PERSONNEL SECURITY
Assessment Guide
December 2016

Office of Cyber and Security Assessments
Office of Enterprise Assessments
U.S. Department of Energy
# Personnel Security Assessment Guide

December 2016

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronyms</td>
<td>PS-1</td>
</tr>
<tr>
<td>Section 1: Introduction</td>
<td>PS-2</td>
</tr>
<tr>
<td>Section 2: Management</td>
<td>PS-8</td>
</tr>
<tr>
<td>Section 3: Personnel Security Clearance Program</td>
<td>PS-14</td>
</tr>
<tr>
<td>Section 4: Human Reliability Program</td>
<td>PS-25</td>
</tr>
<tr>
<td>Section 5: Foreign Visits and Assignments Program</td>
<td>PS-32</td>
</tr>
<tr>
<td>Section 6: Safeguards and Security Awareness Program</td>
<td>PS-36</td>
</tr>
<tr>
<td>Section 7: Interfaces</td>
<td>PS-43</td>
</tr>
<tr>
<td>Section 8: Analyzing Data and Interpreting Results</td>
<td>PS-46</td>
</tr>
<tr>
<td>Appendix A: Data Collection and Analysis Tools</td>
<td>PS-49</td>
</tr>
</tbody>
</table>

## Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Access Authorization</td>
</tr>
<tr>
<td>AR</td>
<td>Administrative Review</td>
</tr>
<tr>
<td>ATF</td>
<td>Alcohol Testing Form</td>
</tr>
<tr>
<td>BAT</td>
<td>Breath Alcohol Technician</td>
</tr>
<tr>
<td>BI</td>
<td>Background Investigation</td>
</tr>
<tr>
<td>CES</td>
<td>Case Evaluation Sheet</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>CI</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>CMPC</td>
<td>Classified Matter Protection and Control</td>
</tr>
<tr>
<td>CPCI</td>
<td>Central Personnel Clearance Index</td>
</tr>
<tr>
<td>D&amp;A</td>
<td>Drug and Alcohol</td>
</tr>
<tr>
<td>DCF</td>
<td>Data Collection Form</td>
</tr>
<tr>
<td>DHHS</td>
<td>Department of Health and Human Services</td>
</tr>
<tr>
<td>DOE</td>
<td>U.S. Department of Energy</td>
</tr>
<tr>
<td>DOT</td>
<td>Department of Transportation</td>
</tr>
<tr>
<td>EA-20</td>
<td>Office of Cyber and Security Assessments</td>
</tr>
<tr>
<td>EA-22</td>
<td>Office of Security Assessments</td>
</tr>
<tr>
<td>EBT</td>
<td>Evidential Breath Testing</td>
</tr>
<tr>
<td>eQIP</td>
<td>Electronic Questionnaire for Investigation</td>
</tr>
<tr>
<td>FACTS</td>
<td>Foreign Access Central Tracking System</td>
</tr>
<tr>
<td>FV&amp;A</td>
<td>Foreign Visit and Assignment</td>
</tr>
<tr>
<td>HRP</td>
<td>Human Reliability Program</td>
</tr>
<tr>
<td>IRTPA</td>
<td>Intelligence Reform and Terrorism Prevention Act</td>
</tr>
<tr>
<td>JTA</td>
<td>Job Task Analysis</td>
</tr>
<tr>
<td>KMP</td>
<td>Key Management Personnel</td>
</tr>
<tr>
<td>LA</td>
<td>Limited Area</td>
</tr>
<tr>
<td>LOI</td>
<td>Letter of Interrogatory</td>
</tr>
<tr>
<td>MAA</td>
<td>Material Access Area</td>
</tr>
<tr>
<td>MRO</td>
<td>Medical Review Officer</td>
</tr>
<tr>
<td>NNSA</td>
<td>National Nuclear Security Administration</td>
</tr>
<tr>
<td>NSI</td>
<td>National Security Information</td>
</tr>
<tr>
<td>OGA</td>
<td>Other Government Agency</td>
</tr>
<tr>
<td>OPM</td>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>OPSEC</td>
<td>Operations Security</td>
</tr>
<tr>
<td>PA</td>
<td>Protected Area</td>
</tr>
<tr>
<td>PE</td>
<td>Psychiatric Evaluation</td>
</tr>
<tr>
<td>PPA</td>
<td>Property Protection Area</td>
</tr>
<tr>
<td>PPM</td>
<td>Protection Program Management</td>
</tr>
<tr>
<td>PSC</td>
<td>Personnel Security Clearance</td>
</tr>
<tr>
<td>PSF</td>
<td>Personnel Security File</td>
</tr>
<tr>
<td>PSI</td>
<td>Personnel Security Interview</td>
</tr>
<tr>
<td>RD</td>
<td>Restricted Data</td>
</tr>
<tr>
<td>SCI</td>
<td>Sensitive Compartmented Information</td>
</tr>
<tr>
<td>SF</td>
<td>Standard Form</td>
</tr>
<tr>
<td>SNM</td>
<td>Special Nuclear Material</td>
</tr>
<tr>
<td>SOMD</td>
<td>Site Occupational Medical Director</td>
</tr>
<tr>
<td>SSAP</td>
<td>Safeguards and Security Awareness Program</td>
</tr>
<tr>
<td>SSP</td>
<td>Site Security Plan</td>
</tr>
<tr>
<td>SSSP</td>
<td>Site Safeguards and Security Plan</td>
</tr>
<tr>
<td>STS</td>
<td>Security Termination Statement</td>
</tr>
<tr>
<td>STT</td>
<td>Screening Test Technician</td>
</tr>
</tbody>
</table>
Section 1: Introduction

Purpose

The Office of Security Assessments (EA-22) Personnel Security Assessment Guide provides assessors with information, guidelines, references, and a set of assessment tools that can be used to plan, conduct, and close out an assessment of personnel security. The guide is designed to promote consistency, ensure thoroughness, and enhance the quality of the assessment process.

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

Office of Enterprise Assessments (EA) protocols provide additional, non-topic-specific information pertaining to the assessment process.

General Considerations

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

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

A significant consideration in developing assessment guides is to provide a repository for the collective knowledge of EA-22’s assessors that can be enhanced and updated as assessment methods improve and EA-22 assessor experience accumulates. Every attempt has been made to develop specific guidelines that offer maximum utility to both novice and experienced assessors. In addition to guidelines for collecting information, the assessment 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 assessment-specific basis, taking into account site-specific factors.

Characterization of the Personnel Security Topic

Historically, EA-22 has included the personnel security clearance (PSC) program, human reliability program (HRP), safeguards and security awareness program (SSAP), and foreign visits and assignments (FV&A) program in the characterization of the personnel security topic.

While these four programs fall under different program managers, all the programs were included because of a similar purpose: 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. Further, each of these programs contains requirements
that are intended to ensure continuing awareness of security responsibilities among program officials and DOE/NNSA employees, contractors, and consultants. Lastly, these programs have a close relationship to national and DOE insider threat mitigation program objectives and aid in meeting insider threat program requirements.

Appendix A, Data Collection and Analysis Tools, includes a baseline list of direct and indirect contractor personnel security program elements; a table of personnel security program direct elements, justifications, and primary data collection activities; and a table of personnel security program lines of inquiry. Referring to the baseline list and the two tables will help assessors maintain a consistent focus on the personnel security program elements most important to protecting National Security Information (NSI), Restricted Data (RD), and SNM, as well as mitigating the insider threat.

Organization of This Guide

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 assessment tools and their use.

Sections 2 through 6 provide detailed guidance for assessing each major personnel security subtopic:

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

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

Section 7 (Interfaces) provides guidelines to help assessors coordinate their activities both within the personnel security topic team and with other topic teams. Typically, the team reviewing personnel security coordinates with the teams reviewing physical security systems, information security, cyber security, protection program management (PPM), and protective force programs. Section 7 emphasizes techniques that assessors can use to improve data collection by coordinating with other teams and identifies data that assessors on other teams can collect that may be relevant to personnel security. The personnel security team should review and conduct the listed interface activities during the planning phase to ensure that all critical elements are covered and that efforts are not duplicated unnecessarily.

Section 8 (Analyzing Data and Interpreting Results) contains guidelines on how to organize and analyze information gathered during data collection activities. These guidelines incorporate statements on the relative significance of potential deficiencies, as well as suggestions for conducting additional activities when these deficiencies are identified. After completing each activity, assessors 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 assessors during data collection.

Organization within Each Subtopic

Sections 2 through 6 provide topic-specific information intended to help assessors prepare for and conduct an assessment. The information is organized by subtopic and further by sub-element:
• Management: Typically management is responsible for the overall personnel security program through planning, training, and providing necessary resources. The degree of protection a personnel security program affords is usually determined by the degree of support received from management.

• Personnel security clearance program: By determining and verifying the eligibility of individuals for access to classified matter and SNM, the PSC program addresses appropriate contractor and Federal organization’s security clearance requirements including general requirements; pre-employment checks; reporting; security clearance suspension, revocation, and denial; classified visits; training; records maintenance; screening and adjudication of cases; and re-investigations.

• Human reliability program: The HRP is designed to ensure that individuals who have 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.

• Foreign visits and assignments program: The FV&A program is concerned with the proper approval and control of foreign visitors to DOE facilities.

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

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 assessed program and identifying findings. Because of periodic changes in policy, assessors should 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 identifies memoranda from DOE Headquarters to clarify or revise the policies and standards defined in DOE orders and other guidance. Assessors must be aware of these clarifications and revisions, since assessment objectives include verifying compliance with DOE directives. New memoranda are continually being issued; assessors should determine whether they apply specifically to the assessed 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 assessors focus on the unique features and problems associated with protecting and assessing 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 EA-22 has encountered on previous assessments and includes a short discussion detailing each potential deficiency. The identified deficiencies are not necessarily evident at every facility, but have been noted often enough to warrant special attention during assessments. Where appropriate, this guide provides general direction to help the assessor 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 assessor further focus the assessment efforts. By reviewing the section before collecting data, assessors can be alerted to commonly identified deficiencies and potential concerns that may exist at the assessed facility.

