to screen investigation reports and in meeting IRTPA standards.

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 clearance 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.

Reporting Information of Personnel Security Interest

To ensure an individual's continued eligibility to hold a DOE clearance, information of security interest (e.g., incidents of security concern/infractions, disciplinary action, and 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 applicable organizations will encourage proper reporting of items of personnel security interest. Even at sites that have established processes designed to provide information of personnel security interest to their servicing DOE/NNSA personnel security organization, problems are sometimes identified regarding inconsistent implementation or administration of these processes.

Planning Activities

- Determine whether sites have developed a formal procedure that requires the reporting of information of personnel security interest to the DOE/NNSA personnel security office.
- Review CPCI or local DOE/NNSA personnel security organization database reports to determine timeframes required to process cases, compared to IRTPA (applicants) and DOE requirements (incumbents).

Data Collection Activities

A. Inspectors should review the workload, overtime, and turnover rate of personnel security specialists to determine whether or not sufficient resources are allocated to perform effective screening and analysis. Individuals should be interviewed when there are indications that these factors are impacting performance.

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.

Performance Test

- C.** Inspectors should review site records to determine if reports of security interests (e.g., security incidents and infractions, written disciplinary actions, terminations for cause) are being forwarded in a timely manner to the cognizant DOE/NNSA personnel security organization.
- D.** Inspectors should review randomly selected PSFs to determine whether screening personnel are consistently and accurately identifying the absence or presence of derogatory information.
- E.** Inspectors should review randomly selected PSFs to determine whether initial screening and notification of continuations of incumbent clearances are completed within seven days of the receipt of completed investigations in clear cases. Inspectors should also determine whether adjudicative actions are initiated within 30 days of receipt of the completed investigations when derogatory information is identified.

3.5 Adjudicating Derogatory Information

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 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 adjudicative guidelines, and to determine whether they contain derogatory information sufficient to raise substantial doubt about clearance eligibility. If substantial doubt is noted, 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 clearance is suspended and the case is referred to the Office of Departmental Personnel Security with a request to proceed with an administrative review. If derogatory information cannot be resolved in an applicant case, the case is referred to the Office of Departmental Personnel Security with a request to proceed with an administrative review.

The implementation of IRTPA standards for applicant cases (DOE/NNSA must currently make an initial clearance determination for 90 percent of the applicant cases within 25 days after the receipt of a completed investigation, and as of December 2009, only 20 days will be allowed for making these determinations) has reduced the time previously allowed for making initial clearance determinations.

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. The failure to properly document 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.

Untimely Clearance Determinations

Although efforts to meet IRTPA standards have improved overall DOE performance, some DOE/NNSA personnel security organizations are still experiencing difficulties in completing initial security determinations in a timely manner. Shortfalls in resources and process inefficiencies are the primary reasons that personnel security organizations exceed the required timeframes.

Planning Activities

- Review procedures for preparing letters of interrogatory, interviews, forwarding cases for psychiatric evaluation, and for denying/suspending clearances.
- Determine whether or not organizational procedures provide sufficient guidance to properly document 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 IRTPA statistics available for the Office of Departmental Personnel Security to determine if DOE/NNSA is meeting processing standards for applicant cases.
- Review OPM Closed Case Reports without 79A to identify reports for possible review.
- 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 inspected site. The listings should identify cases processed by the site in a particular timeframe, usually the preceding 18 months. Separate listings should be requested for each type of case (clear, containing derogatory information, terminations, denials, and suspensions). If backlogs exist (timeliness issues) in the completion of these cases, inspectors should determine the causes. Interviews with security managers will assist in making these determinations.

C. Inspectors should review CESs from a selection of PSFs known to contain derogatory information to determine whether the derogatory information was resolved in a timely manner, and if the adjudicative guidelines were used as the basis for resolution. Case analysis documentation must describe the derogatory information and include the mitigating factors considered by the specialist in making the final clearance determination. Timely CPCI data entry should also be validated for the selected cases.

D. Inspectors should review cases in which the clearance was denied or suspended to determine whether or not proper procedures were followed and if timely CPCI data entries were made.

3.6 Reinvestigations

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” clearance be re-evaluated every five years, and those holding an “L” clearance be re-evaluated every 10 years.

Common deficiencies, potential concerns, planning activities, data collection activities, and performance tests for reinvestigations are the same (with the exception of those items related to applicant cases and meeting IRTPA standards) as for applicant cases.

Section 4: Safeguards and Security Awareness Program

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.

4.1 Administration and Management

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, safeguards and security awareness coordinators may 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 offsite contractors, subcontractors, consultants, and access permittees in their SSAP.

Common Deficiencies/Potential Concerns

Inadequate Documentation

Although all DOE/NNSA sites have mature security awareness programs, self-assessments, surveys, and inspections periodically identify that SF-312, *Classified Information Nondisclosure Agreement*, and/or Security Termination Statements (DOE Form 5631.29) are not always obtained from individuals or maintained in a manner that allows for their expeditious retrieval, when needed.

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 or not the program is effective. Without adequate documentation, current and relevant program materials, and effective communication of program requirements, 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. Although security termination statements are required to be filed in the individual's PSF, some sites have also incorrectly filed SF-312s there as well.

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.

Planning Activities

- Determine whether or not 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 or not 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 documentation exists to reflect conducted briefings by type, date, and the attendance of individuals at the briefing. Record-keeping systems must be capable of providing an accurate 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 planning, or supplemental awareness material could indicate inadequate management support or budget constraints. If problems exist, inspectors should attempt to determine their cause.

C. Inspectors should determine whether or not adequate guidance is established relative to the conduct of briefings, including initial, comprehensive, refresher, foreign travel (when applicable), and termination briefings.

D. Inspectors should determine whether or not comprehensive briefings are conducted prior to the issuance of security badges.

Safeguards and Security Awareness for Contractor Personnel

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

F. A list of security terminations should be compared to badge retrieval/destruction records and CPCI to determine if security terminations were effected in a timely manner. It may also be useful to compare employee terminations with clearance terminations to ensure all security clearances were terminated as required. A list of all terminated cleared contracts and the personnel associated with these contracts should also be reviewed to determine if clearances that are no longer required have been appropriately terminated.

G. 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, relevant, and stimulating are usually more effective in promoting the optimal level of security awareness for the audience.

Performance Test

H. Inspectors should determine the qualifications and performance of awareness coordinator(s) by interviewing the coordinators and by attending live briefings. It is desirable that the coordinators have DOE/NNSA security experience and are able to speak authoritatively on the topics presented.

4.2 Safeguards and Security Awareness Briefings

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 assuming duties. These briefings are the employees' initial introduction to security and set the tone for their overall understanding of security responsibilities and DOE facility requirements.

- **Comprehensive briefings** are designed to ensure that individuals who have been granted DOE security clearances are fully aware of their security responsibilities before they access 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 security clearance and have access to classified matter or SNM. These annual required refresher briefings serve as a continuing reminder to employees of their ongoing security responsibilities and of the intelligence threat. These briefings 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 security 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 clearance and are traveling to sensitive countries. These briefings are normally presented by the local counterintelligence organization, but at some sites, they are performed 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 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 recurring annual refresher briefings, are varied, incorporate new material, contain examples and anecdotes, and reflect up-to-date security procedures and the current facility environment.

- **Initial briefings.** At some sites, a member of the employment department, or someone outside the security organization, presents 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.

- **Annual Security 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.

Significant deficiencies in control and presentation of refresher briefings may indicate inadequate management attention or insufficient resources are 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 offsite employees are often unavailable to sign termination statements or to receive the required termination briefings. It is important to have a system in place to track employee terminations, so that all cleared employees being terminated receive a termination briefing. In those cases where the individual is not available or refuses to sign the termination statement, the records should be annotated accordingly, and, when required, DOE/NNSA should be notified of the situation.
- **Foreign travel briefings.** For those security organizations 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 presented 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 the adequacy and sufficiency of samples of supplemental awareness materials used in support of the SSAP.
- Review listings of all employees' security clearance grant dates, comprehensive security briefing attendees, and annual security refresher briefing attendees for the past 18 months.
- Review a sample of documentation notifying employees of the requirement to attend specific briefings.

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 the materials adequately support the comprehensive briefing.

Annual Security 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. Inspectors should also determine what action (including denial of access) is taken when individuals fail to complete a required annual refresher briefing.

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 for onsite and offsite personnel (may require contacting the designated Facility Security Officer) are conducted, badges are returned, and a security termination statement 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. Inspectors should reconcile the actual dates of termination of DOE clearances with CPCI data to ensure clearance terminations were entered into CPCI within 24 hours.

Foreign Travel Briefing

J. 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.

Performance Tests

K. 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.

L. Inspectors should determine if the SF-312s and security terminations statements are being maintained as required.

4.3 Supplemental Awareness Materials

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.

Section 5: Human Reliability Program

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 ensure 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
- (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” clearance, which includes an initial special BI and a reinvestigation every five years.

Personnel enrolled in HRP are evaluated through a process of continuous observation for signs of aberrant behavior. Annual training in observation of aberrant behavior is provided to HRP supervisors and employees to assure that individuals in the HRP are aware of behaviors 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, or 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.

HRP medical officials do not always 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 a material access area (MAA) 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.

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 oversight 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. Also, the lack of coordination and inter-action with the site vulnerability assessment organization could cause positions to not be identified as requiring inclusion in the HRP.

Another potential concern is failing to enroll individuals who are routinely working in areas that require enrollment. Although these individuals are escorted during these times, the frequency of access by some of these individuals could provide them with knowledge of sensitive operational and security information. In these cases, the absence of effective site tracking mechanisms for escorted visitors has led to the failure to enroll these individuals in HRP. In some of these cases, the frequently escorted visitors were found to be HRP candidates. Their access to sensitive areas is prohibited as they are not to perform HRP duties prior to certification. Care must be taken to review site procedures that allow HRP candidates to access sensitive areas for the purpose of training on their future HRP duties.

Inadequate HRP Drug and Alcohol Testing Program

In carrying out the drug and alcohol testing program, sites might not have established a methodology that ensures random selection and testing that provides effective detection and deterrence of illegal drug use or abuse of alcohol. The best method for providing the maximum capability to detect and deter is selection and testing 24/7 every day that workers are performing HRP duties, both during normal work shifts and during off-shifts, weekends and holidays. Individuals working off-shift and on holidays and weekends must have the same probability to be selected as individuals working during the day shifts.

Some sites have developed selection algorithms that significantly reduce the probability of selecting individuals once they have already been tested. 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 do not have a process for conducting tests for reasonable suspicion, following an occurrence, incidents, and unsafe work practices. 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 or on the job.

Some sites may not have a process in place to ensure that random drug and alcohol testing occurs at least once during the 12 months since the previous test.

Drug and alcohol testing facilities do not always meet established requirements (no access to a source of water, chemicals in the testing area, and lack of visual and aural protection). The existence of this shortfall can be directly attributed to failure of self-assessments or surveys to comprehensively evaluate the HRP.

With regard to alcohol testing, some sites have not established a quality assurance program that ensures that breathalyzers used by site testing technicians meet functioning requirements as prescribed by the manufacturer and are producing accurate test results. For the drug testing program, blind test programs are required to ensure that the certified testing laboratory used to conduct analyses of collected urine specimens is producing accurate test results. The lack of either program diminishes the overall effectiveness of the alcohol and drug testing program.

Inadequate HRP Medical Assessment

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 re-certification. 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 applicable medical professionals or be placed in the files to ensure its availability each time an HRP-certified individual is seen.

Improperly Conducted HRP Supervisory Reviews

If supervisors 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 to be able to realistically complete the annual supervisory review and/or report each observed safety or security concern to the HRP Management Official.

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 determine the affects of prescribed medications on the cognitive ability of HRP employees. Many opiate-based medications 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 a security

concern 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 JTAs), how long personnel have been in these positions, and all personnel pending initial certification.
- Determine if the site has established a process for identifying positions and employees for HRP. This process should include the requirement for the formal analysis to be conducted in support of enrollment of individuals who can significantly impact national security (criteria 4 positions). Furthermore, each site should have a process in place that allows for the tracking and trending of escorted visitors to the MAA to assist in determining if such access requires the individual to be enrolled in HRP or denied further escorted MAA access. HRP officials should also be in close coordination with vulnerability assessment team members.
- Determine if the site has a process in place for the immediate removal of individuals who test positive for illegal drugs or alcohol abuse.
- Determine whether or not the facility(s) has a random drug and alcohol testing program and if the program includes: testing for reasonable suspicion following an occurrence, incident, or unsafe work practice; chain-of-custody procedures; unannounced selection and testing procedures; employees notification for testing and how this is documented; procedures and documentation for employees selected for testing, but not tested; process for tracking if at least one test is conducted within 12 months of the last test; and availability of all materials required to effectively conduct the tests.
- Identify the level of direct or non-random drug and alcohol testing to determine if testing is sufficiently random. Also, determine the authorized excuses for not completing a drug or alcohol test after being selected.
- Determine whether or not the drug and alcohol testing program technicians are trained and/or certified, testing equipment is approved by the Department of Transportation, procedures are in place to ensure that all whom test 0.02 or greater are sent home, concentrations above 0.04 are recorded, and additional actions are taken to determine if the consumption occurred on the job. Also determine if the site has established an effective quality assurance program that includes external calibration checks on all breath testing devices used and a drug testing blind sample program.
- Review the site's list, if any, 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 or not managers, supervisors, and HRP personnel receive awareness training in the recognition of aberrant behavior every 12 months.

- Determine whether or not 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 removed individuals have also been removed from the site's access control system for the MAA or areas that store or possess nuclear weapons, components, or SNM.
- Determine if supervisors are able to adequately observe subordinate HRP-certified employees or have a mechanism in place to obtain input from those who do observe HRP-certified employees when completing the annual supervisor review.

Data Collection Activities

HRP Plans and Enrollment

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. Evidence should be available to substantiate that HRP officials are considering vulnerability assessment results when identifying positions that require HRP enrollment.

B. Inspectors should review MAA access records to determine if there are individuals who are granted escorted access to the MAA 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 information between 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 if initial and annual refresher training is completed, and whether or not the records 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 or not medical personnel who support HRP have received adequate training concerning program objectives and their individual roles and responsibilities, that they are knowledgeable of what medical/mental conditions constitute a security concern, and they understand the requirement to report these conditions to the HRP Management Official.

E. Inspectors should determine whether sufficient training materials have been developed for the training staff and for all other 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 facilities, equipment (including the quality assurance program), and 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. Inspectors should observe drug and alcohol tests being performed to determine whether policy and procedures match actual practice. For drug testing, inspectors should review procedures for handling specimens to determine whether an effective chain of custody is maintained, and determine if the site has established a blind sample test program. Inspectors should also observe the administration of a breath alcohol test.

G. Review the selection process for random testing to determine whether it is, in fact, conducted on a random, unannounced basis, and that individuals selected for testing arrived within two hours of notification. Additionally, 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 excusing individuals from testing; testing employees for reasonable suspicion; and testing following an incident, unsafe practice, or occurrence. Additionally, it should be determined how information is communicated among supervisors and the safety and security organizations. If some employees have not been tested, determine why they were excluded. Determine if there is consistency in testing for these reasons and if reasons for conducting these types of testing are well known and specified in written procedures. Inspectors should also review lists of disciplinary actions, accidents, and security incidents to determine if applicable individuals are being tested for occurrences and/or reasonable suspicion.

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 or not all parts have been completed annually, including the 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 eQIP on an annual basis (normally part of the supervisory review), and that the forms are submitted in a timely manner. Re-certifications must be completed within 12 months of the last certification or re-certification 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, what action was taken, and whether the action was taken in a timely manner.

Reporting Requirements

L. Inspectors should determine whether a full understanding exists between the site's HRP medical 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

M. 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.

N. Inspectors should review randomly selected files to determine if a system is in place for maintaining HRP, medical, and psychological 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. This review will also assist the inspector in determining if good lines of communications exist between HRP and medical officials.

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

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 visitors must ensure that the potential threat that these foreign visitors 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 visitors to these security interests. The analysis should be based on the foreign visitors' 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, 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 Customs Enforcement 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 Customs Enforcement information for review and documentation in the Foreign Activities Central Tracking System (FACTS). This is required in order to verify identity, to verify authority to work, and to ensure that the foreign visitor is currently eligible to be in the United States. Upon arrival at the site, foreign visitors must be required to produce personal identification and legal status documentation prior to the foreign visitor receiving a site badge or being granted access to site facilities.

Inadequate Security Plans for Visits

“Generic” and “specific” security plans are required for all FV&A. “Generic” plans are for non-sensitive visits and assignments, while “specific” security plans must be developed 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.

Some sites utilize SSSPs to serve as a “generic” security plan. However, these plans do not provide adequate control measures for foreign visitors. Security planning is more effective when the unique access requirements of each visit are addressed separately. Although most sites develop “specific” security plans, the plans do not always include all security interests, existing protection measures, and actions to address unmitigated potential security concerns. 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 visitor 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.

Badge Issues

Inappropriate issuance, control, and retrieval of foreign visitor badges continue to be a problem at some DOE/NNSA sites. In many cases, badge office personnel are incorrectly issuing foreign visitor badges that are reserved for site employees. In other cases, foreign national visitors are allowed to enter site facilities either without a badge or with an expired foreign national badge. These issues are especially prevalent at sites that employ many foreign nationals. Nevertheless, sites have the responsibility to only issue the appropriate badge to foreign visitors, and site employees have the responsibility to not allow foreign visitors (or anyone) to access site facilities without a badge.

Deterioration of Escort Procedures

Vigilance in escorting foreign visitors, 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

Although recent inspection experience has shown that many 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 also often not reported by hosts, and, in other cases, new hosts or escorts are not designated.

Another potential concern can arise if the host is not assigned to the facility or location where the foreign 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 also assist in escort training.

Inadequate Computer Access Controls

Determining the implications of allowing foreign visitors and assignees access to computer systems is a matter for review by the Office of Cyber Security Evaluations. 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 visitor and are not password protected. A particular problem occurs with foreign personnel who are provided remote access to computer networks and these individuals 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 close out a visit or to indicate that the visit was cancelled. Additionally, some sites are not validating that automatic uploads into FACTS have been successful. When validation is not being completed, 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.

Planning Activities

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

Data Collection Activities

Plans and Procedures

A. Inspectors should determine whether or not 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 appropriate security plans 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 or not 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 selected site subject matter experts (operations security, 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.

Security Plan Data

D. 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 visitors are allowed to visit or are assigned. Effort should be taken to ensure that security plans recognize the existence of classified and/or sensitive material in, near, or adjacent to foreign visitors at the site and that appropriate protection is afforded to these materials.

Non-Compliance

E. Inspectors should review all incidents involving a foreign national visitor/assignee and determine whether or not actions the site has taken appropriately identify causes for the incidents and assign consequences.

Performance Tests

F. Inspectors should consider conducting one of the following performance tests of the unclassified FV&A elements.

- Conduct walking tours of areas that have or are hosting foreign visitors to determine the sufficiency of actions taken to mitigate the threat represented by the presence of foreign visitors, and if other personnel in the area are aware that foreign visitors are present.
- During the walking tours, interview the host or escorts for the visit or assignment to determine if each host/escort is knowledgeable of security plan requirements and their responsibilities pertaining to the visit.
- Interview any visiting foreign nationals who are on site to determine their knowledge of authorized access and their own responsibilities.

This page intentionally left blank.

Section 7: Interfaces

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 element of the inspection activities. Thorough integration creates a synergism that stimulates the inspection process and enhances the quality and validity of the OIO inspection report. Effective integration 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 that other topic teams 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, which 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.

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 regarding escort procedures for foreign visitors may be valuable to security systems, cyber, and CMPC topical areas.

Protection Program Management

The personnel security topic team often interfaces with the 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 clearances; 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 management's 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 visitor 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 violations of the need-to-know principle and improper levels of access should be reported to the personnel security topic team. In addition, the location of classified and sensitive data on a site (as identified by the CMPC topic team) can be used to identify potential access to this data by foreign visitors and assignees.

The CMPC topic team can also review OPSEC working group meeting minutes and interview staff to determine whether foreign 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 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 to engage in various activities. Visitors may be conducting unclassified work or working on classified projects with an appropriate clearance. 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 clearances.

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 visitors who are in a particular area.

This page intentionally left blank.

Section 8: Analyzing Data and Interpreting Results

Introduction

This section provides guidelines to help inspectors analyze data and interpret the results. The guidelines include information on the analysis process and 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 clearances 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 Questionnaires for National Security Positions, 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 is 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 clearances 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 Department of Energy Acquisition Regulation, 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 clearances 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's 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 visitors 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 HRP-certified employees 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. However, in the discussion and opportunities for improvement, the inspectors may choose to discuss the general problem with assignment of responsibilities as a contributing factor.

As part of the analysis process, Independent Oversight inspectors should review the results (both positive aspects and weaknesses/findings) of the review of the personnel 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

Personnel Security Program Performance Measures	A-2
Personnel Security Detailed Inspection Plan.....	A-5
Personnel Security Inspection Process Matrix	A-23
Document Request List.....	A-37
DOE Site.....	A-37
NNSA Site	A-44
Methodology for Reviewing Personnel Security Files	A-51
Personnel Security File Data Collection Forms	A-52
Derogatory Information	A-52
Terminations.....	A-54
Clear Cases	A-56
Pending Re-investigation	A-57
Unscreened Files	A-59
Pre-employment Check Data Collection Form	A-62
Clearance Justification Data Collection Form.....	A-63
HRP File Review Data Collection Form	A-66
HRP Breath Alcohol Test Checklist.....	A-67
HRP Drug Test Checklist.....	A-71
Data Collection Form and Instructions.....	A-75
Instructions for Completing an Issue Form	A-77
Report Preparation	A-78

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 Accountability 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 the following:

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 RELIABILITY PROGRAM

The insider threat has been mitigated by the following:

1. All positions meeting the requirement for enrollment have been identified and communicated to applicable managers 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 tests for drugs, alcohol, and prescription 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, including 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 the following:

1. All awareness program briefings and supplemental materials are accurate and up to date.
2. Access to classified matter or special nuclear material is not authorized prior to completion of all program requirements (initial and comprehensive briefings).
3. For all persons who no longer require 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 the following:

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 (e.g., security, counterintelligence, export control, cyber, operations security [OPSEC], classification), 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 visitor have been reported to DOE/NNSA, thereby indicating that hosts and escorts are knowledgeable of their duties and responsibilities.