Planning Activities

The Planning Activities section identifies activities normally conducted by the personnel security topic team during the planning phase of an assessment, including pre-planning, review of documents and materials, and interviews with representatives of the facility to be assessed. 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 assessors in planning assessment activities, Appendix A includes a detailed assessment 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 relevant to all the elements of the personnel security topic and help define the scope of assessment 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 that define all property protection areas (PPAs), Limited Areas (LAs), Protected Areas (PAs), or material access areas (MAAs).

Data Collection Activities

This section identifies activities assessors may choose to perform during data collection. The information is intended to be reasonably comprehensive; however, not every conceivable variation can be addressed here. Typically, the activities are selected during the planning effort and organized by functional element or by the type of system used to provide protection. The Data Collection Activities section includes activities most often conducted, reflecting as much previous EA-22 data collection experience and expertise as possible. Activities include tours, interviews, observations, and performance tests, although assessors do not normally perform every activity on every assessment. Activities are identified by an alphabetical letter for easy reference and assignment of data collection tasks. Assessors 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 assessment. EA-22 assessors must verify the accuracy of the information obtained during data collection activities. The process for performing validations of assessment results with site representatives is discussed in detail in EA protocols, including a discussion of on-the-spot validations, daily validations, and summary validations.
Assessors should ensure that they are validating facts, conclusions, and impact, not their own conjectures. Facts (data points) noted during the assessment of the personnel security program should be validated with representatives of the assessed facility as they become apparent (on-the-spot), if representatives accompany the assessment team. When representatives do not accompany the assessment team, the data points should be validated during daily validation meetings with site personnel.

Validation becomes more difficult when personnel security assessment team members must separate and work independently 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, team members must make a particular effort to coordinate and share information in a timely manner, and validation becomes even more important, not only for team members but also for site representatives who may have also been separated as they accompanied EA-22 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 the facts reconfirmed during the daily and summary validations.

Using the Tools in Each Assessment Phase

The assessment tools should be used throughout all assessment phases. The following enumerates some of the tools usually considered during each assessment phase.

In the planning stage, assessors:

- Use the General Information section to characterize the program and focus the assessment.
- Perform the activities identified under Planning Activities to collect the information necessary to further characterize the program and focus the assessment. Thorough planning for an assessment cannot be overemphasized.
- Review Common Deficiencies/Potential Concerns to determine whether any 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 assessors (or small teams of assessors) by selecting specific items from the Data Collection Activities section. The assignments should be made to optimize efficiency and ensure that all high-priority activities are accomplished. The guidelines under the Interfaces section should be considered when assigning tasks to ensure that efforts are not duplicated.
- Schedule data collection activities to optimize efficiency by ensuring that high-priority activities are conducted early in the process.
- Review the referenced DOE orders and memoranda to ensure that they are current.

In the conduct phase, assessors:

- 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 common deficiencies are apparent at the facility. If so, assessors should determine what 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 is needed to evaluate the program.

In the closure phase, assessors:

• 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 consider the potential impacts of identified deficiencies.

In the follow-up phase, assessors:

• 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.
Section 2: Management

References

DOE Order 470.4B, Admin Chg 1, Safeguards and Security Program  
DOE Order 470.5, Insider Threat Program  
DOE Order 472.2, Change 1, Personnel Security  
DOE Order 142.3A, 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 protecting 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 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 certain elements of protection systems. Further, insiders may have extensive knowledge of an assessed 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, management must recognize the significance of an effective personnel security program. Coupled with HRP participation for 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 flawed.

Effective security planning can make the difference between a weak and a strong protection program. Management must 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. 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 facilities where a SSSP is not required, planning and budgeting for the personnel security program must be formally documented in a site security plan (SSP).

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 performing critical personnel security tasks should be trained.
properly. Staffing and training are especially important because personnel security organizations are frequently tasked with performing 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, including the clearance process and the SSAP, which are discussed in detail in subsequent sections.

**Common Deficiencies/Potential Concerns**

**Individual Responsibility and Participation**

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

**Incidents of Security Concern.** Similarly, DOE/NNSA organizations that experience recurring incidents of security concern probably have deficient SSAPs. Although not the only measure of program effectiveness, causal analysis of these incidents often indicates either that individuals do not understand their safeguards and security responsibilities or that awareness briefings do not effectively communicate 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. These programs can better control approved foreign visitors and assignees, but if employees fail to utilize these programs and host a foreign visitor prior to or without formal approval, facility managers assume the unanalyzed and unmitigated risks. Employees must realize that they are the most important link in mitigating the risk foreign national visitors pose.

**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. Management must 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 – that is, 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 enrolled properly or removed expeditiously from the 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 guaranteed.
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 security awareness briefings, improper badging of approved foreign visitors, and foreign visits that take place without formal approval). When an accumulation of deficiencies exists, and the results of interviews with personnel security professionals indicate that they are unable to accomplish their assigned tasks due to overload, additional management commitment and support are likely needed. Many personnel security specialists are assigned secondary duties and thus have insufficient time to dedicate to 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, training personnel security staff in analyzing derogatory information and conducting interviews is key to the proper application of the criteria (10 CFR 710) for the adjudication of cases containing derogatory information and, when necessary, the preparation of cases for administrative review. Additionally, the lack of proper host and escort training can lead to unauthorized disclosure of sensitive information or classified matter.

Although assessors must determine whether deficiencies in the personnel security program result from a lack of personnel or poor utilization of existing staff, deficiencies are usually found when personnel security functions are assigned to untrained and/or inexperienced people.

Identification of Safeguards and Security 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 SSPs for other facilities). During planning, managers must consider how changes impact the PSC and FV&A programs 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, relying instead 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 naturally focus on elements of the personnel security program 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 of program inefficiencies may remain unidentified.

Inadequate Surveys. Organizations responsible for conducting surveys rarely have sufficient staff to perform comprehensive evaluations of the personnel security program. In such cases, surveys often lack the necessary scope and fail to evaluate all the critical elements of the personnel security program. Operations offices and Headquarters elements conducting surveys must take appropriate 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 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 uncorrected deficiencies. 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 slippages can be identified early and progress monitored effectively; 3) assign responsibility for completion to specific organizations and individuals; 4) modify the plan as known deficiencies are corrected and new ones identified; and 5) ensure that adequate resources are applied to correct deficiencies. Frequently, facility managers devote their resources to correcting the most recently identified deficiency instead of the most serious, and correcting symptoms rather than the root causes of systemic deficiencies.

No Root Cause Analysis of Deficiencies. Another potentially serious management shortcoming is the failure of organizations to determine the underlying causes of deficiencies, usually resulting 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. A root cause analysis must be performed to reveal the underlying cause of errors (e.g., ambiguous procedures or insufficient training). Management must accurately perform a root cause analysis of identified deficiencies to prevent similar deficiencies from reoccurring.

Planning Activities

- Review standard operating procedures to determine whether 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 in a manner that ensures efficiency without negatively impacting 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.

- Review training records to determine whether personnel security program staff have had the opportunity to attend personnel security courses at the National Training Center or at other government agency (OGA) training facilities.

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

- Determine whether the site contractor has established a program of reviews designed to periodically validate the need for security clearances held by contractor and Federal employees.

- Review the results of recent feedback activities (for example, surveys and self-assessments) to determine whether they produce comprehensive evaluations of the personnel security program, and review applicable corrective action plans to determine whether program deficiencies are 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 supports an effective protection program. To help make this determination, performance testing should be conducted during the assessment in each of the subtopical elements of the personnel security topic, discussed in Sections 3 through 6.

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

A. Interviews with managers, supervisors, and personnel security professionals help determine the extent of personnel security involvement in the overall security activity. Interviews may indicate the extent to which personnel security professionals participate in meetings, budget discussions, and management-level decisions. Typically, interviews reveal whether supervisors are aware of staff concerns, daily staff activities, workflow bottlenecks, and other personnel security issues. Interviews help assessors determine the level of managers’ and supervisors’ understanding of personnel security’s impact 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, assessors can gain insight into whether adequate resources are devoted to the program by determining:

- The extent of backlogged requests for clearances, screening investigation reports, additional adjudicative actions, and HRP enrollment and re-certifications
- The extent of temporary or short-term use of overtime or other resources to assist in the reduction of backlogs
- The PSC organization’s ability to effectively respond to “surge” situations.

Competence Commensurate With Responsibilities

C. Assessors must determine how well the personnel security program staff are trained. When necessary, supervisors and staff should be interviewed to determine the reason why training provided by the National Training Center was unavailable for the staff. Effectively implementing the personnel security program sub-elements indicates how well the staff has been trained.

D. When a formal in-house training program exists, assessors may elect to review samples of training records or certifications to indicate what training is available and who has completed the training. Also, needs analyses and job task analyses, as well as lesson plans, should be reviewed. These tools, when undeveloped or poorly conceived, undermine the integrity of the entire training program. Time permitting, assessors may also elect to attend a training session to determine whether the training covers all relevant information and is appropriately tailored to the audience’s needs.

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 help identify process inefficiencies, training deficiencies, and failures to meet DOE requirements.
F. Assessors should determine how management communicates goals and objectives and emphasizes the importance of personnel security. Assessors 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. Assessors should determine whether the persons responsible for the personnel security program are in appropriate positions to ensure compliance and whether they receive adequate management support, especially with respect to implementation of the HRP, SSAP, and FV&A programs. Managers in the security department and the operations and production departments should be interviewed to determine whether the security organization has difficulty obtaining cooperation with the operations or production personnel to implement required procedures. Reviews of self-assessments, survey findings, and corrective action plans may 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. Assessors should coordinate with the PPM team to determine whether surveys and self-assessments are performed regularly and whether all aspects of the personnel security program are reviewed. Comparing the results of the facility surveys and self-assessments to EA assessment findings or other audit results can help determine the relative effectiveness of self-assessments.

I. Assessors should determine whether corrective action plans have identified all causal factors, specific actions (with milestones) to address all causal factors, and specific individuals responsible for implementing corrective measures.

J. Assessors should assess the role of DOE/NNSA oversight by examining recent survey reports to determine whether they are comprehensive, and whether survey results correlate with the results of EA activities. Specific items to cover include how DOE/NNSA reviews the contractor personnel security program functions during surveys, how DOE/NNSA tracks program status, and how DOE/NNSA and the facility interact on a daily basis.