PERSONNEL SECURITY DETAILED INSPECTION PLAN

(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>MANAGEMENT: Does management ensure that the personnel security program represents a logical and cost-effective approach to protecting against the insider threat?</p> <p>Is senior management support evidenced by proper funding and personnel security program resources, and by support for recommendation to suspend or revoke clearances?</p> <p>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.</p>			
<p>Management: Line management responsibility for safeguards and security is exhibited by management’s recognition of the significance of an effective personnel security program.</p>	<ol style="list-style-type: none"> 1. Have self-assessments, surveys, and/or inspections identified systemic deficiencies concerning delays resulting from processing unnecessary clearance 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. Has the number of access authorizations been reduced to the least possible number to still meet operational requirements? 	<ol style="list-style-type: none"> 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 the conduct of 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. 	<p>pre-planning</p> <p>pre-planning and on site</p> <p>pre-planning</p> <p>on site</p> <p>pre-planning</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	5. Are there sufficient funds in the budget to support retention of adequate staff and for training?	6. Review records to determine the number of personnel assigned against the number authorized. 7. Conduct interviews and review records to determine whether an action plan exists for the review and elimination of clearances.	pre-planning on site
Management: Personnel competence and training are maintained by management making adequate resources available to perform all personnel security program functions.	1. Does the Safeguards and Security Director use a sufficient basis for asserting that individuals performing personnel security functions are technically competent? 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 and Security Director or person responsible for the training of the personnel security professionals to determine whether the program has been formalized, whether it is based on a needs analysis 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. Conduct interviews and/or 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

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>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.</p> <p>Management ensures that personnel security plans, policies, and priorities are adjusted to meet changing threat situations.</p>	<ol style="list-style-type: none"> 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 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? 	<ol style="list-style-type: none"> 1. Interview managers and personnel security professionals to determine the extent to which personnel security professionals participate in planning meetings, budget discussions, and management-level decisions. 2. Review the SSSP and other security and operational planning documents to determine how personnel security concerns are addressed. 3. Review site policies to determine whether personnel security program officials are in a position to ensure compliance. 4. Conduct interviews and/or 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. 	<p>on site</p> <p>pre-planning</p> <p>pre-planning</p> <p>on site</p> <p>pre-planning</p> <p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>Management: Feedback and improvement is supported by effective self-assessment and corrective action programs.</p>	<p>1. Has the self-assessment program identified significant program weaknesses that, when addressed, would materially enhance program implementation?</p> <p>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 of progress, assign responsibility for each action to a specific individual, continually update the plan, and ensure that adequate resources are applied) to ensure that identified weaknesses are addressed in the most effective and efficient manner?</p>	<p>1. Review past self-assessments to determine whether they reflect thorough coverage of the personnel security program and are conducted on a regular basis.</p> <p>2. Review records to determine who conducts the self-assessments and their qualifications.</p> <p>3. Review records to determine whether concerns identified during self-assessments are entered into a central tracking system.</p> <p>4. Review procedures to determine whether the corrective action process contains all the required elements.</p> <p>5. Review records to determine whether some form of independent verification of closure of findings is in place.</p>	<p>pre-planning</p> <p>pre-planning</p> <p>pre-planning</p> <p>pre-planning</p> <p>pre-planning</p>
<p>PERSONNEL SECURITY CLEARANCE: Are only the most demonstrably reliable and trustworthy individuals (free of unadjudicated derogatory information) determined to be eligible and therefore granted access to classified matter and/or special nuclear material?</p> <p>Is the process used to determine eligibility credible and timely?</p> <p>IMPACT: Flaws in the process to determine reliability and trustworthiness undermine the first line of defense against the insider threat.</p>			
<p>Clearance: Request process (type of clearance) ensures that the type of clearance is appropriate.</p>	<p>1. Is the system in place sufficient to ensure the proper and timely review of clearance requests?</p> <p>2. Are all of the key elements in place to process requests? -Certification that the request is justified?</p>	<p>1. Review site procedures and interview program personnel to determine how the process is conducted.</p> <p>2. Review a sample of security files to evaluate whether local criteria for justifications are being used consistently.</p>	<p>pre-planning and on site</p> <p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN

(pages A-5 through A-22)

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

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>Clearance: DOE screening and analysis support the action taken (grant, disapprove, or send to Office of Personnel Security) concerning a request for clearance.</p> <p>The contractor badge program ensures that badges are issued only after a clearance is granted and awareness requirements have been completed.</p>	<ol style="list-style-type: none"> 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 clearance requests? 7. Is there an active quality assurance process? 8. Are PSFs organized in a consistent manner, accurate, and complete? 	<ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> -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 	<p>pre-planning and on site</p> <p>on site</p> <p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	9. Are procedures in place to ensure that badges are issued only to properly cleared individuals?	-Case reference sheets document the resolution or mitigation of all identified derogatory information -All derogatory information has been identified 4. Review the 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?	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 whether: -Local procedures are being followed -All derogatory information was reviewed, evaluated, and adjudicated in a timely manner	on site pre-planning on site

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	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?	-Case results are supported by the information provided by LOI and interviews -Decisions to refer for additional investigation are justified -Decisions to grant a clearance that have been made without a referral are justifiable -In cases where access was suspended, all procedures were followed and appropriate documentation exists to justify suspension -There is 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 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

PERSONNEL SECURITY DETAILED INSPECTION PLAN

(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>HUMAN RELIABILITY PROGRAM (HRP): Is the program identifying and enrolling all positions identified in the SSSP to mitigate the threat represented by insiders and therefore providing all the intended benefits of an enhanced safeguards and security human reliability program?</p> <p>Does the system of continuous evaluation identify those individuals who may represent a reliability, safety, and/or security concern?</p> <p>IMPACT: Weaknesses in this program could lead to unacceptable damage to specific national security interests.</p>			
<p>Human Reliability Program: Plans, policies, and procedures are complete and up to date.</p>	<ol style="list-style-type: none"> 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 serving in HRP positions meet all HRP requirements? 3. Have program responsibilities been formally assigned? 4. Has a comprehensive implementation plan and/or schedule for implementation been developed? 	<ol style="list-style-type: none"> 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. 	<p>pre-planning</p> <p>pre-planning</p> <p>on site</p>
<p>Human Reliability Program: Reviews and evaluations are completed as required and are comprehensive.</p>	<ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 1. Interview supervisors, medical personnel, personnel security specialists, HRP certifying officials, and individuals serving in HRP positions to determine whether the required evaluations and assessments are being completed. 	<p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		2. Review HRP forms, QNSPs, and other parts of evaluations and assessments to determine whether they are complete and whether they were completed in a timely manner.	on site
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 who have been recently tested to verify that testing was conducted 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 for being able to identify aberrant behavior and take appropriate action (immediate removal/reporting)?	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

PERSONNEL SECURITY DETAILED INSPECTION PLAN

(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	2. Are supervisors aware of their responsibility for reporting any security concerns to the appropriate officials, and if necessary, taking immediate action?		
Human Reliability Program: Reporting requirements are met.	1. Is there sufficient coordination among 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
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 (SSAP): 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?			

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>Has a method been developed to measure the effectiveness of the program?</p> <p>IMPACT: The ultimate effectiveness of the site protection program depends on the actions of all employees. Consequently, a poorly designed and implemented SSAP can have a serious impact.</p>			
<p>Safeguards and Security Awareness Program: Administration and management supports program implementation.</p>	<ol style="list-style-type: none"> 1. Do program procedures and documentation support full implementation? 2. Do the parameters of the program include coverage for subcontractors? 	<ol style="list-style-type: none"> 1. Review policies and procedures to determine whether a structured SSAP has been implemented for onsite personnel and offsite 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. Conduct interviews and/or review records to determine whether the Operations Office has delegated the authority for oversight/implementation of contractor and subcontractor SSAPs. 	<p>pre-planning and on site</p> <p>pre-planning</p> <p>on site</p>
<p>Safeguards and Security Awareness Program: Briefings are comprehensive and are conducted as a precondition to initial and continuing access.</p>	<ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 1. Review a sample of SF-312 forms to determine whether the date of the comprehensive briefing preceded the date when clearance was granted. 2. Compare badging dates with dates of initial briefings to ensure that the briefings were conducted prior to badging. 	<p>on site</p> <p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	4. Do all onsite and offsite personnel complete annual refresher briefings? 5. Are required briefings given to personnel traveling abroad?	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.	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 procedures are 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, 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 SSAP questionnaire to determine the effectiveness of aids and other materials.	on site on site

PERSONNEL SECURITY DETAILED INSPECTION PLAN
(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>Safeguards and Security Awareness Program: Coordinator training is evident in the quality of the briefings.</p>	<p>1. Do the individuals assigned the responsibility to coordinate and present safeguards and security awareness briefings possess the proper skills and knowledge?</p>	<p>1. Review records to determine whether the coordinator has attended the DOE-required training.</p> <p>2. Review records that substantiate the qualifications of other personnel responsible for the development and presentation of the briefings.</p> <p>3. Attend briefings to evaluate the presenter’s skill and knowledge.</p>	<p>pre-planning</p> <p>pre-planning</p> <p>on site</p>
<p>Safeguards and Security Awareness Program (SSAP): Feedback is continuous and leads to program enhancements.</p>	<p>1. Does employee knowledge reflect an effective SSAP?</p> <p>2. Which feedback mechanisms (surveys, self-assessments, OPSEC programs, questionnaires, tests, etc.) provide data (written or verbal) to the program manager?</p> <p>3. Are the results of these mechanisms analyzed to identify lessons learned or potential enhancements?</p>	<p>1. Review the results of the SSAP questionnaire.</p> <p>2. Interview the coordinator to determine what type of feedback mechanism is used, if any, how the data is used.</p> <p>3. Incidents of security concern records should be reviewed for any trends that are relative to the effectiveness of the SSAP.</p>	<p>on site</p> <p>on site</p> <p>on site</p>
<p>UNCLASSIFIED FOREIGN VISITS AND ASSIGNMENTS (FV&A): Does the FV&A program prevent or mitigate unauthorized access to or unintentional disclosure of classified information, sensitive unclassified information, and/or special nuclear material?</p> <p>IMPACT: The lack of a comprehensive FV&A 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.</p>			

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
<p>Unclassified Foreign Visits and Assignments: Procedures provide a basis for an integrated approach.</p>	<ol style="list-style-type: none"> 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 do they ensure proper integration and communications between all parties? 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? 	<ol style="list-style-type: none"> 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. 4. Review records to determine whether approval is held by either the Operations Office Manager or Laboratory Director (delegation to only one level down is 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 FV&A program is periodically assessed to identify and correct program weaknesses. 	<p>pre-planning</p> <p>on site</p> <p>on site</p> <p>pre-planning</p> <p>pre-planning and on site</p>
<p>Unclassified Foreign Visits and Assignments: Indices checks are used to identify potential risks.</p>	<ol style="list-style-type: none"> 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? 	<ol style="list-style-type: none"> 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. 	<p>on site</p> <p>on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	2. Are counterintelligence (CI) consultations used appropriately in lieu of indices checks?		
<p>Unclassified Foreign Visits and Assignments: Security plans and coordination ensure the consideration of all security factors.</p>	<p>1. Are all security plans (especially generic security plans) sufficiently detailed to ensure that inadvertent compromises of security interests do not occur?</p> <p>2. Does the approach to assessing risks include the identification of all classified and sensitive unclassified information and activities, why the information is sensitive, mechanisms for compromise, and actions to mitigate any residual risks?</p> <p>3. Do security plans adequately address and control remote access to site computing assets?</p> <p>4. Do FV&A officials coordinate requests with OPSEC, CI, and export control program officials/subject matter experts?</p> <p>5. Are foreign nationals permitted access to or use of computing assets?</p> <p>6. Are foreign nationals appropriately badged?</p>	<p>1. Review records to develop an understanding of the site’s approach to assessing risk (including coordination with OPSEC, CI, and export control program officials).</p> <p>2. Interview subject matter experts to determine whether they are qualified.</p> <p>3. Review the Sensitive Subjects List and determine whether it is current and whether it includes a site-specific addendum for identifying additional subjects.</p> <p>4. Review a selection of specific and generic security plans to determine whether they are sufficiently detailed to make decisions concerning their adequacy and comprehensiveness.</p> <p>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.</p> <p>6. Conduct interviews and/or review records to determine the level of coordination with cyber security program managers regarding onsite and offsite use of computing assets.</p>	<p>pre-planning</p> <p>on site</p> <p>on site</p> <p>pre-planning and on site</p> <p>pre-planning and on site</p>