Performance Test

K. Assessors should review all deficiencies indicated as “closed” and collect data to verify that the prior deficiency has been corrected adequately.
Section 3: Personnel Security Clearance Program

References

Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 (50 U.S.C. 435b)  
Security Clearances; Limitations, (amends the IRTPA of 2004, and is referred to as the Bond Amendment)  
DOE Order 472.2, Change 1, Personnel Security  
DOE Order 470.4B, Admin Chg 1, Safeguards and Security Program, Attachment 3, Section 1, Chapter V,  
Personnel Security Clearances and Exclusion Procedures Required in Connection with Contractor Facility  
Clearances  
DOE Order 470.4B, Admin Chg 1, Safeguards and Security Program, Attachment 3, Section 4, Control of  
Classified Visits  
Department of Energy Acquisition Regulation 48 CFR 970.2201-1-2(a)(1)(ii), Labor Relations  
DOE Order 470.5, Insider Threat Program  
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

General Information

The PSC program is the fundamental process for determining the eligibility of an individual seeking access to  
classified information and SNM, and is the first line of defense against the insider threat. The DOE PSC program  
establishes a structured and uniform approach for determining eligibility. Only individuals whose jobs require  
access to classified matter or SNM are to be processed for security clearances.

The following responsibilities of a contractor organization’s PSC program are of primary importance and are  
within the scope of EA-22 appraisal activities:

- General Requirements for Security Clearances
- Pre-employment Checks
- Security Clearance Suspension, Revocation, or Denial
- Classified Visits
- Processing Clearance Requests
- Screening and Analysis
- Adjudicating Derogatory Information.

Figure 1 provides a summary description of the DOE clearance process.

The key components of the clearance process include verifying that clearance requests are justified and that  
pre-employment checks are completed prior to requesting a clearance, 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.

Although resources are addressed in Section 2, Management, assessors should specify whether sufficient  
personnel are assigned to security clearance processing. If too few adequately trained personnel are assigned to  
this function, significant deficiencies and backlogs in the processing system can result.
Pre-employment checks identify derogatory information that would preclude employment for a potential contractor employee. Pre-employment checks include verification of citizenship, a credit check, and 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. Secretarial direction added proof of a negative drug test to the pre-employment process. The pre-employment checks and resulting suitability review must be completed prior to submission to the DOE/NNSA personnel security organization for processing.

Contractors must report to their servicing personnel security office any change in the need for a security clearance, potentially disqualifying information, restriction or withdrawal of an employee’s access to classified matter, termination of employment, or transfer of an employee to a different location. All reports must be made within two working days, followed by written confirmation within the next ten working days. Of equal importance is the need to share this information with the site badge office and other applicable site security and operational organizations in order to prevent unauthorized access. Assessors should determine whether information regarding any changes in clearance or employment status has been reconciled with all relevant site databases. Reporting is an integral part of the General Requirements for Security Clearances, Pre-employment Checks, Processing of Security Clearances, and Screening and Analysis subtopics, so common deficiencies/potential concerns, planning, data collection activities, and performance testing related to reporting are included in the applicable sections of those subtopics below.

When the servicing personnel security organization suspends an employee’s security clearance or denies a final security clearance, the contractor, once notified, must ensure that the employee is denied access to classified information or SNM.

Contractors must ensure that classified matter and SNM is protected by limiting access to such matter to DOE/NNSA or OGA employees or individuals from foreign governments with the appropriate security clearance, need-to-know, and programmatic authorizations. Contractor organizations must control classified visits consistent with the site’s mission, national laws and regulations, and international treaties and agreements.

Contractor assistance to obtain employees’ compliance and cooperation with re-investigations is critical to the timely completion of these functions. Common deficiencies, potential concerns, planning activities, data collection activities, and performance tests for re-investigations are the same as for applicant cases.

The contractor must maintain current records that reflect, by contract number, all contractor employees granted security clearances. Accurate contract information is necessary to ensure that clearances are not held unnecessarily when the governing contract no longer requires access to classified information.

Although not normally within the scope of EA-22 appraisal activities, the following primary DOE/NNSA personnel security organizational responsibilities for the security clearance program and supporting processes are discussed in this section of this assessment guide:

- Processing Clearance Requests
- Screening and Analysis
- Adjudicating Derogatory Information.

To effectively process clearance requests, paperwork flows from the initiation of the clearance request, through certification of need, to verification of completeness, and finally to forwarding of the request to the appropriate investigative agency by the DOE/NNSA personnel security organization. The process ends with the notification of the DOE/NNSA personnel security organization’s grant, reinstatement, or denial of the clearance. Staffing, training, procedural guidance, and oversight significantly affect the success of this process. DOE’s
implementation of IRTPA-related initiatives, such as electronic fingerprinting and using the Electronic Questionnaire for Investigation Processing (eQIP), has resulted in more timely and accurate submissions of requests for investigation.

Screening and analysis of the background investigation (BI) reports or other reported information (self-reporting, security infractions, employee concerns programs, Inspector General investigation reports, pre-employment check results, and other sources) are among the most important aspects of the overall PSC program.

Upon receipt of completed reports of investigation, the personnel security specialist, using screening and analysis functions including checking, must ensure that all items on the eQIP were covered; that the scope of the investigation was met; and that the reported information was evaluated (in relation to the criteria in 10 CFR 710) to determine whether the reported information raises significant doubt about 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, reducing the time to screen investigation reports and meet IRTPA standards.

The evaluation of how well the DOE/NNSA personnel security organization adjudicates derogatory information is a challenge to the assessor because of the common sense judgment required to determine an individual’s eligibility for a security clearance. Assessors should avoid placing 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 case evaluation sheet (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 significant doubt about clearance eligibility. When significant doubt is noted, a number of alternatives are available for resolution, including letters of interrogation, interview, psychiatric evaluation, information from outside sources, and additional investigation. When 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.

IRTPA standards for applicant cases state that as of December 2009, DOE/NNSA must make an initial clearance determination for 90 percent of the applicant cases within 20 days after the receipt of a completed investigation.

The DOE re-investigation 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 ten years. Common deficiencies, potential concerns, planning activities, data collection activities, and performance tests for re-investigations are the same as for applicant cases, except for those items specifically related to applicant cases and meeting IRTPA standards.

**Common Deficiencies/Potential Concerns**

**General Requirements for Security Clearances**

**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 that they be consistent with the work performed. A DOE Federal employee must review all clearance requests and justifications to ensure that they meet these criteria. Requests not meeting these criteria should not be processed. Further, contractor personnel security
organizations must establish a process that periodically validates 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.

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 assessments can affect justification for continuing a clearance.

A particular problem has been noted 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, thus making it difficult to determine whether the clearance needs to continue after job completion. Consequently, the clearance may not be terminated in a timely manner, and security badges may not be returned. Over time, the number of contractor personnel no longer needing access continues to grow, increasing the possibility of unauthorized personnel gaining access to DOE/NNSA facilities.

Pre-employment Checks

Derogatory Information Not Forwarded to DOE. Contractors may not always forward all derogatory information revealed during pre-employment checks or may not provide sufficient detail to ensure that unnecessary requests for clearances are not processed or that processing is stopped (i.e., clearance is denied), that current clearances are not inappropriately continued (i.e., clearance suspended), and that adjudicative actions can begin as soon as possible. Failure to forward all derogatory information may result from an oversight or from ineffective contractor procedures for providing information to the DOE/NNSA personnel security organization. All derogatory information obtained during pre-employment checks must be forwarded so that the DOE/NNSA personnel security organization can properly scope the investigation being submitted to the Office of Personnel Management (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 (such as drug testing) may not be reported on eQIP. Failure to provide proof of drug test completion along with the request for clearance can delay processing of the clearance request.

Security Clearance Suspension, Revocation, or Denial

Even though contractor organizations may take timely action to update local files or databases with information on action to suspend or revoke an employee’s security clearance, actions to restrict that employee’s access may be delayed or sometimes not completed because of inadequate coordination between the personnel security organization and the site badge office or other applicable site organizations. Reliance on individual action instead of formal procedures and training is often the cause of failure to either restrict access or allow only authorized access.

Classified Visits

The contractor personnel security or visitor organization may fail to ensure that the identity and clearance level of the visiting DOE or OGA employee are verified. Unless this essential step is correctly completed before a visitor gains access to sensitive site facilities or information, there can be no assurance that these sensitive facilities and information are adequately protected.
Processing Clearance Requests

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 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. Individuals responsible for processing the requests must be kept informed of any changes. When an individual is no longer a candidate for a position requiring a security clearance or has terminated employment, DOE must be notified immediately, and the request for clearance must be canceled/terminated.

Screening and Analysis

Lack of Timely Screening and Analysis. Lack of timely screening and analysis usually results in a backlog of clearance requests and re-investigation 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, reducing 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 screening and analysis process may be inadequate or out of date. This process is critical to the PSC process and must 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, and supervisors/managers are reluctant to share this information, thereby allowing individuals with unresolved derogatory information to 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 encourages 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.

Adjudicating Derogatory Information

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 resolving 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 security concerns remain unresolved. Inadequate 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 still experience difficulties in completing initial security determinations in a timely manner. Shortfalls in resources and process inefficiencies are the primary reasons for personnel security organizations exceeding the required timeframes.

**Planning Activities**

**General Requirements for Security Clearances**

- 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 contracts. Use this list to select files for review to determine whether clearance levels meet or exceed work requirements.
- Obtain a list of all inactive classified contracts to determine whether any current clearance holders are no longer performing work under a classified contract.

**Pre-employment Checks**

- 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 before a request for a clearance was submitted.
- Review the methods used to determine the accuracy and completeness of pre-employment checks.
- Review local site procedures to determine the requirements imposed on contractors regarding their submission of the results of pre-employment checks, including all derogatory information, to DOE/NNSA.
- Determine whether DOE/NNSA personnel security organizations have a process to ensure that the results of pre-employment checks and proof of drug testing are provided before submission to the investigative agency.

**Security Clearance Suspension, Revocation, and Denial**

- Review personnel security organization procedures.
- Obtain a list from CPCI of all applicable suspensions and revocations.