PERSONNEL SECURITY DETAILED INSPECTION PLAN
(pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
		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 the areas that host foreign national visitors to determine whether those visitors are in possession of their badges.	
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/instruction. 2. Examine escort training materials to determine whether they are adequate. 3. Interview escorts to determine whether they are periodically reminded of their responsibilities.	pre-planning pre-planning on site
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 (identify enhancements, conduct investigations, issue infractions, etc.)?	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.	on site on site

PERSONNEL SECURITY DETAILED INSPECTION PLAN
 (pages A-5 through A-22)

PERFORMANCE MEASURE	CRITICAL CRITERIA/LINES OF INQUIRY	DATA COLLECTION ACTIVITIES	REMARKS
	3. Are incidents of security infractions reported?	3. Determine whether the host report is 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. Conduct interviews and/or 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.	pre-planning and on site on site pre-planning and on site

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

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. <i>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.</i>
Review site protection strategy, vulnerability assessments (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

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
After the completion of the above, complete the following: -Confirm topic and subtopic 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 e-mail) topic objectives, data collection activities/schedule, and the document request list, which identifies items that need to be sent to Germantown in advance of onsite 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 FV&A data collection activities.		Team Leader

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

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 onsite 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; e-mail 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 ONSITE 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

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
When required, prepare Issue Forms. Review Issue Forms and provide to inspection management. Resolve site comments.		Team Member Team Leader Team Leader and Member
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.		Team Leader

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
(pages A-23 through A-36)

STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
(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.)		
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
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 (<i>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</i>). -Revise data collection plan and adjust resources to collect this data. -Revise topic annex/subtopical 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

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

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
When required, prepare data collection forms, and distribute to Deputy Inspection Chief and Admin Coordinator.		Team Leader
STEPS	COMPLETION DATE	ACTION OFFICER(S)/REMARKS
When required, prepare Issue Forms, review Issue Forms, and provide to Deputy Inspection Chief; resolve site comments on Issue 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
Collect data, Monday through Thursday -Interview personnel security clearance program officials and specialists. -Complete PSF reviews and record results on file review form. 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 Team

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

<p>*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.</p> <p>*Issues that could impact the topic rating should normally be discussed in the evening meeting only after:</p> <ul style="list-style-type: none"> -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). <p><i>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).</i></p>		<p>Team Leader</p>
<p><i>Must keep Team Leader informed of location and phone number (may be done via admin support personnel).</i></p>		<p>Team</p>

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

<p>-Integration with other topic teams has been completed -Inspection team management has been informed off-line (no surprises).</p> <p>Assign a team member the responsibility to capture on an Issue Form those issues that could impact the topic rating.</p> <p>(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.)</p>		
<p>Attend daily team meeting (as before, team members may be absent with approval).</p>		Team
<p>Finalize evening bullet points for Office of Health, Safety and Security (HSS) Management.</p>		Team Leader
<p>Conduct end-of-the-day security checks.</p>		Team
<p>FINAL DATA COLLECTION ACTIVITIES, DRAFT REPORT TOPIC APPENDIX PREPARATION, AND CLOSEOUT (TWO WEEKS)</p>		
<p>Collect data, Monday through Thursday -Conduct review 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.</p> <p>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).</p> <p>*The topic team leader is responsible for deciding when an issue will be raised during the evening</p>		Team

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

<p>meeting and may want to delay discussion of that issue during the evening meeting until team consensus can be achieved.</p> <p>*Issues that could impact the topic rating should normally be discussed in the evening meeting only after:</p> <ul style="list-style-type: none"> -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). <p><i>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)</i></p>		
<p><i>Must keep Team Leader informed of location and phone number (may be done via admin support personnel).</i></p>		Principal Writer
<p>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).</p> <p>Distribute to Deputy Inspection Chief and Administrative Coordinator.</p>		<p>Team</p> <p>Team Leader</p>

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

When required, prepare Issue Forms.		Team Member
Review Issue Forms and provide to inspection management.		Team Leader
Resolve site comments.		Team Leader and Member
Conduct LSPTs, as required.		Team
<p>Conduct brief topic discussion before daily team meeting on the results of data collection, leading to drafting the evening bullets, and confirm/revise schedule.</p> <p>*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.</p> <p>*Issues that could impact the topic rating should normally be discussed in the evening meeting only after:</p> <ul style="list-style-type: none"> -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). <p>Assign a team member the responsibility to capture on an Issue Form those issues that could impact the topic rating.</p>		Team Leader

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

(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.)		
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
Subtopic inspectors turn in all data collection forms and/or draft subsections 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, and 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

PERSONNEL SECURITY INSPECTION PROCESS MATRIX
 (pages A-23 through A-36)

Provide list of acronyms, interviews, and references to Admin Support Manager, Tuesday		Team
Address QRB /HS-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
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**

The information below is requested to support the Personnel Security topic team in the subtopical areas of the personnel security clearance program, human reliability program (HRP), safeguards and security awareness program (SSAP), and foreign visits and assignments (FV&A) program. This information is to be made available by all appropriate organizations, including the DOE Operations Office, the DOE site primary operating or integrating contractor, and/or the site protective force contractor or other major contractor organizations (as necessary).

Questions should be addressed to **(topic team leader)**, at **(301) (as appropriate)** or e-mail **(address as appropriate)**.

The following documents and/or information is requested to be provided by **(date)**. The preferred method of transmission of any unclassified items is in hardcopy to: **(topic team leader) DOE Headquarters – Germantown Building (Attention – applicable name, HS-61)**. If necessary, an alternative method of transmission is an attached file to an e-mail message to: **e-mail address as appropriate**. Any classified information must be sent to HS-61 according to DOE directives for mailing classified information. *(Sites may be requested to forward some portions of the document request list to specific team members instead of the topic team leader. Dates and address information for these addressees are to be provided immediately preceding the affected section(s) of the document request list.)*

1. GENERAL INFORMATION: (as appropriate)

An **organization chart(s)** or other means of describing the structure supporting the overall personnel security 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.

2. CONTRACTOR PERSONNEL SECURITY CLEARANCE PROGRAM (as appropriate)

a. Provide the following **separate, alphabetized (last name first) lists** for (contractor organizations) personnel **with a “Q” access authorization**. The timeframe for all lists is (an 18-month period—*the same 18-month period will be used throughout the document request list*).

- (1) A listing of all **clearance requests**.
- (2) A listing of all completed **pre-employment checks**.
- (3) A listing of all contractor/subcontractor employees for whom (contractor organization) 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 those requested by the Classified Matter Protection and Control topic team, but should include the reason for the disciplinary action, and the date reported to (the servicing DOE personnel security organization). Also indentify the organizations (human

relations, security, labor relations, internal contractor investigations, etc.) that are involved in making disciplinary action determinations.

b. Provide a copy of the current procedure or a description of the **badge process**, including the process for acting upon a lost badge and for retrieving badges from individuals who no longer require an access to (site) facilities (including visiting foreign nationals) and from employees who no longer do work that requires access classified information.

c. Provide a description of and procedures for **pre-employment and annual random drug testing** for (applicable contractor organizations), and their subcontractor clearance applicants and currently cleared employees, including the organization responsible for this drug testing program. Testing of these individuals is required by Secretarial memorandum, *Decisions regarding drug testing for Department of Energy positions that require access authorizations (Security Clearances)*, dated September 14, 2007.

d. Provide a list of cleared (site) employees (including support contractor employees), **as of** (a specific date—*the same date should be used throughout the document request list*), who were performing duties that may include one of the following position descriptions: **contract manager/specialist, human resource manager/specialist, labor relations manager/specialist, medical doctor/nurse/specialist/technician, computer support, building/facility manager, maintenance personnel, and cleaning personnel**. This list should include the work location of each individual (building and room) and the type of area (property protection area, Limited Area, exclusion area, Protected Area, or non-security area) where the individual's work space resides.

3. PERSONNEL SECURITY CLEARANCE PROGRAM, IDENTIFICATION AND ADJUDICATION OF DEROGATORY INFORMATION (servicing DOE personnel security organization)

a. Provide the following **separate line numbered alphabetized lists (last name first)** of personnel security cases for Federal and contractor incumbent **“Q”** clearance holders to assist in the random selection of personnel security files (PSFs) for review. The lists should include the DOE number for each individual. The timeframe for all lists is (an 18-month period).

- (1). A listing of cases for personnel who have a completed 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.
- (2). A listing of cases for personnel who have a completed 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.
- (3). A listing of all reinvestigation reports that are pending screening.
- (4). A listing of individuals who have any derogatory information and information of personnel security interest reported by their organization. This includes all potential sources for the derogatory information, such as investigations of security incidents, infraction reports, ORPS, on the job disciplinary action, or self-reporting.

- (5). A listing of all approved suspension actions.
- (6) A listing of all cases for which suspension is pending.
- b. A listing of all “Q” and “L” applicant cases that required adjudication actions to resolve drug issues. As a point of clarification, the list should include cases with other security issues as well as drug issues.
- c. Intelligence Reform and Terrorism Prevention Act statistical reports for the last six months.
- d. A copy of OPM Closed Case Reports w/out 79A for the previous two quarters.

4. FOREIGN VISITS & ASSIGNMENTS (DOE and applicable site organization)

- a. The **total number of foreign national visitors and assignees** who have visited (site) between (an appropriate 18-month period). The total number of visitors and assignees should be broken out in the following categories of visits and assignments: non-sensitive, sensitive country foreign nationals, sensitive subjects, and access to security areas (Limited, exclusion or Protected Areas).
- b. Separate **alphabetized (last name first)** listings or computer printouts of FV&As that have occurred between (an appropriate 18-month period) for each of the following: (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 onsite access to computing systems.)
 - (1) FV&As involving foreign nationals from sensitive countries.
 - (2) FV&As involving sensitive subjects.
 - (3) FV&As involving access to a Protected, Limited, or exclusion area.
 - (4) FV&As involving foreign nationals from terrorist countries.
 - (5) A listing of any foreign nationals who have approval for unescorted access to any (site) security area (Limited, exclusion, or Protected Areas).
 - (6) A listing of all visiting foreign nationals who have been granted access to (site) computing assets, with a termination date for access to the computing assets.
 - (7) A listing of foreign national visitors and assignees who have been granted remote access to (site) computing assets, with a termination date for remote access.
 - (8) A listing of all visiting foreign nationals who have been granted after duty hours access to any (site) facility.
 - (9) A listing of all security incidents and inquiries that involved either visiting foreign nationals or their hosts/escorts.
 - (10) A list of the most frequently visited site facilities (building or areas) and program organizations.

5. SAFEGUARDS AND SECURITY AWARENESS PROGRAM (DOE and applicable contractor organizations)

- a. Total number of “Q” and “L” cleared DOE and contractor employees as of (a specific date) for each organization.
- b. Separate **alphabetized (last name first), line numbered** lists (using Excel if at all possible to assist in selection to complete the questionnaire) of all cleared (DOE and applicable contractor) employees. (DOE and applicable contractor organizations) should also provide a separate listing for cleared support/subcontractor employees and their duty location.
- c. The following **separate, alphabetized (last name first) lists** for personnel **with a “Q” access authorization**. The timeframe for all lists is (an appropriate 18-month period).
 - (1) A listing of clearance **terminations**, and the date of termination. This list should **not** include transfers or anything that is not a termination of the clearance.
 - (2) A listing of all individuals whose employment has been **terminated** (this list should **not** include individuals who were re-employed by (applicable contractor organization) or a subcontractor within six months), and the date that employment was terminated. This list should be based on employment and not clearance records.
 - (3) A listing of all individuals who have been **granted** an initial access authorization, the date action to grant was taken by DOE, and the date a DOE security badge was issued.