**Classified Visits**

- Review site procedures governing classified visits.
- Ask the site to provide a list of recent classified visitors, highlighting those granted access to RD.
Processing Clearance Requests

- Review the DOE/NNSA personnel security organization’s PSC processing system, tracking system, and procedures.
- Determine whether the DOE/NNSA personnel security organization has encountered any problems in reviewing eQIP packages.
- Review methods for processing naturalized citizens.
- Examine procedures for entering information into the CPCI.
- Examine procedures for the return of OPM form 79A.

Screening and Analysis

- Determine whether sites have developed a formal procedure that requires reporting 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 how long it takes to process cases, compared to the timelines specified in IRTPA (applicants) and DOE requirements (incumbents).

Adjudicating Derogatory Information

- Review procedures for preparing letters of interrogatory, interviewing, forwarding cases for psychiatric evaluation, and 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 from the Office of Departmental Personnel Security to determine whether DOE/NNSA is meeting the processing standards for applicant cases.
- Review OPM Closed Case Reports without 79A to identify reports for possible review.
- Verify that OPM form 79A is returned after completion of actions to resolve derogatory information.

Data Collection Activities

General Requirements for Security Clearances

A. Assessors should interview individuals responsible for handling requests for clearances to determine how the process is conducted and how the need for access is certified. The justification for the access is based on the duties of the position, the need for access to classified matter or SNM, and the appropriate type of clearance. Interviews with the responsible individuals provide helpful information, such as overall explanations, step-by-step procedures, and the process for determining the need for access and the type of clearance.
Pre-employment Checks

**B.** Assessors should review DOE/NNSA survey and site contractor self-assessment reports to determine whether they adequately address the performance of pre-employment checks and drug testing.

**C.** Assessors should interview personnel security managers and review files to determine whether DOE/NNSA personnel security organizations have processed clearance requests without pre-employment checks and drug testing results.

**Security Clearance Suspension, Revocation, and Denial**

**D.** Compare the list of recent suspensions and revocations to site badge and access control records.

**Classified Visits**

**E.** Randomly select individuals who have recently completed a classified visit to the site and determine whether their clearance was sufficient for the level of information being accessed.

**F.** Review badge office records to ensure that all visitors were processed for a classified visit.

**Processing Clearance Requests**

**G.** Assessors 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, if so, whether they are primarily caused by a lack of personnel or inappropriate use of existing personnel.

When an office has established production quotas in the clearance process, these quotas can be examined to determine whether they are realistic and contribute to or detract from achieving objectives.

**H.** Assessors should determine how the DOE/NNSA personnel security organization resolves and tracks derogatory information identified on the eQIP submission.

**I.** Assessors should verify that the procedures for processing naturalized citizens are in accordance with DOE directives.

**Screening and Analysis**

**J.** Assessors should review the workload, overtime, and turnover rate of personnel security specialists to determine whether sufficient resources are allocated to perform effective screening and analysis. Individuals should be interviewed when there are indications that these factors are impacting performance negatively.

**K.** Assessors should determine whether specialists consider using letters of interrogatory, personnel security interviews (PSIs), supplemental investigations, requests for information from outside sources, or psychiatric evaluations to gain additional information to adjudicate a case. CESs should reflect the rationale for these considerations.
Adjudicating Derogatory Information

L. Assessors should review staffing to determine whether adequate personnel resources are assigned to process derogatory information.

Performance Tests

General Requirements for Security Clearances

M. Assessors should review PSFs to determine whether their duties justify the clearance. Alternatively, assessors should interview selected cleared personnel (especially human resources, contracts, finance, medical, and maintenance personnel) to determine their access requirements.

N. Assessors should obtain a list of contractor and subcontractor personnel whose employment has been terminated, whose security clearances have been suspended or revoked, or whose security clearances have been downgraded to determine whether appropriate action was taken to report applicable actions to the servicing DOE/NNSA personnel security organization, make necessary changes in site databases, restrict site access as necessary, and obtain the return of invalid security badges in a timely manner.

O. Assessors should compare the list of inactive contracts with the site’s list of cleared individuals to determine whether there are any individuals who are no longer working on an active contract and whose clearances should therefore be terminated.

Pre-employment Checks

P. Assessors 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 correlates with information forwarded to the DOE/NNSA personnel security organization, and whether the contractor ensures that pre-employment checks include all required elements.

Q. Assessors 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.

Security Clearance Suspension, Revocation, and Denial

R. See General Requirements for Security Clearances, above.

Classified Visits

S. Observe visitor control personnel identifying visitors and verifying their clearance level.

Processing Clearance Requests

T. Assessors 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 were made as required by DOE policy. In preparation for this performance test, assessors should coordinate with the Office of Departmental Personnel Security to obtain a CPCI report indicating the date of entry of information related to the selected files.
U. Assessors should review selected PSFs to ensure appropriate return of OPM form 79A.

V. While reviewing randomly selected PSFs (see items X and Z below), assessors should determine 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.

**Screening and Analysis**

W. Assessors should review site records to determine whether reports of incidents of security interest (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.

X. Assessors should review randomly selected PSFs to determine whether screening personnel are consistently and accurately identifying the absence or presence of derogatory information.

Y. Assessors should review randomly selected PSFs to determine whether initial screening and notification of continuations of incumbent clearances were completed within seven days of the receipt of completed investigations in clear cases. Assessors should also determine whether adjudicative actions are initiated within 30 days of receipt of the completed investigations when derogatory information is identified.

**Adjudicating Derogatory Information**

Z. Assessors should randomly select a number of PSFs for review from listings provided by the assessed site. The listings should identify cases processed by the site in a particular timeframe, usually the preceding six months. Separate listings should be requested for each type of case (clear, containing derogatory information, terminations, denials, and suspensions). If backlogs (timeliness issues) are evident in the completion of these cases, assessors should determine the causes. Interviews with security managers will assist in making these determinations.

AA. Assessors 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 whether 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 be validated for the selected cases.

BB. Assessors should review cases in which the clearance was denied or suspended to determine whether or not proper procedures were followed and whether timely CPCI data entries were made.
Section 4: Human Reliability Program

References

DOE Order 470.5, Insider Threat Program
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 owns, leases, operates, and/or supervises activities at facilities in various locations in the United States. Many of these facilities are involved in researching, testing, producing, disassembling, and/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 and the nation have the highest interest in protecting these facilities and activities from potential misuse by employees or contractors 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 and/or 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.

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 recertification reviews, assessments, and evaluations consisting of:
• Supervisory review

• Medical assessment (including psychological evaluations)

• Management evaluation (including 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 re-investigation every five years. Personnel enrolled in the 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 ensure that individuals in the HRP are aware of behaviors that may indicate a security concern.

Alcohol testing for HRP-enrolled employees is 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 remains 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 is conducted randomly; or following an incident, unsafe work practice, or occurrence; or 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 may create significant vulnerabilities.

HRP medical officials do not always properly identify and report security concerns. In some cases, HRP medical officials do not report or recommend temporary removal to the HRP Management Official when a medical restriction has been placed on an HRP-certified employee or when security concerns are uncovered as part of the medical assessment. As a result, HRP employees could have access to an MAA and SNM while no longer being suitable for performing 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, workers may be performing HRP duties in positions that have not been identified as HRP positions, as defined by 10 CFR 712. This discrepancy may result from the lack of a systematic method for identifying HRP positions. In other cases, it 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 interaction with the site’s vulnerability assessment organization could cause positions to be misidentified as not requiring inclusion in the HRP.

Another potential concern is failure to track and analyze the threat represented by non-HRP individuals routinely working in areas where access to Category I quantities of SNM is possible. Although these individuals are normally escorted when working in such areas, some of them spend enough time in those areas to give them knowledge of sensitive operational and security information. In some of these cases, the absence of effective site tracking mechanisms for escorted visitors has led to the failure to enroll these individuals in HRP.
Improper Performance of HRP Duties

When frequently-escorted visitors are determined to be HRP candidates, they should not perform HRP duties until they are HRP certified. Site procedures that allow HRP candidates to access sensitive areas for training in their future HRP duties should be reviewed carefully to ensure that adequate controls are in place that prevent candidates from unilaterally performing HRP duties. At some sites, controls that prevent unilateral performance of HRP duties by candidates will not support on-the-job training activities in normal work areas, and alternative training approaches, such as training in surrogate facilities, will better accomplish security and training objectives.

Unassigned HRP Responsibilities

Facilities may fail to assign or properly document the assignment of responsibilities to organizations and persons for various aspects of the HRP, inevitably leading to some elements of the program not being implemented and possibly resulting in unidentified HRP positions. An effective approach is to specifically assign responsibility for every aspect of the program in writing, first to an organization and then to a specific position or positions within that organization.

Improperly Conducted HRP Supervisory Reviews

If supervisors do not conduct their reviews thoroughly and responsibly, the evaluation process may become reactive rather than proactive and the HRP will become less effective. Supervisors might lack sufficient interaction with employees or may supervise too many employees to effectively complete the annual supervisory review and/or report each observed safety or security concern to the HRP Management Official.

Inadequate HRP Drug and Alcohol Testing Program

When conducting the drug and alcohol testing program, sites might not have established a methodology to ensure random selection and testing to provide effective detection and deterrence of illegal drug use or abuse of alcohol. The best method for maximizing detection and deterrence is to conduct random selection and testing 24/7 every day that workers are performing HRP duties. Individuals working off-shift and on weekends and holidays should not be excluded from the selection pool of candidates.

Some sites have developed selection algorithms that significantly reduce the probability of selecting individuals who have already been tested. In other cases, sites may exclude individuals who have been tested multiple times from the testing pool until after re-certification. In either case, individuals might become aware of these practices, thus reducing the ability to detect 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 when HRP-certified employees are tested multiple times. If the site yields to this temptation, its drug and alcohol testing program will be ineffective and will not provide the intended benefits to the site protection program.