6. HUMAN RELIABILITY PROGRAM (DOE and applicable contractor organizations)

- a. Copy of the **HRP Implementation Plan(s)** and documentation of review and approval by the Manager.
- b. A **separate, alphabetized (last name first)** listing for (DOE and applicable contractor organizations) employees enrolled in the HRP program as of (a specific date). Include each individual’s duty position and the name of the supervisor who completes the annual supervisor review (and signs the supervisor review block on DOE Form 470.3) for each individual.
- c. Description of process used to **evaluate positions** for designation as HRP.
- d. An alphabetized (last name first) listing of all individuals who are **pending HRP certification** as of (a specific date), including the date they were submitted for certification, and the date their clearance was granted.
- e. An alphabetized listing (last name first and then first name/initial) of **non-HRP enrolled escorted visitors (including those individuals pending HRP certification)** to a (site) MAA between (an appropriate 18-month period). If at all possible, the listing should group all the entries for each escorted visitor and should include all of the date(s) of access (earliest to latest), the MAA(s) accessed on each date, the reason for each access, the individual’s employer (DOE or applicable contractor organization), and the individual’s clearance status (uncleared, “Q” cleared, or “L” cleared).

f. List of positions and job titles for which **job task analyses** (JTAs) have been developed for each organization, and an example (blank form) of the JTA format used by each organization.

g. A list of all HRP positions that you have deemed are subject to the **CI polygraph examination** in accordance with 10 CFR 709.

h. The following **separate, alphabetized (last name first) lists** for (DOE and applicable contractor organization) employees enrolled in the **HRP program**. The timeframe for all lists is (an appropriate 18-month period).

- (1) A listing of all HRP individuals who have been temporarily removed, with the date of removal and the reason for temporary removal indicated (security, safety, medical or changes of position/employment) and, if applicable, the date of reinstatement.
- (2) A listing of all HRP individuals who have had their HRP certification revoked, with the date and the reason for revocation indicated (security, safety, medical or changes of position/employment).
- (3) A listing of all HRP individuals who have had any disciplinary action(s), including the reason for the disciplinary action, the date the disciplinary action was taken, whether the individual was temporarily removed from HRP as a result of the disciplinary action, and, if applicable, the date of reinstatement.
- (4) A listing of all HRP individuals who have been involved in an accident or incident that was reported to the HRP management official.
- (5) A listing of all HRP individuals who were tested for drugs/alcohol as a result of an accident or for reasonable suspicion, and the date of testing.
- (6) A listing of all HRP individuals who were selected for drug and alcohol testing but were not tested, the date selected, and the reason for not being tested.
- (7) A listing of all HRP individuals who have been designated as prohibited from consuming alcohol for eight hours preceding schedule work.

i. List of the **equipment used for alcohol testing**.

j. An alphabetized listing of all current (a specific date) HRP-certified individuals (last name first), initial certification date, and the **dates of the last three drug and alcohol tests** for each.

Please provide the following documents to the Personnel Security topic team at the inspection worksite on (specific date of first day of the inspection).

1. General Information: A copy of the last two **self-assessment reports** of any element of the personnel security program. If these reports identified any personnel security deficiencies that required the development of one or more corrective action plans (CAPs), please provide a copy of the plans. Please treat this request separately from the request made by the Protection Program Management topic team for all self-assessment and survey reports and CAPs.

2. FV&A

- a. **Procedures** and/or protocols used to process and approve all FV&As.
- b. An **example** of a generic security plan and a specific security plan.
- c. A copy of host/escort **guidance, or training materials**.

3. HRP

- a. **HRP initial and annual unannounced drug and alcohol testing procedures** and/or protocols, the names of all technicians who are authorized to conduct these tests, date of initial certification, date of last refresher training for each technician, and, if applicable, the name and phone number of the individual (information technology support technician/programmer) responsible for developing drug and alcohol testing software selection protocols.
- b. Procedures that describe the **actions that will be taken for positive** drug and alcohol test results.
- c. A copy of all **HRP instructional materials** for supervisors, HRP certified individuals, and site occupational medical providers.
- d. A copy of the site drug test blind test program, and a list of the last six months of test program results.
- e. A copy of the alcohol test equipment quality assurance program, and the assurance program results for the last six months.

Access to the following documents and/or information may be required during the onsite phases of the inspection.

1. Personnel Security Clearance Program

- a. Local/desk-side procedures.
- b. Pre-employment check files.
- c. Badge Office records and database.
- d. Personnel Security Files.

2. HRP

- a. Records that document completion of HRP initial and annual instruction.

- b. HRP records and HRP-associated medical and psychological files.
- c. JTAs that have been developed and provided to the designated physician and psychologist.
- d. Letters of designation/certification for the Site Occupational Medical Director (SOMD), Designated Physician, Designated Psychiatrist, and Breath Analysis Technicians.
- e. Letters, if used, that give the Designated Physician or Designated Psychiatrist authority to sign for the SOMD.

3. SSAP

- a. Initial, comprehensive, annual refresher, and termination briefings and any supporting materials/handouts.
- b. Records (attendance rosters, SF 312, *Classified Information Nondisclosure Agreement*, DOE Form 5631.29, etc.) of completion of initial, comprehensive, refresher, and termination briefings.
- c. Documentation substantiating completion of required DOE training by the SSAP coordinator, and documentation that appoints the individual as the coordinator.

4. FV&A

- a. Requests for foreign national visits and assignments.
- b. Records of reviews and approvals of foreign national visits and assignments.
- c. Specific and generic security plans.
- d. Local FACTS terminal.

DOCUMENT REQUEST LIST**NNSA Site****Personnel Security**

The information below is requested to support the Personnel Security topic team in the subtopical areas of the personnel security clearance program, human reliability program (HRP), safeguards and security awareness program (SSAP), and foreign visits and assignments (FV&A) program. This information is to be made available by all appropriate organizations, including the NNSA Site Office, the NNSA site primary operating or integrating contractor, and/or the site protective force contractor or other major contractor organizations (as necessary).

Questions should be addressed to **(topic team leader)**, at **(301) (as appropriate)** or e-mail **(address as appropriate)**.

The following documents and/or information is requested to be provided by **(date)**. The preferred method of transmission of any unclassified items is in hardcopy to: **(topic team leader) DOE Headquarters – Germantown Building (Attention – applicable name, HS-61)**. If necessary, an alternative method of transmission is an attached file to an e-mail message to: **e-mail address as appropriate**. Any classified information must be sent to HS-61 according to DOE directives for mailing classified information. *(Sites may be requested to forward some portions of the document request list to specific team members instead of the topic team leader. Dates and address information for these addressees are to be provided immediately preceding the affected section(s) of the document request list.)*

1. GENERAL INFORMATION: (as appropriate)

An **organization chart(s)** or other means of describing the structure supporting the overall personnel security 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.

2. CONTRACTOR PERSONNEL SECURITY CLEARANCE PROGRAM (as appropriate)

a. Provide the following **separate, alphabetized (last name first) lists** for (contractor organizations) personnel **with a “Q” access authorization**. The timeframe for all lists is (an 18-month period—*the same 18-month period will be used throughout the document request list*).

(1) A listing of all **clearance requests**.

(2) A listing of all completed **pre-employment checks**.

(3) A listing of all contractor/subcontractor employees for whom (contractor organization) has notified or reported to (the servicing NNSA personnel security organization) **information of personnel security interest** as a result of a disciplinary action. The listing should **not** include security infraction reports like those requested by the Classified Matter Protection and Control topic team, but should include the reason for the disciplinary action, and the date reported to (the servicing NNSA personnel security organization). Also indentify the organizations (human

relations, security, labor relations, internal contractor investigations, etc.) that are involved in making disciplinary action determinations.

- b. Provide a copy of the current procedure or a description of the **badge process**, including the process for acting upon a lost badge and for retrieving badges from individuals who no longer require an access to (site) facilities (including visiting foreign nationals) and from employees who no longer do work that requires access classified information.
- c. Provide a description of and procedures for **pre-employment and annual random drug testing** for (applicable contractor organizations), and their subcontractor clearance applicants and currently cleared employees, including the organization responsible for this drug testing program. Testing of these individuals is required by Secretarial memorandum, *Decisions regarding drug testing for Department of Energy positions that require access authorizations (Security Clearances)*, dated September 14, 2007.
- d. Provide a list of cleared (site) employees (including support contractor employees), **as of** (a specific date—the same date should be used throughout the document request list), who were performing duties that may include one of the following position descriptions: **contract manager/specialist, human resource manager/specialist, labor relations manager/specialist, medical doctor/nurse/specialist/technician, computer support, building/facility manager, maintenance personnel, and cleaning personnel**. This list should include the work location of each individual (building and room) and the type of area (property protection area, Limited Area, exclusion area, Protected Area, or non-security area) where the individual's work space resides.

3. FOREIGN VISITS & ASSIGNMENTS (NNSA and applicable site organization)

- a. The **total number of foreign national visitors and assignees** who have visited (site) between (an appropriate 18-month period). The total number of visitors and assignees should be broken out in the following categories of visits and assignments: non-sensitive, sensitive country foreign nationals, sensitive subjects, and access to security areas (Limited, exclusion, or Protected Areas).
- b. Separate **alphabetized (last name first)** listings or computer printouts of FV&As that have occurred between (an appropriate 18-month period) for each of the following: (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 onsite access to computing systems.)
 - (1) FV&As involving foreign nationals from sensitive countries.
 - (2) FV&As involving sensitive subjects.
 - (3) FV&As involving access to a Protected, Limited, or exclusion area.
 - (4) FV&As involving foreign nationals from terrorist countries.
 - (5) A listing of any foreign nationals who have approval for unescorted access to any (site) security area (Limited, exclusion, or Protected Areas).

- (6) A listing of all visiting foreign nationals who have been granted access to (site) computing assets, with a termination date for access to the computing assets.
- (7) A listing of foreign national visitors and assignees who have been granted remote access to (site) computing assets, with a termination date for remote access.
- (8) A listing of all visiting foreign nationals who have been granted after duty hours access to any (site) facility.
- (9) A listing of all security incidents and inquiries that involved either visiting foreign nationals or their hosts/escorts.
- (10) A list of the most frequently visited site facilities (building or areas) and program organizations.

4. SAFEGUARDS AND SECURITY AWARENESS PROGRAM (NNSA and applicable contractor organizations)

- a. Total number of “Q” and “L” cleared NNSA and contractor employees as of (a specific date) for each organization.
- b. Separate **alphabetized (last name first), line numbered** lists (using Excel if at all possible to assist in selection to complete the questionnaire) of all cleared (NNSA and applicable contractor) employees. (NNSA and applicable contractor organizations) should also provide a separate listing for cleared support/subcontractor employees and their duty location.
- c. The following **separate, alphabetized (last name first) lists** for personnel **with a “Q” access authorization**. The timeframe for all lists is (an appropriate 18-month period).
 - (1) A listing of clearance **terminations**, and the date of termination. This list should **not** include transfers or anything that is not a termination of the clearance.
 - (2) A listing of all individuals whose employment has been **terminated** (this list should **not** include individuals who were re-employed by (applicable contractor organization) or a subcontractor within six months), and the date that employment was terminated. This list should be based on employment and not clearance records.
 - (3) A listing of all individuals who have been **granted** an initial access authorization, the date action to grant was taken by DOE, and the date a DOE security badge was issued.

5. HUMAN RELIABILITY PROGRAM (NNSA and applicable contractor organizations)

- a. Copy of the **HRP Implementation Plan(s)** and documentation of review and approval by the Manager.
- b. A **separate, alphabetized (last name first)** listing for (NNSA and applicable contractor organizations) employees enrolled in the HRP program as of (a specific date). Include each individual’s

duty position and the name of the supervisor who completes the annual supervisor review (and signs the supervisor review block on DOE Form 470.3) for each individual.

- c. Description of process used to **evaluate positions** for designation as HRP.
- d. An alphabetized (last name first) listing of all individuals who are **pending HRP certification** as of (a specific date), including the date they were submitted for certification, and the date their clearance was granted.
- e. An alphabetized listing (last name first and then first name/initial) of **non-HRP enrolled escorted visitors (including those individuals pending HRP certification)** to a (site) MAA between (an appropriate 18-month period). If at all possible, the listing should group all the entries for each escorted visitor and should include all of the date(s) of access (earliest to latest), the MAA(s) accessed on each date, the reason for each access, the individual's employer (NNSA or applicable contractor organization), and the individual's clearance status (uncleared, "Q" cleared, or "L" cleared).
- f. List of positions and job titles for which **job task analyses (JTAs)** have been developed for each organization, and an example (blank form) of the JTA format used by each organization.
- g. A list of all HRP positions that you have deemed are subject to the **CI polygraph examination** in accordance with 10 CFR 709.
- h. The following **separate, alphabetized (last name first) lists** for (NNSA and applicable contractor organization) employees enrolled in the **HRP program**. The timeframe for all lists is (an appropriate 18-month period).
 - (1) A listing of all HRP individuals who have been temporarily removed, with the date of removal and the reason for temporary removal indicated (security, safety, medical or changes of position/employment) and, if applicable, the date of reinstatement.
 - (2) A listing of all HRP individuals who have had their HRP certification revoked, with the date and the reason for revocation indicated (security, safety, medical or changes of position/employment).
 - (3) A listing of all HRP individuals who have had any disciplinary action(s), including the reason for the disciplinary action, the date the disciplinary action was taken, whether the individual was temporarily removed from HRP as a result of the disciplinary action, and, if applicable, the date of reinstatement.
 - (4) A listing of all HRP individuals who have been involved in an accident or incident that was reported to the HRP management official.
 - (5) A listing of all HRP individuals who were tested for drugs/alcohol as a result of an accident or for reasonable suspicion, and the date of testing.
 - (6) A listing of all HRP individuals who were selected for drug and alcohol testing but were not tested, the date selected, and the reason for not being tested.

(7) A listing of all HRP individuals who have been designated as prohibited from consuming alcohol for eight hours preceding schedule work.

i. List of the **equipment used for alcohol testing**.

j. An alphabetized listing of all current (a specific date) HRP-certified individuals (last name first), initial certification date, and the **dates of the last three drug and alcohol tests** for each.

Please provide the following documents to the Personnel Security topic team at the inspection worksite on (specific date of first day of the inspection).

1. General Information: A copy of the last two **self-assessment reports** of any element of the personnel security program. If these reports identified any personnel security deficiencies that required the development of one or more corrective action plans (CAPs), please provide a copy of the plans. Please treat this request separately from the request made by the Protection Program Management topic team for all self-assessment and survey reports and CAPs.

2. FV&A

- a. **Procedures** and/or protocols used to process and approve all FV&As.
- b. An **example** of a generic security plan and a specific security plan.
- c. A copy of host/escort **guidance, or training materials**.

3. HRP

- a. HRP **initial and annual unannounced drug and alcohol testing procedures** and/or protocols, the names of all technicians who are authorized to conduct these tests, date of initial certification and date of last refresher training for each technician, and, if applicable, the name and phone number of the individual (information technology support technician/programmer) responsible for developing drug and alcohol testing software selection protocols.
- b. Procedures that describe the **actions that will be taken for positive** drug and alcohol test results.
- c. A copy of all **HRP instructional materials** for supervisors, HRP certified individuals, and site occupational medical providers.
- d. A copy of the site drug test blind test program, and a list of the last six months of test program results.
- e. A copy of the alcohol test equipment quality assurance program, and the assurance program results for the last six months.

Access to the following documents and/or information may be required during the onsite phases of the inspection.

1. Personnel Security Clearance Program

- a. Local/desk-side procedures.
- b. Pre-employment check files.
- c. Badge Office records and database.

2. HRP

- a. Records that document completion of HRP initial and annual instruction.
- b. HRP records and HRP-associated medical and psychological files.

- c. JTAs that have been developed and provided to the designated physician and psychologist.
- d. Letters of designation/certification for the Site Occupational Medical Director (SOMD), Designated Physician, Designated Psychiatrist, and Breath Analysis Technicians.
- e. Letters, if used, that give the Designated Physician or Designated Psychiatrist authority to sign for the SOMD.

3. SSAP

- a. Initial, comprehensive, annual refresher, and termination briefings and any supporting materials/handouts.
- b. Records (attendance rosters, SF 312, *Classified Information Nondisclosure Agreement*, DOE Form 5631.29, etc.) of completion of initial, comprehensive, refresher and termination briefings.
- c. Documentation substantiating completion of required DOE training by the SSAP coordinator, and documentation that appoints the individual as the coordinator.

4. FV&A

- a. Requests for foreign national visits and assignments.
- b. Records of reviews and approvals of foreign national visits and assignments.
- c. Specific and generic security plans.
- d. Local 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/clearance 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 clearance 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 clearance.

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 <input type="checkbox"/> Initial/Applicant <input type="checkbox"/> Incumbent <input type="checkbox"/> Reinstate <input type="checkbox"/> Other (AA=Access Authorization)	5. High-risk Program Status <input type="checkbox"/> Yes <input type="checkbox"/> HRP <input type="checkbox"/> SCI <input type="checkbox"/> No	6. Pre-employment Check Documented <input type="checkbox"/> Yes Date: <input type="checkbox"/> No <input type="checkbox"/> NA (if employment began more than 5 years ago)	7. Justification Adequate <input type="checkbox"/> Yes Date: <input type="checkbox"/> No <input type="checkbox"/> 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 most recent issue(s)]

	CRITERIA OF ALL DEROGATORY INFORMATION	RESOLUTION METHOD(S) TO RESOLVE DEROGATORY INFORMATION
CASE EVALUATION SHEET (CES) IDENTIFYING the MOST RECENT issue(s) date: analyst:	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: <input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed: ACTION TAKEN AND DATE OF ACTION <input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> S <input type="checkbox"/> D <input type="checkbox"/> N Date:
Complete for each additional CES develop as a result of	Second Additional Adjudicative Action CES date: _____ Analyst: _____ <input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed: ACTION TAKEN AND DATE OF ACTION <input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> S <input type="checkbox"/> D <input type="checkbox"/> N Date:	Third Additional Adjudicative Action CES date: _____ Analyst: _____ <input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed: ACTION TAKEN AND DATE OF ACTION <input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> S <input type="checkbox"/> D <input type="checkbox"/> N Date:

the adjudicative actions that were required to resolve this issue.	Fourth Additional Adjudicative Action CES date: _____ Analyst: _____ <input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: _____ Date Approved: _____ Date Completed: _____ ACTION TAKEN AND DATE OF ACTION <input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> S <input type="checkbox"/> D <input type="checkbox"/> N Date: _____	Fifth Additional Adjudicative Action CES date: _____ Analyst: _____ <input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: _____ Date Approved: _____ Date Completed: _____ ACTION TAKEN AND DATE OF ACTION <input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> S <input type="checkbox"/> D <input type="checkbox"/> 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*? <input type="checkbox"/> Yes <input type="checkbox"/> 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? <input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

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	5. Pre-employment Check Documented	6. AA Justification Adequate	7. High-risk Program Status	8. Date Most Recent BI or partial BI (if last investigation) received:
				<input type="checkbox"/> Initial/Applicant <input type="checkbox"/> Incumbent <input type="checkbox"/> Reinstated <input type="checkbox"/> Other	<input type="checkbox"/> Yes Date: <input type="checkbox"/> No <input type="checkbox"/> NA (if employment began more than 5 years ago)	<input type="checkbox"/> Yes <input type="checkbox"/> No Date: <input type="checkbox"/> NA	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> HRP <input type="checkbox"/> SCI	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 |
| Association | Emotional, Mental Disorders |
| Membership | Refusal to Testify |
| Overthrow of Government | Alcohol Consumption |
| Foreign Influence | Use of or Trafficking in Illegal Drugs |
| Falsification | Personal Conduct/Finance |

- Grant
- Continue
- None Taken

12. Was consideration of applicable mitigating factors documented*? <input type="checkbox"/> Yes <input type="checkbox"/> 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	13. For Federal employee, was OPM Form 79A returned after completion of the security clearance determination? <input type="checkbox"/> Yes <input type="checkbox"/> No
--	--

PERSONNEL SECURITY FILE DATA COLLECTION FORM: PENDING RE-INVESTIGATION

PSF REVIEW FORM FOR PENDING RE-INVESTIGATIONS Rev-10/15/09	1. File Number	2. Site/Employer & Work Location	3. Job Title/Position	4. Pre-employment Check Documented? <input type="checkbox"/> Yes Date: <input type="checkbox"/> No <input type="checkbox"/> NA (if employment began more than 5 years ago)	5. AA Justification Adequate <input type="checkbox"/> Yes <input type="checkbox"/> No Date: <input type="checkbox"/> NA	6. High-risk Program Status <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> HRP <input type="checkbox"/> 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 Disorders |
| Membership | Refusal to Testify |
| Overthrow of Government | Alcohol Consumption |
| Foreign Influence | Use of or Trafficking in Illegal Drugs |
| Falsification | Personal Conduct/Finance |

<p>13. Did the investigation report identify any new derogatory information? <input type="checkbox"/> Yes <input type="checkbox"/> 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:</p> <table border="0"> <tr> <td>Acts of Treason</td> <td>Violation of Security Requirements</td> </tr> <tr> <td>Association</td> <td>Emotional, Mental and Personality Disorders</td> </tr> <tr> <td>Membership</td> <td>Refusal to Testify</td> </tr> <tr> <td>Overthrow of Government</td> <td>Alcohol Consumption</td> </tr> <tr> <td>Foreign Influence</td> <td>Use of or Trafficking in Illegal Drugs</td> </tr> <tr> <td>Falsification</td> <td>Personal Conduct/Finance</td> </tr> </table>	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
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											

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	5. High-risk Program Status?	6. Pre-employment Check Documented?	7. AA Justification Adequate?	8. Date Unscreened Report Received	9. When Applicable, Date Report Screened by Site after Receipt of Data Call
				<input type="checkbox"/> Initial/Applicant <input type="checkbox"/> Incumbent <input type="checkbox"/> Reinstate <input type="checkbox"/> Other	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> HRP <input type="checkbox"/> SCI		<input type="checkbox"/> Yes/date: <input type="checkbox"/> No <input type="checkbox"/> NA (if employment began more than 5 years ago)		

10. Identification of Derogatory Information Contained in Unscreened Report

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

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

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

<input type="checkbox"/> Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:
<input type="checkbox"/> Criteria H, Emotional, Mental Disorders ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:
<input type="checkbox"/> Criteria I, Refusal to Testify ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:
<input type="checkbox"/> Criteria J, Alcohol Consumption ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:
<input type="checkbox"/> Criteria K, Use of or Trafficking in Illegal Drugs ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:
<input type="checkbox"/> Criteria L, Personal Conduct/Finances ↑ or ↓ ≤ 5 years or ≥ 5 years	<input type="checkbox"/> LOI <input type="checkbox"/> PSI <input type="checkbox"/> PE <input type="checkbox"/> CI <input type="checkbox"/> AR Date Recommended: Date Approved: Date Completed:	<input type="checkbox"/> G <input type="checkbox"/> C <input type="checkbox"/> R <input type="checkbox"/> N Date:

RESOLUTION METHODS: ACTION TAKEN:
 LOI: Letter of Interrogatory G: Grant
 PSI: Personnel Security Interview C: Continue
 PE: Psychiatric Evaluation S: Suspend
 CI: Counterintelligence Review R: Revoke
 AR: Administrative Review N: None/Pending

CLEARANCE JUSTIFICATION DATA COLLECTION FORM

NAME: _____ JOB TITLE: _____

WORK BUILDING NUMBER OR FACILITY DESIGNATION: _____

CURRENT DOE SECURITY CLEARANCE LEVEL: “Q” “L”

1. Approximately how long have you possessed a DOE security clearance?

a. less than 6 months:

b. 6 months to 1 year:

c. 1-3 years:

d. 3-5 years:

e. longer than 5 years:

2. Does your job require you to handle or use classified information?

a. Yes:

b. No:

If yes, how often and last time: _____

If a is checked above, please provide the following additional information by checking all boxes that apply.