Assessors may discover that some sites do not have a process for conducting tests on the basis of reasonable suspicion or after an occurrence, incident, or unsafe work practice. The absence of such a process can result from inadequate training of supervisors and employees. More often, the problem exists because the sites have failed to establish lines of communication among safety and security organizations, and/or sites may not have developed specific criteria to help individuals decide when testing should occur. HRP training programs must emphasize the need to test whenever a suspicion arises regarding drug use or alcohol abuse by HRP personnel, whether 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 (e.g., no access to a source of water, chemicals in the testing area, and lack of visual and aural protection). Such shortfalls 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 the breathalyzers used by site testing technicians meet the functional requirements prescribed by the manufacturer and produce accurate test results. For the drug testing program, blind test programs are required to ensure that the certified testing laboratory used to analyze collected urine specimens produces 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 may not refer to the job task analysis (JTA) when assessing employees seeking HRP certification or re-certification. When medical professionals are unfamiliar with the JTA, they may be unable to accurately assess the impact of a medical or mental condition on the individual’s ability to perform HRP duties. The JTA should be readily available to applicable medical professionals or placed in the files to ensure its availability each time an HRP-certified individual is seen.

**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 to ensure timely reporting of medical restrictions that may impact an individual’s 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 how prescribed medications affect 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 site’s HRP medical official may decide that a particular observation is strictly a safety concern and not a security concern, and thus may not report it to the SOMD, HRP management, or certifying official. In some instances, this decision may be wrong, and a security concern goes unreported. The HRP implementation plan should clearly stipulate the procedures for 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 occupied these positions, and all personnel pending initial certification.

- Determine whether the site has a process for identifying positions and employees for HRP. This process should include the requirement for a formal analysis to support the enrollment of individuals who can significantly impact national security (“criteria 4” positions). Each site should have a process for tracking and trending escorted visits to the MAA to help determine whether any frequent visitors should be enrolled in HRP or denied further escorted MAA access. HRP officials should be in close communication with vulnerability assessment team members.

- Determine whether the site has a process for immediately removing individuals who test positive for illegal drugs or alcohol abuse.
• Determine whether the facility has a random drug and alcohol testing program and whether the program includes: testing for reasonable suspicion after an occurrence, incident, or unsafe work practice; chain-of-custody procedures; unannounced selection and testing procedures; employee notification for testing and documentation; procedures and documentation of employees selected for testing, but not tested; a process for tracking whether each employee is tested within 12 months of the last test; and availability of all materials required to effectively conduct the tests.

• Identify the level of directed or non-random drug and alcohol testing to determine whether testing is genuinely random. Also, identify the authorized excuses for failing to complete a drug or alcohol test after being selected.

• Verify that 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 who test 0.02 or greater are sent home, concentrations above 0.04 are recorded, and additional actions are taken to determine whether the consumption occurred on the job. Determine whether the site has an effective quality assurance program that includes external calibration checks on all breath testing devices used and a blind sample drug testing 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 so designated.

• Review training materials (including instructor guides and student handouts) to determine whether a training program exists for instructors, managers, supervisors, medical officials, and HRP personnel.

• Determine whether managers, supervisors, and HRP personnel receive awareness training every 12 months on the topic of recognizing aberrant behavior.

• Determine whether managers, supervisors, medical personnel, and security specialists conduct the required reviews and where the copies of these reviews are kept.

• Review the procedures for immediate or temporary removal and determine whether there are protocols permitting escorted access for individuals who have been removed. Determine whether removed individuals are also removed from the site’s access control system for the MAA or areas that store or possess nuclear weapons, components, or SNM.

• Determine whether supervisors can adequately observe subordinate HRP-certified employees or have a mechanism 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. Assessors 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 use vulnerability assessment results when identifying positions requiring HRP enrollment.
B. Assessors should review MAA access records to determine whether there are individuals who have been 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 be compared to all individuals pending HRP certification.

C. Assessors 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, the HRP Management Official, and the HRP Certifying Official; immediate and temporary removal; termination; and an effective program for maintaining appropriate data on HRP positions.

HRP Training Program

D. Assessors should review training records to determine whether initial and annual refresher training is completed and whether the records are complete and adequately maintained. Assessors should consider interviewing managers, supervisors, and HRP personnel when training materials appear to be deficient in order to determine the impact of such deficiencies on these individuals’ understanding of their HRP responsibilities.

E. Assessors should determine whether the medical personnel supporting HRP received adequate training on program objectives and their individual roles and responsibilities, whether they are knowledgeable of medical/mental conditions constituting a security concern, and whether they understand the requirement to report these conditions to the HRP Management Official.

F. Assessors should determine whether sufficient training materials have been developed for the training staff and for all other personnel involved with the program. When possible, one or more assessors should attend a training session to determine the effectiveness of training and observe the completion of duties.

HRP Drug/Alcohol Testing Program

G. Assessors should review drug and alcohol testing procedures and the quality assurance program and should assess facilities, equipment, and the materials used to conduct the tests. Individuals responsible for conducting drug/alcohol testing should explain each of the steps of the testing process. Assessors should observe drug and alcohol tests being performed to verify that policy and procedures match actual practice. For drug testing, assessors should review procedures for handling specimens to determine whether an effective chain of custody is maintained and whether the site has established a blind sample test program. Assessors should also observe the administration of a breath alcohol test.

H. Assessors should review the selection process for random testing to determine whether it is, in fact, conducted on a random, unannounced basis, and whether individuals selected for testing arrived within two hours of notification. Assessors should review the procedures for alcohol testing when individuals are called in for unscheduled work. Assessors should review a sampling of any positive drug and alcohol test results to ensure that appropriate actions are taken, including timely reporting.

I. Assessors 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 is implemented as described. Assessors should also review the processes for excusing individuals from testing; testing employees for reasonable suspicion; and testing following an incident, unsafe practice, or occurrence. In addition, assessors should determine how information is communicated between supervisors and the safety and security organizations. If some employees have not been tested, determine why they were excluded. Assessors should verify the consistency of testing and whether the reasons for conducting these types of tests are well known and specified in written procedures. Assessors should review lists of disciplinary actions, accidents, and security incidents to determine whether the appropriate individuals are tested for occurrences and/or reasonable suspicion.
J. Similarly, assessors should review records to verify whether individuals in designated positions prohibiting the consumption of alcohol eight hours prior to reporting for work are sent home if they test at 0.02 or greater, and whether additional tests are conducted if they test at greater than 0.04. Individuals returning to work after testing positive should be re-tested until they test at less than 0.02 before they are allowed to perform HRP duties. This process should be part of the reasonable-suspicion test procedure.

**HRP Reviews and Evaluations**

K. Assessors should examine the HRP evaluations to determine whether all parts have been completed annually, including the supervisory review, medical assessment (including a determination of whether the JTA was used and is adequate), security review, and management evaluation. Re-certifications must be completed within 12 months of the last certification or re-certification date.

L. Assessors should 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.

**HRP Records and Files**

M. Assessors should examine the system in place for maintaining HRP records. Assessors must verify that the information contained in the files is pertinent to the program; is timely, accurate, and structured; and is maintained to allow an audit trail of events and actions.

**Reporting Requirements**

N. Assessors should determine whether a complete understanding of what constitutes a reportable HRP concern exists between the site's HRP medical officials (psychologists, physicians, physician’s assistants, etc.), the DOE/NNSA site office, and the DOE/NNSA personnel security organization.

**Performance Tests**

O. Assessors should evaluate drug and alcohol testing technicians to determine whether they are conversant with all the drug and alcohol testing requirements, and whether the technicians understand their responsibilities.

P. Assessors should review randomly selected files to determine whether a system exists for maintaining HRP, medical, and psychological records. Assessors must 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 assists the assessor in determining whether good lines of communication exist between HRP and medical officials.

Q. Assessors should compare access control records with the list of individuals removed from performing HRP duties as a test of site HRP program procedures intended to ensure that these individuals do not enter HRP-required areas (either alone or under escort) and do not continue to perform HRP duties while on restriction.
Section 5: Foreign Visits and Assignments Program

References

DOE Order 142.3A, Unclassified Foreign Visits and Assignments
DOE Order 470.5, Insider Threat Program

General Information

In the conduct of Departmental operations, Federal and contractor facilities often host visits and assignments by foreign nationals. DOE and international partners benefit from the exchange of information that results from a managed process of unclassified FV&As. However, contractor organizations that host foreign visits must ensure that the potential threat that foreign visitors may pose to sensitive information, classified matter, and SNM is thoroughly analyzed and mitigated. The analysis must also consider the inherent risk in the proximity of foreign visitors to these security interests. DOE policy follows a graded security approach for reviewing and approving access by foreign nationals to sites, programs, information, and technologies based on subject, location, and length of time for the requested access, as well as the country affiliation(s) of the individual granted access. The analysis should be based on foreign visitors’ abilities to observe operations or security measures and should ensure that unauthorized access to information, equipment, and technologies is denied.

The graded security approach is also evident in FV&A policy regarding the requirements to:

- Depending on the country of residence, document the requests (if required) in the Foreign Access Central Tracking System (FACTS) either no later than the start date, or in time to obtain indices checks, or within five days after the start date.

- Complete indices checks (if required) based on the country of residence either before approval determination, or by the start date, or before site access.

- Choose the appropriate level of approval authority for contractor-hosted foreign nationals based on the country of origin or citizenship, as follows:
  - Non-sensitive country: Site management official or laboratory director
  - Sensitive country: Site management official or laboratory director
  - State sponsor of terrorism:
    - Visits: Lawful permanent residents – site management official or laboratory director; all others – Deputy Secretary/cognizant Under Secretary
    - Assignments: Lawful permanent residents – site management official or laboratory director; all others, initial – Deputy Secretary/cognizant Under Secretary, subsequent – site management official or laboratory director.

A large majority of FV&As each year occur at sites that do not perform classified work (primarily Office of Science laboratories), so using the graded approach has led to fewer visits and assignments being documented in FACTS, fewer requests submitted in time for completion of an indices check before site access is permitted, and fewer requests approved at Headquarters. Therefore, assessors should focus their activities on FV&As from sensitive countries and from state sponsors of terrorism, and on sensitive subjects, because these represent the most serious threats and are subject to greater scrutiny and requirements.
Pursuant to a recent change in policy, FV&As no longer require the development of a general or specific security plan. Instead, the SSP or SSSP must provide adequate direction for site personnel to successfully host a foreign national.

Despite these impacts and changes, sites must still verify the identity of foreign nationals and their legal status to be in the United States, and sites must still ensure the protection of sensitive and classified information and SNM.

**Common Deficiencies/Potential Concerns**

**Incomplete Notice for FV&A Requests**

Previous assessments have shown that visits and assignments are sometimes requested with less than the required advance notice. In such cases, necessary actions – such as operations security (OPSEC) and export control reviews and indices checks – are not given appropriate consideration or may not be completed at all.

**Identity, Lawful Immigration Status, and Documentation**

In addition to the information required to be submitted for FV&A requests, all sites, facilities, and laboratories must collect sufficient identification (passport) and lawful immigration status (visa) documentation for review and for entry into FACTS. This documentation is required to verify identity and authority to work and to ensure that the foreign visitor is currently eligible to be in the United States. When a site fails to collect this information, the FV&A request may be improperly processed.

**Access Control**

Inappropriate issuance, control, and retrieval of badges; changes in security areas and their sensitive contents; and poor computer access control all have a direct and significant impact on the effectiveness of the FV&A program. In some cases, badge office personnel issue the wrong badges to foreign visitors, allowing an improper level of access that should be reserved for site employees. In other cases, foreign national visitors are allowed to enter site facilities without a badge or with an expired foreign badge. These issues are especially prevalent at sites that employ many foreign nationals. Nevertheless, sites have the responsibility to issue the appropriate badge to foreign visitors, and site employees must deny access to site facilities if foreign visitors lack the proper badges.

**Deterioration of Escort Procedures**

Vigilance in escorting foreign visitors, especially long-term assignees, may wane as escorts become familiar with the assignee. Procedures must be 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, giving them a degree of access that could allow them to compromise security interests. Security awareness on the part of hosts, escorts, and other individuals in the facility must be maintained.

**Inadequate Host Actions**

Hosts are responsible for ensuring that no unauthorized access occurs. Although past assessments have shown that many hosts are aware of the applicable requirements and their responsibilities, hosts do not always adequately report changes to approvals and plans regarding a visitor’s physical location, duties, and approved subject matter. Hosts also fail to report changes in assigned escorts, 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, a manager or employee with full knowledge of facility security interests and measures should be formally identified as an additional host. This individual can help ensure that adequate control measures are in place for the duration of the visit or assignment and can also assist in escort training.
Use of Site Computing Assets

Because nearly all visiting foreign nationals are provided access to a site’s computing systems, it is important to balance the visitor’s needs against the need to protect the information stored on these systems (and the systems themselves) from unauthorized use or modification (including access after duty hours) to ensure that no improper access is permitted. After-hours access presents special concerns when a foreign visitor can access other computer workstations that are not password protected. A particular problem occurs when foreign personnel are given remote access to computer networks and are not stationed on site, or possibly accessing these networks from outside the United States. Personnel security assessors reviewing the FV&A program should ensure that risk assessments and required security plans have been developed and approved. Assessors may also review any incidents of security concern that involve foreign nationals to determine whether any have included improper access to site computing assets. Changes in computer access should be reviewed to ensure coordination with cyber security. Assessors should also determine whether the site has a process 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 (FACTS)

Over the past several years, a concerted effort has been made to keep the information contained in FACTS current and correct. Recent assessment results have indicated that most sites are achieving more success in accomplishing this objective. However, some problems have been noted. One of the most common problems is that some sites do not validate that automatic uploads in FACTS were completed successfully. Lacking validation, inadequate or incorrect information can reside in FACTS for an extended period of time before being discovered. Correcting this problem often requires manpower-intensive solutions until the software is modified, and because sites may not have identified the resources needed to modify the software, these manpower-intensive solutions may remain in place for an extended period.

Planning Activities

During the planning phase, assessors should identify points of contact for both the DOE/NNSA site office and the appropriate contractor to discuss the scope of the FV&A review and determine whether all data call requests will be available. (Some sites have more than one contractor involved in FV&A activities.) Planning activities should include:

- Review local procedures for requesting, processing, and approving visits and assignments by foreign nationals.
- Determine whether adequate controls are in place for issuing site-specific DOE security access badges and proximity badges to foreign visitors.
- Review the procedures for escorting foreign visitors.
- Identify all site PPAs, LAs, PAs, and MAAs that hosted sensitive country and state sponsor of terrorism foreign visitors and assignees during the past six months.
- Determine the number of sensitive country, state sponsor of terrorism, and sensitive subject visits and assignments that have occurred during the past six months, including the dates of each visit or assignment and the names of the hosts.
- Coordinate with the classified matter protection and control (CMPC) topic team to determine where classified matter is stored, and compare this information with areas where foreign visitors and assignees are authorized access.
- Obtain a list of all incidents of security concern involving foreign visitors and their escorts or hosts.
Data Collection Activities

Plans and Procedures

A. Assessors should determine whether the site has a comprehensive and integrated approach to FV&As by reviewing a sample of request forms and the SSP or SSSP (as applicable) to determine whether they cover the elements required by DOE Order 142.3A. A random sample of visit requests should be examined to determine whether they are timely and complete, and whether they have the appropriate level of approval. Special attention should be given to ensuring that indices checks and documentation in FACTS have been completed. If deficiencies are noted, reviewing additional visit requests would be prudent.

B. Assessors should determine whether individual and organizational roles and responsibilities are clearly understood, and whether the site has an integrated approach to assessing the risks to classified and sensitive unclassified information (including cooperative research and development agreements) that the visit or assignment poses. This approach should identify the location of classified and sensitive assets, assessment of current security measures, and development of additional protective measures to mitigate risks.

Host/Escort Procedures

C. Assessors should determine the site’s requirements for hosting and escorting foreign nationals and examine procedures and host/escort training to determine whether they are adequate and provide the information necessary to promote a high degree of security awareness. Additionally, hosts/escorts should be interviewed to determine their knowledge of and adherence to program requirements. Assessors may want to determine whether similar interviews are conducted during periodic safeguards and security surveys, self-assessments, and counterintelligence assessments.

Coordination

D. Assessors should interview selected site subject matter experts (OPSEC, counterintelligence, classification, and export control personnel) to determine whether the site has an effective and integrated approach for assessing risks to classified matter and sensitive information before approval of a visit or assignment. Assessors should also determine whether the requirements for this coordination are included in the SSP or SSSP.

Non-Compliance

E. Assessors should review all incidents involving a foreign national visitor/assignee and determine whether these incidents reveal systemic weaknesses in the site FV&A program. Assessors should also determine whether the site’s actions in response to these incidents appropriately cover all identified causal factors.

Performance Tests

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

- Conduct walking tours of areas that have hosted, or are hosting, foreign visitors to determine the adequacy of actions taken to mitigate the threat represented by the presence of foreign visitors, and whether 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 whether they are knowledgeable of security plan requirements and their responsibilities pertaining to the visit.

- Interview any visiting foreign nationals on site to determine their knowledge of authorized access and their own responsibilities.
Section 6: Safeguards and Security Awareness Program

References

DOE Order 470.4B, Admin Chg 1, Safeguards and Security Program
DOE Order 472.2, Change 1, Personnel Security
DOE Order 470.5, Insider Threat Program
Executive Order 12968, Access to Classified Information
Executive Order 13526, Classified National Security Information
Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts
32 CFR 2003.20, Classified Information Nondisclosure Agreement: SF-312

General Information

The DOE/NNSA SSAP is designed to inform all individuals 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.

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, the site/facility must develop and implement briefing plans, briefing objectives, supplemental awareness materials, and evaluation methods.

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. In some cases, the SSAP may be delegated to contractor support personnel.

Normally, the facility security department is responsible for managing 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.

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

- **Initial briefings** inform cleared and uncleared individuals of local security procedures and access control requirements before those individuals begin their 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 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 are also used to communicate 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 are the final reminder to 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. In the latter 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, so special emphasis must be placed on evaluating the site procedures for scheduling and conducting these briefings.

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**

**Inadequate Documentation**

Although all DOE/NNSA sites have mature security awareness programs, the various self-assessments, surveys, and assessments periodically identify that Standard Form (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 permitting their expeditious retrieval.

Written implementation procedures, briefing plans, supplemental awareness materials, and program records reflect how the facility conducts its SSAP. The presence and quality of these materials can indicate whether the program is effective. Without adequate documentation, current and relevant program materials, and effective communication of program requirements, employees might not receive the required safeguards and security information.

Documenting the completion of the comprehensive briefing, normally accomplished on an SF 312, is of special interest. This level of formality is needed to establish a legally sufficient confirmation that the individual has received the comprehensive briefing before 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 as well.
Inadequate Briefing Content and Material

In some cases, briefings fail to address all required subjects. Some sites use video presentations exclusively. Although some films and slide presentations look professional, they are often outdated and lacking the required subject matter and purpose of the DOE order.

Some sites have approved briefing plans that incorporate all program objectives and ensure that attendees are provided with standard information, but sites do not always keep those plans up to date and available.

Presentations, especially the recurring annual refresher briefings, are usually more effective if they are varied, incorporate new material, contain examples and anecdotes, and reflect up-to-date security procedures and the current facility environment.

Specific concerns that have been observed include:

- **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, the person conducting the briefing must be 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 presented improperly, 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 that 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 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.** At some sites, the security organizations responsible for conducting these briefings fail to maintain up-to-date travel advisories disseminated by the U.S. Department of State (via their website) and OGAs. Failure to maintain the current status of foreign country activity could jeopardize both travelers and sensitive information.

  Some computer-based awareness briefing programs fail to include measures that will ensure that an individual has actually reviewed the material before receiving credit for completion.
Quality of Supplemental Materials

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

Planning Activities

- Determine whether copies of materials (briefings, computer-based programs, etc.) produced to support local SSAPs are periodically updated.

- Review the process used to ensure that completion of briefing requirements is properly documented and recorded (SF 312, DOE Form 5631.29, and attendance rosters).

- Determine whether subcontractor employees are receiving required awareness briefings.

- 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 the documents used to notify employees of their requirement to attend specific briefings.

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

Data Collection Activities

Safeguards and Security Awareness Documentation

A. Assessors should examine policies and procedures to determine whether a structured SSAP has been implemented, whether adequate records are kept, and whether a responsible individual receives and updates briefing materials. Records should be examined to determine whether they are current and complete, whether documentation exists to reflect conducted briefings by type and date, and whether the records indicate which individuals attended 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, assessors should attempt to determine their cause.