Classification level of the information:

Top Secret Secret Confidential

Category of the classified information: Restricted Data NSI

Identify the **primary** location (building/facility) where you handle or use classified information: _____

3. Does your job require you to work with special nuclear material?

a. Yes:

b. No:

If yes, how often and last time _____

If a is checked above, please provide the following additional information by checking all boxes that apply.

Category of special nuclear material: Cat I Cat II Cat III Cat IV

Identify the **primary** location (building/facility) where you handled special nuclear material (SNM): _____

4. Does your work require you to access a limited, exclusion, protected or material access area?

a. Yes:

b. No:

If yes, how often and last time _____

5. Do you attend meetings or conferences that include the discussion of classified information?

a. Yes:

b. No:

If yes, how often and last time _____

If a is checked above, please provide the following additional information by checking all boxes that apply.

Level of the classified information: Top Secret Secret Confidential

Category(s) of the classified information: Restricted Data NSI

Identify the **primary** location (building/facility) where you attend a meeting, conference or participate in classified discussions _____.

Purpose of the meeting: _____

[After the conduct of this interview, complete a review of the last clearance justification/request (recording the results of the review on the table on next page of this guide) that is filed in the individual's personnel security file. The review is intended to determine if there is consistency between the actual work being performed and the clearance justification/request.]

DOE PERSONNEL SECURITY FILE REVIEW OF LATEST CLEARANCE JUSTIFICATION/REQUEST
Name: _____ Contract Number: _____
Last Clearance Justification/Request Date: _____
Clearance Level Requested: <input type="checkbox"/> "Q" <input type="checkbox"/> "L"
Requested Clearance Justification Based On Access To: Protected Area: <input type="checkbox"/> Yes <input type="checkbox"/> No Material Access Area: <input type="checkbox"/> Yes <input type="checkbox"/> No SNM: <input type="checkbox"/> Yes <input type="checkbox"/> No Highest Category: <input type="checkbox"/> Cat I <input type="checkbox"/> Cat II <input type="checkbox"/> Cat III <input type="checkbox"/> Cat IV Limited Area: <input type="checkbox"/> Yes <input type="checkbox"/> No Exclusion Area: <input type="checkbox"/> Yes <input type="checkbox"/> No Classified Information: <input type="checkbox"/> Yes <input type="checkbox"/> No Highest Level: <input type="checkbox"/> TS <input type="checkbox"/> S <input type="checkbox"/> C Category(s): <input type="checkbox"/> RD <input type="checkbox"/> FRD <input type="checkbox"/> NSI

HRP FILE REVIEW DATA COLLECTION FORM

Name/Duty Position:

File ID:

**Temp Removal/Reinstate Date(s) from Data Call:
Disciplinary Action Date(s):**

PSYCH	MEDICAL	HRP
Date(s) of Last Assessment: Initial <input type="checkbox"/> Re-cert <input type="checkbox"/> Evidence of access to JTA? <input type="checkbox"/> Yes <input type="checkbox"/> No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info) Sec. Concerns? Date Reported?	Date(s) of Last Assessment: Initial <input type="checkbox"/> Re-cert <input type="checkbox"/> Evidence of access to JTA? <input type="checkbox"/> Yes <input type="checkbox"/> No Evidence of Psych Integration? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> NA Current Prescription Medications noted? <input type="checkbox"/> Yes <input type="checkbox"/> No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info) Sec. Concerns? Date Reported?	Data from Current and Last Prior DOE Form 470.3: Current Certification Date: (should be within 12 months of each other) Last Prior Certification Date: Current Drug & Alcohol (D&A) Test Date: (should be within 12 months of each other) Last Prior D&A Test Date: Current Training Date: (should be within 12 months of each other) Last Prior Training Data: Is Section B always signed after the medical and psychological evaluations? <input type="checkbox"/> Yes <input type="checkbox"/> No Is Section C always signed after drug and alcohol testing? <input type="checkbox"/> Yes <input type="checkbox"/> No Reported Restrictions/Removals?(dates/info) Notifications made: Unreported Restrictions/Removals?(dates/info)

(OFFICIAL USE ONLY WHEN FILLED IN)

HRP BREATH ALCOHOL TEST CHECKLIST

In accordance with Department of Transportation (DOT) 49 CFR Part 40

Name: _____

- | | | |
|----------|-----------------|-------------|
| 1. _____ | Location: _____ | Date: _____ |
| 2. _____ | Location: _____ | Date: _____ |
| 3. _____ | Location: _____ | Date: _____ |

EQUIPMENT AND CHECKS

1. Does the device used for testing meet the DOT requirements? Yes|_|_|_|_| No|_|_|_|_|

(Does the technician know that evidential grade breath alcohol testing (EBT) devices as listed **without** "*" on the conforming products list of evidential breath measurement devices.)

2. Does the BAT/STT training certificate, showing the EBT device they are qualified to operate, match the EBT they are operating? [40.213(b)(2)] Yes|_|_|_|_| No|_|_|_|_|

They must have a certificate for each EBT they operate including the back-up device if they have one.

3. Do they have a Quality Assurance Plan (QAP) for the EBT device? [40.233(a)] Yes|_|_|_|_| No|_|_|_|_|
Does not know|_|_|_|_|

(Before the EBT device can be placed on the conforming products list, the manufacturer of the EBT device must submit a QAP to the NHTSA for approval.)

4. Does the BAT/STT perform external calibration checks at the specified intervals required in the QAP? [40.233.(c)] Yes|_|_|_|_| No|_|_|_|_|
Does not know|_|_|_|_|

(The QAP specifies the intervals that the external calibration checks must be completed and the tolerance levels.)

Note the QAP will specify a tolerance level between the external calibration checks performed and the test standard. If the external calibration check produces a result that differs by more than the tolerance stated in the QAP from the known value of the test standard, every **test result at 0.02 or above** obtained on the EBT since the last **valid** external calibration check is cancelled [40.267(c)(5)].

- Does the BAT/STT have records of the calibration checks? Yes|_|_|_|_| No|_|_|_|_|

[Review documentation - 40.233.(c)(4) requires that records be maintained of the inspection, maintenance, and calibration of the EBTs]

- Does the BAT/STT understand that if the external calibration check produces a result that differs more than the tolerance specified in the QAP from the known value of the test standard that every test of 0.02 or above obtained on the EBT since the last valid external calibration check is cancelled? [40.267(c)(5)] Yes|_|_|_|_| No|_|_|_|_|

5. Does the BAT/STT know what two regulations govern HRP breath alcohol testing?
(10 CFR 712 HRP and DOT 49 CFR, Part 40) Yes|_|_|_|_| No|_|_|_|_|

TESTING PROCESS

6. Does the BAT/STT verify the employee through positive identification?
[40.241(c)] Yes|_|_|_|_| No|_|_|_|_|

7. Does the BAT/STT explain the process and completes DOE ATF Step 1?
[40.241(e) & (f)] Yes|_|_|_|_| No|_|_|_|_|

8. Does the employee complete ATF Step 2 and sign certification statement?
[40.241(g)] Yes|_|_|_|_| No|_|_|_|_|

Does the technician know that it is considered a refusal to test if the employee refuses to sign step 2 prior to the test? [40.241(2)(g)] Yes|_|_|_|_| No|_|_|_|_|

9. Does the BAT/STT unwrap and install a fresh mouthpiece with each test?
[40.243.(b)] Yes|_|_|_|_| No|_|_|_|_|

Note: employee may select their own mouthpiece, but they cannot install it on the EBT device.

10. Does the BAT/STT instruct the employee to continue blowing until device or operator signals to stop? (6 sec) [40.243(c)] Yes|_|_|_|_| No|_|_|_|_|

Does the BAT/STT know that they can allow an employee 3 attempts to provide adequate breath for the test? [10 CFR 712.15(c)(3)(ii)] Yes|_|_|_|_| No|_|_|_|_|

11. Does the BAT/STT show the test result to the employee? [40.243(c)] Yes|_|_|_|_| No|_|_|_|_|

12. Does the BAT/STT verify that the test # and time have printed correctly?
[40.243(e)-(g)] Yes|_|_|_|_| No|_|_|_|_|

[Three options for the BATT/STT: print directly onto the ATF; print to a separate report affixed to the ATF; or enter in Step 3 of the ATF.]

13. If the test result is less than 0.02, are these steps then taken by the BAT/STT? [40.247(a)(1)-(2)]

Circles "BAT" and "breath" at top of Step 3 on ATF Yes|_|_|_|_| No|_|_|_|_|

Signs and dates bottom of Step 3 on ATF Yes|_|_|_|_| No|_|_|_|_|

Transmits ATF original, gives a copy to the employee, and retains a copy Yes|_|_|_|_| No|_|_|_|_|

14. Are the requirements for privacy (visual and aural) met? [40-221(c)] Yes|_|_|_|_| No|_|_|_|_|

Was anyone else besides, the donor, the technician and you the DOE agency representative, allowed to observe the testing? [40.223(b)] Yes|_|_|_| No|_|_|_|

Is the technician aware that when performing a test due to reasonable suspicion or following an accident that must be conducted at the scene, that not all facility requirements have to be met? [40.221(e)] Yes|_|_|_| No|_|_|_|

15. Does the BAT/STT attach the test results and any confirmation test results to side or back of the ATF with tamper evident tape? (unless printed directly on form) [40.243(f)] Yes|_|_|_| No|_|_|_|

16. Is a list of fatal flaws readily available to the BAT/STT? Yes|_|_|_| No|_|_|_|
(Not a DOT requirement, just a good business practice)

17. Are there two EBTs available for use? [40.221(d)] Yes|_|_|_| No|_|_|_|
(This is in case the EBT normally used breaks down)

Are they kept under lock and key when not in use? [40.223(c)] Yes|_|_|_| No|_|_|_|

ACTIONS FOLLOWING A POSITIVE ALCOHOL TEST

Waiting period

18. Does the BAT/STT instruct the donor that a waiting period of at least 15 minutes is required? (40.251.(a)(1)) Yes|_|_|_| No|_|_|_|

Does the BAT/STT understand that if the confirmatory test begins prior to the 15 minute waiting period they must cancel the test? [40.267(c)(1)] Yes|_|_|_| No|_|_|_|