C. Assessors should determine whether adequate guidance is established for the conduct of briefings, including initial, comprehensive, refresher, foreign travel (when applicable), and termination briefings.

D. Assessors should determine whether comprehensive briefings are conducted before the issuance of security badges.

**Safeguards and Security Awareness for Contractor Personnel**

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

F. Assessors should compare a list of security terminations to badge retrieval/destruction records and CPCI to determine whether security terminations were effected in a timely manner. Comparing employee terminations with clearance terminations helps ensure that 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 whether clearances that are no longer required have been appropriately terminated.

G. If contractors, subcontractors, or consultants have established their own SSAP, assessors should conduct interviews and document reviews to determine whether the operations/site office has provided direction for the implementation of these programs and has 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.

**Documentation**

H. Assessors 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**

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

**Comprehensive Briefing**

J. Assessors 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.

K. Assessors should determine whether an SF 312, or some other appropriate form, was completed by all individuals.

L. Assessors should review all materials (briefing plans and supplemental awareness materials) to ensure that the materials adequately support the comprehensive briefing.
Annual Security Refresher Briefing

M. Assessors 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.

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

Termination Briefing

O. Assessors should review the termination briefing content to ensure that briefings are comprehensive and factual, and that they meet the requirements of the order. Assessors 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 was completed, signed, and dated.

P. Assessors should reconcile the actual dates of termination of DOE clearances with CPCI data to ensure that clearance terminations were entered into CPCI within 24 hours.

Foreign Travel Briefing

Q. 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.

Policies, Procedures, and Files

R. Assessors 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

S. Assessors 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. Assessors should also determine whether themes are appropriate, relate to safeguards and security problems, and agree with DOE policy.

Performance Tests

T. Assessors should attend scheduled briefings (or ask appropriate personnel to provide a briefing for the assessors) 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 assessor should determine whether any feedback mechanisms (question-and-answer sessions, tests, etc.) are used.
U. Assessors should determine whether the SF 312s and security termination statements are maintained as required.

V. Assessors should verify the qualifications and performance of awareness coordinator(s) by interviewing the coordinators and by attending live briefings. The coordinators should have DOE/NNSA security experience and speak authoritatively on the topics presented.
Section 7: Interfaces

Integration

Integration is the coordination and interface among assessment teams designed to achieve a more effective and organized assessment effort. Effective integration requires an enhanced knowledge of the assessed site, current assessment techniques, and overall goals of the assessment.

Integration may be the most important and productive element of assessment activities. Thorough integration creates a synergism that stimulates the assessment process and enhances the quality and validity of the assessment report. Effective integration strengthens EA-22’s ability to provide significant, value-added contributions to the safeguards and security community, as well as to DOE/NNSA as a whole.

The integration process between topic teams must continue throughout all assessment phases to ensure that all pertinent assessment data has been shared.

Integration has several major objectives. 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 performing duties that require enrollment in the HRP. Also, assessment 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. Ideas from one topic team can help another topic team focus assessment 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 occurring simultaneously. This lack of coordination causes undue disruption at the assessed 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 assessed in isolation. Assessment activities must acknowledge and reflect this interaction to determine how well the required interfaces are accomplished, so each assessment team must interface with assessment teams responsible for other areas. Information developed by the personnel security topic team may impact the results of assessment activities in other topics. Similarly, results in other topical areas may influence how the personnel security program is viewed and how success is measured.

The personnel security topic team should be prepared and willing to provide assistance and support to other topic teams. For example, information on escort procedures for foreign visitors may be valuable to the physical security systems, cyber, and CMPC topic teams.
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 in such areas as management’s involvement in reduction and justification of clearances; the role of personnel security in the overall protection strategy; and, if an HRP is in place, management’s involvement in determining the impact of the HRP on noted threats. The PPM topic team may be able to elicit and provide information to verify whether the budget process adequately considers personnel security and HRP requirements. Interviews may include members of both topic teams to limit the impact on site management’s time.

The PPM topic team’s review of the survey and self-assessment programs can provide data on the status of personnel security program effectiveness as viewed by the assessed site’s security organizations. The personnel security topic team should be able to provide information about the status of corrective actions taken to address survey or self-assessment findings.

The PPM topic should be consulted about insider analysis, which is part of the vulnerability assessment process. Of special interest is validation that all HRP positions have been identified and are 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. Assessment teams evaluating these areas can provide information about the briefings’ effectiveness, enhancing the overall evaluation of safeguards and security awareness. The cyber security topic team can address foreign visitor access to computer systems, particularly networked systems. Such coordination should occur during the planning meeting.

 Classified Matter Protection and Control

The CMPC topic team can provide insight about a site’s administration of the incidents of security concern program. The personnel security topic team can ensure 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 at a site (as identified by the CMPC topic team) can be used to identify potential threats and/or improper 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. Access control 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, OGAs, 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 physical security systems topic team responsible for assessing 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 Assessment Guide under the Entry and Search Control subtopic.

**Protective Force**

The protective force topic team may help the personnel security topic team determine whether protective force post orders contain current and accurate information on foreign visitors in a particular location or area.
Section 8: Analyzing Data and Interpreting Results

Introduction

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

When analyzing the data collected on a particular aspect of the personnel security program, it is important to consider how the performance of that aspect may affect the performance of an overall program. Failure of a single facet does not ensure failure of the overall system, unless that facet is critical to the success of the personnel security program. Assessors must remember that even if the analysis determines that the personnel security program would, despite one or more failures, have maintained a secure environment, questions about sustaining an acceptable level of performance may remain and require analysis.

Analysis of Results

The analysis process involves careful consideration by topic team members of all assessment results, particularly identified strengths, weaknesses, and deficiencies. Analysis leads to a logical, supportable conclusion about the personnel security program’s ability to meet the required standards and satisfy the intent of DOE policy. If more than one subtopic has been assessed, a workable approach is to first analyze each subtopic individually. The results of the individual analyses can be integrated to determine: 1) the effects of subtopics on each other, if subtopics must be rated separately; or 2) the overall status of the topic, if a single topic rating must be given.

When no deficiencies are identified, the analysis is relatively simple. If there are negative findings, weaknesses, deficiencies, or standards that are not fully met, the analysis must consider the impact of those conditions. Deficiencies must be analyzed individually and collectively, and balanced against their strengths and other mitigating factors impacting the program’s ability to meet required standards. Factors to consider during analysis include:

- Whether the deficiency is isolated or systemic
- Whether the responsible individuals had previous knowledge 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 justify conclusions concerning the degree to which the personnel security program meets the required standards and the resulting effect on the personnel security program’s ability to accomplish its mission.

Management

Insufficient staff assigned to process clearances can harm the entire personnel security program and is a problem that must be addressed by management. To interpret the results of the personnel security resources subtopic, the assessor must consider the results of the assessment of other personnel security subtopics. Such deficiencies as a lack of timely action to suspend clearances and late or incorrect CPCI data entries can indicate insufficient resources, insufficient training, or ineffective use of existing resources.
Training for personnel who administer and maintain the personnel security program is a crucial aspect of the program. Therefore, when performance issues are identified in a personnel security subtopic, assessors should determine whether training is a causal factor for poor performance.

When assessors discover multiple deficiencies in most or all of the personnel security subtopical areas, it is important to identify the root cause of these deficiencies. This effort may identify a number of systemic problems in management support affecting the overall personnel security program.

**Personnel Security Clearance Program**

Contractor security organizations represent the first line of defense in ensuring that access to NSI, RD, and SNM stored or in use at their sites is not granted before DOE grants a security clearance. Contractor organizations are responsible for ensuring that changes (upgrades and downgrades) in an individual’s clearance status and clearance terminations (for cause, due to a change in employment status, or due to a position no longer requiring access to classified information or SNM) are promptly shared with the servicing DOE/NNSA personnel security organization and site organizations (badge office and employee parent organization). Failing to do so could allow an individual to continue to have unauthorized access while no longer meeting all eligibility requirements.

Contractor organizations must report potentially disqualifying information to the servicing DOE/NNSA personnel security organizations so that the information can be adjudicated and the eligibility of the individual for continued access to classified information and SNM can be determined. In some cases, contractor security managers must decide whether it is appropriate to recommend preventing these individuals from accessing security areas while the appropriate DOE/NNSA personnel security organization completes its deliberations.

A contractor pre-employment check program that does not ensure 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 for clearance processing delays, since the time consumed by personnel security specialists in rectifying errors in pre-employment checks can significantly impact budget and personnel resources.

DOE/NNSA site office officials have the following key functions in the clearance process: 1) certifying the request, 2) ensuring the appropriate level of access, 3) ensuring that the clearance is terminated when no longer needed, and 4) ensuring that derogatory information is reported promptly to the servicing DOE/NNSA personnel security organization.

DOE/NNSA personnel security organizations complete several essential clearance functions, which include resolving or mitigating all derogatory information before a clearance is granted and, after the receipt of derogatory information, ensuring that this information is adjudicated in a timely manner. Granting or continuing a clearance when derogatory information is unresolved poses an unacceptable risk to national security.

Failure to screen and analyze the results of personnel security investigations in a timely manner can adversely impact the organization in need of cleared personnel and the quality of the process of granting clearances. Such failure might result from lack of resources, inadequate training, or both. Personnel assigned to the screening and analysis function must be adequately trained and supported by quality assurance and management attention. Analyzing data in the BI is a critical element of the personnel security program. Poor analysis of the data in the BI can result in unacceptable delays, the granting of clearances to unreliable individuals, or the denial of access to reliable and valuable individuals.

**Human Reliability Program**

Of the highest importance, all individuals performing HRP duties must be identified and certified. Noncompliance with this basic first step in the HRP eliminates all possibility of program effectiveness. Whenever such a failure is
identified, assessors must determine the causal and contributing factors and the specific impact(s) on the site protection program. One example of a damaging impact is a site unknowingly accepting increased risk by assuming that the HRP has effectively mitigated the potential insider threat. When the HRP is cited as a reason for accepting existing risks, assessors 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 to ensure that HRP incumbents are always eligible to perform HRP duties. The benefits of an active enrollment process can be rendered useless if not all required individuals are 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, overall program effectiveness is reduced. When assessors discover that managers, supervisors, and personnel occupying HRP positions are not fully aware of their responsibilities, the program may prove deficient and unable to function effectively. Assessors should view supervisors and HRP-certified employees who are not trained to recognize security concerns and unusual conduct as an indication of a deficiency in the program and, possibly, a lack of management attention.