Does the BAT/STT understand that if they make a mistake that causes a test to be cancelled, they must undergo error correction training? [40-213(f)] Yes|_|_|_| No|_|_|_|

19. Does the BAT/STT inform the donor of the following?

During the waiting period they cannot put anything into their mouth or belch. [40.251.(a)(2)(i)] Yes|_|_|_| No|_|_|_|

The reason for the waiting period (to prevent an accumulation of mouth alcohol from leading to an artificially high reading). [40.251.(a)(2)(ii)] Yes|_|_|_| No|_|_|_|

That following the instructions concerning the waiting period is to the employee's benefit. [40.251(a)(2)(iii)] Yes|_|_|_| No|_|_|_|

That the confirmation test will be conducted at the end of the waiting period, even if the instructions have not been followed. [40.251(a)(2)(iv)] Yes|_|_|_| No|_|_|_|

20. Is the donor observed by the BAT/STT or another employee throughout the entire waiting period? [40.251(a)(1)(iii)] Yes|_|_|_| No|_|_|_|

Conduct of confirmation test

21. Does the BAT/STT conduct an air blank in the presence of the employee and show the employee the reading? [40.253(a)] Yes|_|_|_| No|_|_|_|
22. Does the BAT/STT open a new individually wrapped mouthpiece in view of the employee and insert it into the device? [40.253(b)] Yes|_|_|_| No|_|_|_|
23. Does the BAT/STT ensure that the employee reads the unique test number displayed on the device? [40.253(c)] Yes|_|_|_| No|_|_|_|
24. Does the BAT/STT instruct the employee to blow steadily and forcefully into the mouthpiece for at least 6 seconds or until the device indicates that an adequate amount of breath has been obtained? [40.253(d)] Yes|_|_|_| No|_|_|_|
25. Does the BAT/STT show the employee the result displayed on the device? [40.253(e)] Yes|_|_|_| No|_|_|_|
26. Does the BAT/STT show the employee the result and unique test number that the device prints out either directly onto the ATF or onto a separate printout? [40.253(f)] Yes|_|_|_| No|_|_|_|
27. If the device does not print the result directly onto the ATF, but on a separate printout, does the BAT/STT attach the printout to the designated space on the ATF with tamper-evident tape, or use a self-adhesive label that is tamper evident? [40.253(g)] Yes|_|_|_| No|_|_|_|

Actions following the confirmation test

28. Does the BAT/STT sign and date Step 3 of the ATF? [40.255(a)(1)] Yes|_|_|_| No|_|_|_|
29. If the confirmation test was positive, does the BAT/STT direct the employee to sign and date Step 4 of the ATF? [40.255(a)(3)] Yes|_|_|_| No|_|_|_|
30. Does the BAT/STT immediately inform the HRP MO of the result in a confidential manner? (40.255(a)(5)) Yes|_|_|_| No|_|_|_|
31. Have the BAT/STT and the HRP Management Official established a mechanism to ensure if the result is provided by phone that the identity of the BAT is established? [40.255(b)(1)] Yes|_|_|_| No|_|_|_|
32. Are the results of all breath tests stored in a way that protects the confidentiality of the employee? [40.255(b)(2)] Yes|_|_|_| No|_|_|_|

HRP DRUG TEST CHECKLIST

In accordance with Department of Health and Human Services (DHHS) Mandatory Guidelines

Name: _____

1. _____	Location: _____	Date: _____
2. _____	Location: _____	Date: _____
3. _____	Location: _____	Date: _____

1. Does the collector know the two regulations that govern the collection of urine samples? (10 CFR 707 and DHHS Mandatory Guidelines) Yes|_____| No|_____|
2. Has the collector received training from a qualified trainer?[4.3(a)] Yes|_____| No|_____|
 Does the collector have documentation of the training? [4.3(c)] Yes|_____| No|_____|
 If appropriate has the collector received refresher training 5 years from the date of the last training? [4.3(b)] Yes|_____| No|_____|

NOTE: a collector cannot collect urine specimens until his or her training has been properly documented

3. Does the collector understand that collection begins without delay even if a donor states he/she is not ready or is unable to urinate? [8.3(b) and 8.5(a) and (b)] Yes|_____| No|_____|
4. Does the collector understand that if the donor refuses to cooperate, he/she will be treated as if he/she had a positive test? [707.12(b)(1)] Yes|_____| No|_____|
5. Is there a bluing agent in the toilet?[8.2(a)] Yes|_____| No|_____|
6. Is there any other source of water in urination area? [8.2(b)] Yes|_____| No|_____|
7. Are there any soaps, cleaners, or other chemicals in the urination area? [8.3(i)] Yes|_____| No|_____|
8. Was a photo ID presented by the donor? [8.3(c)] Yes|_____| No|_____|
 Does the collector understand that if the employee cannot present photo ID that the collector must contact the donor’s supervisor or agency rep.? [8.3(c)] Yes|_____| No|_____|
 Does the collector understand that if the employee’s identity cannot be established, the collector cannot proceed with the collection? [8.3(c)] Yes|_____| No|_____|
 Does the collector understand that if the donor asks for ID that the collector must provide it? [8.3(d)] Yes|_____| No|_____|

9. Did the collector determine whether the donor arrived within 2 hours?
[712.15(b)] Yes|_|_|_|_| No|_|_|_|_|
(Determine how this is documented)
- Does the collector understand that if the donor does not arrive within 2 hours, it must be considered a refusal to test? **[1.7(a)(1)]** Yes|_|_|_|_| No|_|_|_|_|
10. Does the collector understand how a refusal to test must be documented on the CCF?
[1.7(d)(1)] Yes|_|_|_|_| No|_|_|_|_|
11. Is the donor asked to remove unnecessary outer garments? **[8.3(h)]** Yes|_|_|_|_| No|_|_|_|_|
12. Is the donor asked to empty pockets and/or contents checked?
[8.3(h)(2)] Yes|_|_|_|_| No|_|_|_|_|
- Does the collector know that if something is found that could be used to dilute or adulterate the specimen that a test under direct observation must be completed?
[8.3(h)(4)] Yes|_|_|_|_| No|_|_|_|_|
- Does the collector understand that if the donor refuses to show the collector the items in his/her pockets, that it is considered a refusal to test and that the test is then considered a positive test?
[8.3(h)(5) and 707.12(b)(1)] Yes|_|_|_|_| No|_|_|_|_|
13. Do purses/briefcases remains with outer garments? **[8.3(h)(1)]** Yes|_|_|_|_| No|_|_|_|_|
14. Is the donor instructed to wash/dry hands prior to urination? **[8.3(i)]** Yes|_|_|_|_| No|_|_|_|_|
15. After washing hands, does the donor remain in the presence of the collection site person and does not have access to any water fountain, faucet, soap dispenser, cleaning agent or any other materials, which may used to adulterate the specimen? **[(8.3(i)]** Yes|_|_|_|_| No|_|_|_|_|
16. Is a new specimen collection container is provided to donor? **[8.4(a)]** Yes|_|_|_|_| No|_|_|_|_|
- Does the collector understand that the donor can select his/her own specimen container?
[8.4(a)] Yes|_|_|_|_| No|_|_|_|_|
17. Does the collector understand what steps must be taken if a donor is unable to provide a specimen?
(8.5) Yes|_|_|_|_| No|_|_|_|_|
- The donor must enter the stall and attempt to provide a specimen (before a determination can be made that he/she cannot provide a specimen).
 - The donor demonstrates his/her inability to provide a specimen when he/she comes out of the stall with an empty collection container.
 - An 8 oz. glass of water every 30 minutes not to exceed 40 ounces over a 3 hour period can be given until the donor can provide a specimen. (If the donor simply needs more time to urinate, drinking water is not required.)
 - If the donor states he/she cannot provide a urine specimen, the collector records the reason on the CCF, notifies the designated representative and sends copies of the CCF to the MRO.

18. Following urination and receipt of specimen, does the collection site person determine the temperature (**must be done within 4 minutes**) and volume (45 ml) of urine in the container?
[8.6(c) and (e)(1)] Yes|_|_|_| No|_|_|_|

19. Does the collector understand what steps are taken if the donor has provided a specimen that is less than 45 ml? [8.6(e)(2)(i-iii)] Yes|_|_|_| No|_|_|_|

If less than 45 ml and if temp is in acceptable range (90-100 degrees), the specimen is discarded and a second specimen is collected. Donor is given a reasonable amount of liquid (8 oz. glass of water every 30 min - not to exceed 40 oz. over a period of 3 hours). If donor fails for any reason to provide 45 ml of urine for the second collection **after 3 hours from the unsuccessful attempt**, the collector:

- Stops the collection procedure
- Notifies the HRP management official
- Discards the insufficient amount
- Requests the donor to leave the collection site
- Sends the appropriate copies of the CCF to the MRO and HRP Management Official

NOTE: Whenever a donor is unable to provide a sufficient amount of urine, a medical examination must be performed to determine if a medical condition exists. (See 13.3(d)) If none exists, it should be determined a lack of cooperation or a refusal to test under 10 CFR 707.12(b)(2) and 13.5(c)(2).

20. Does the collector understand that if the temp is outside the acceptable range, a second specimen shall be collected under direct observation (acceptable range: 32-38 degrees C or 90-100 degrees F)?
[8.6(c)(2)] Yes|_|_|_| No|_|_|_|

Does the collector understand that both the specimens must be forwarded for analysis?
[8.6(c)(2)] Yes|_|_|_| No|_|_|_|

21. After a good specimen has been provided and submitted, is the donor instructed to wash his/her hands?
[8.6(b)] Yes|_|_|_| No|_|_|_|

22. Do the donor and the collector keep the specimen bottle in view at all times prior to it being sealed and labeled? (8.7(a)-(c)) Yes|_|_|_| No|_|_|_|

23. Does the collection site person securely place a tamper-evident seal/label on the specimen bottle with the date? [8.7(c)] Yes|_|_|_| No|_|_|_|

24. Does the donor initial the tamper-evident seal/label on the specimen bottle?
[8.7(d)] Yes|_|_|_| No|_|_|_|

25. Is the donor asked to read and sign a statement on the CCF certifying the specimens identified were collected from him or her? [8.7(e)] Yes|_|_|_| No|_|_|_|

Does the collector understand that if the donor refuses to sign this statement that the refusal must be documented on the CCF? **[8.7(e)]** Yes|_|_|_| No|_|_|_|

26. Does the collector ensure that the required information is entered on the Federal chain of custody form? **[8.7(f)]** Yes|_|_|_| No|_|_|_|

27. Does the collector seal the specimens (bottle A and bottle B) and CCF in a package as specified on the CCF? **[8.7(g)]** Yes|_|_|_| No|_|_|_|

Does the collector understand that any urine collected in excess of 45 ml must be discarded and no further testing can be performed on the excess urine? **[8.7(i)]** Yes|_|_|_| No|_|_|_|

DATA COLLECTION FORM AND INSTRUCTIONS

Preparation of a data collection form (DCF) may/will begin while various subtopic data collection activities are ongoing. An **INTERIM** DCF may be turned in to the writer with one or more elements of the DCF incomplete with appropriate statements about follow-up activities or additional data collection activities. An example of a DCF is provided below.

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.

(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, etc.), 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 subtopic processes; for example, FV&A request process, or HRP certification process)

-(next major subtopic 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.
2. (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-headings 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 the data collection sheet(s). On 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 HRP, SSAP, and FV&A will be collected the first week of the data collection phase. The principal writer will complete data collection for the subtopic 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.

Onsite Planning Phase

- 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

Onsite Data Collection Phase

- 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, along with conclusions on the 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: Finalize 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 Quality Review Board.

This page intentionally left blank.