**Foreign Visits and Assignments Program**

DOE/NNSA’s approval of FV&As authorizes access for a large number of foreign nationals to Headquarters buildings, national laboratories, and nuclear weapons facilities. A site’s failure to verify the citizenship and the eligibility of these visitors before authorizing access or to provide adequate control of these visitors once they are on site could endanger sensitive security interests, Departmental facilities, and employees.

**Safeguards and Security Awareness Program**

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 discover 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 SSAP effectiveness, thereby weakening safeguards and security awareness and the overall security posture of the facility.
Appendix A: Data Collection and Analysis Tools

Baseline List of Contractor Personnel Security Program Direct and Indirect Elements .................. PS-50
Personnel Security Program Direct Elements, Justifications, and Primary Data Collection Activities .... PS-54
Personnel Security Program Lines of Inquiry ................................................................................ PS-59
Personnel Security Assessment Process Matrix ............................................................................ PS-67
Document Request List .................................................................................................................... PS-72
  Overall Personnel Security Topic .................................................................................................. PS-72
  Servicing Personnel Security Organization .................................................................................. PS-77
Pre-employment Check Data Collection Form .............................................................................. PS-79
Clearance Justification Data Collection Form ................................................................................ PS-80
HRP File Review Data Collection Form ......................................................................................... PS-83
HRP Breath Alcohol Test Checklist ................................................................................................ PS-84
HRP Drug Test Checklist ................................................................................................................ PS-87
Methodology for Reviewing Personnel Security Files ................................................................. PS-90
Personnel Security File Data Collection Forms ............................................................................ PS-91
  Derogatory Information ................................................................................................................ PS-91
  Terminations ................................................................................................................................ PS-93
  Clear Cases ................................................................................................................................... PS-95
  Pending Re-investigation .............................................................................................................. PS-96
  Unscrened Files .......................................................................................................................... PS-98
Data Collection Form and Instructions ........................................................................................ PS-101
Report Preparation ........................................................................................................................ PS-102

The following tools and forms may help assessors 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 assessor’s discretion. However, these tools and forms must be tailored for each assessment, 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 assessor through all phases of the assessment 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.
When evaluating the protection of special nuclear material (SNM) by contractor personnel security programs, assessors should focus on how well certain subtopical elements are performing and on confirming that certain compliance requirements are being met. The following baseline list of contractor personnel security program direct and indirect topic elements is intended as an assessment aid. Evaluating these direct and indirect subtopical elements will help ensure the comprehensiveness of assessments or reviews of the personnel security topic.

**Direct subtopical elements:**

- Directly related to the ability of contractor personnel security programs to prevent unauthorized access.

**Indirect subtopical elements:**

- Represent causal factors that could lead or contribute to unauthorized access
- Effective performance of these elements is necessary for sustainment of the personnel security program.

**Personnel Security Clearance Program**

**Direct:**

**General Requirements for Security Clearances:**

- Coordination between the contractor personnel security organization and site badge office regarding the issuance of security badges that allow access to classified matter or SNM only after receipt of notification of clearance approval
- Obtaining security clearances for key management personnel (KMP) or ensuring that KMPs are excluded from access.

**Reporting:**

- Preventing unauthorized access through coordination between the contractor personnel security and human resource organizations and the site badge office regarding individuals whose employment has been terminated or whose position (work) no longer requires access to classified information or SNM
- Preventing unauthorized access by notifying the site badge office of “for cause” security clearance terminations that have been made by the DOE/National Nuclear Security Administration (NNSA) personnel security organization.

**Classified visits:**

- Ensuring that visiting DOE/NNSA or other government agency (OGA) employees are afforded access to classified information or SNM under the protection of a DOE/NNSA contractor only after appropriate actions have been taken to confirm that these employees possess the appropriate security clearances, need to know, and programmatic authorizations.
Indirect:

- Pre-employment checks, confirmation of U.S. citizenship, and not concurrently submitting an employee for a DOE security clearance when the employee possesses a current security clearance authorized by an OGA
- Security clearance request process, types, and justifications
- Maintaining accurate employee clearance status data in the DOE Central Personnel Clearance Index (CPCI) and site personnel security databases (downgrades, clearance administrative withdrawals and terminations, and changes in employment status)
- Reporting potentially disqualifying information, changes in employment status, and administrative termination of security clearance to the servicing DOE/NNSA personnel security organization
- Periodic re-investigation process
- Maintaining the minimum number of cleared employees
- Training of personnel security clearance staff
- Program protocols (including desk-side procedures).

**Human Reliability Program (HRP)**

Direct:

- HRP enrollment process: identification and enrollment of all employees whose work positions require the performance of HRP duties
- HRP annual re-certification process: documented completion of all annual re-certification requirements
- Removal process: supervisor, management official, or certifying official action to prevent employee access and the performance of HRP duties based on the identification of a potentially disqualifying safety or security concern
- Medical assessments: medical officials are expected to determine whether incumbents are medically and psychologically capable of performing their HRP duties, and to report to the management official when an incumbent is no longer capable so that such incumbents are removed from the HRP until resolution of the medical or psychological concern
- Reinstatement process: action by the management official to ensure that reinstatement is fully supported and does not permit an unqualified employee to perform HRP duties
- Eight-hour alcohol exclusion rule: supervisor questioning of workers reporting for unscheduled work and actions to prevent potentially impaired employees from performing HRP duties
- For cause and incident drug and alcohol testing: supervisor or management official action to conduct testing after an incident or based on reasonable suspicion.
Indirect:

- HRP supervisor and employee training
- Knowledge of HRP officials (including medical officials), supervisors, and individual roles and responsibilities
- Reporting of potentially disqualifying medical and psychological conditions to the management official
- Implementation plan and other implementation procedures and protocols (including desk-side procedures)
- Drug and alcohol testing program selection and notification process, testing facilities, technician knowledge, and availability of technicians
- Job task analyses (JTAs).

**Foreign Visits and Assignments Program**

Direct:

- Review and approval of sensitive foreign visits and assignment (FV&A) requests: ensuring that a visit or assignment does not commence or occur before the foreign national’s eligibility for access has been verified and validated
- Review and approval of sensitive FV&A requests: process for ensuring that authorizing access to site computing systems does not permit improper access to or use of computing systems
- Hosts and escorts: improper action by a host or escort that allows an opportunity for unauthorized access (including the failure to notify other employees of the access and work limitations placed on a visiting foreign national).

Indirect:

- Site security plan coverage of FV&As
- FV&A request procedures and protocols
- Content of training material for hosts and escorts
- Documenting and tracking visits and assignments in site and DOE Foreign Access Central Tracking System (FACTS) electronic databases.

**Program Management**

Direct: None

Indirect:

- Adequate resources (personnel and training)
- Contractor security program manager’s involvement
- Personnel security clearance procedures and protocols
- Contractor self-assessment and corrective action programs
- Risk management processes
• Supervisor action in response to incidents of security concern
• Definition and communication of program responsibilities.

**Safeguards and Security Awareness Program**

**Direct:** None

**Indirect:**

• Completion of initial and comprehensive security briefings prior to accessing classified matter
• Conduct of an annual security refresher briefing
• Maintenance of documentation of the completion of all required security briefings
• Security briefing content
• Training of the individual(s) who presents these briefings.
This table aligns the direct contractor personnel security program elements presented above to a justification (impact) for inclusion in the scope of an appraisal activity (assessment or review) evaluating the protection of SNM and classified information as it relates to the prevention of unauthorized access.

<table>
<thead>
<tr>
<th>SUBTOPIC: PERSONNEL SECURITY CLEARANCE PROGRAM</th>
<th>DIRECT ELEMENTS*</th>
<th>JUSTIFICATION/IMPACTS FOR DIRECT ELEMENTS</th>
<th>PRIMARY DATA COLLECTION ACTIVITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Coordination between the contractor personnel security organization and site badge office(s).</td>
<td>- Proper coordination prevents the premature issue (prior to receipt of notification of clearance approval) of a security badge that will allow unauthorized (because the DOE clearance process has not been completed) or improper (due to the wrong clearance level being assigned to an employee) access to classified matter or SNM.</td>
<td>- Compare CPCI listing for recently cleared individuals to site badge issue dates to determine if a security badge was issued prior to the clearance date, and to verify that the correct clearance level badge was issued.</td>
<td>RESOURCES: 1 assessor for 1 day.</td>
</tr>
<tr>
<td>- Obtaining security clearances for KMP or ensuring that KMP are excluded from access.</td>
<td>- Vetting KMP mitigates the potential for improper influence on the protection program.</td>
<td>- Obtain a list of KMP and compare to CPCI records to verify that an appropriate clearance has been granted.</td>
<td></td>
</tr>
<tr>
<td>- Coordination between the contractor personnel security and human resource organizations and the site badge office regarding individuals whose employment has been terminated, whose position (work) no longer requires access to classified information or SNM, or whose clearance has been downgraded.</td>
<td>- Timely coordination (including updating site databases) ensures that employees will be issued a security badge with the appropriate clearance level.</td>
<td>- Review employment termination records and contract records, and compare to the CPCI database to determine if any terminated employees or those who no longer require a clearance still have a security badge.</td>
<td></td>
</tr>
<tr>
<td>SUBTOPIC: HUMAN RELIABILITY PROGRAM</td>
<td>DIRECT SUBTOPIC ELEMENTS*</td>
<td>JUSTIFICATION/IMPACTS FOR DIRECT ELEMENTS</td>
<td>PRIMARY DATA COLLECTION ACTIVITIES</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>- A systematic process must be in place for identifying HRP positions that is consistent with policy and enrolling individuals who will be filling these positions.</td>
<td>- Employees who occupy positions that meet the requirements of 10 CFR 712.10(a)(1-4), but who have not been enrolled in the HRP, are not subject to the continuous evaluation that the HRP provides to ensure that individuals who perform HRP duties meet the highest standards of reliability and physical and mental suitability. Therefore, these individuals may represent a reliability, safety, and/or security concern that could lead to unacceptable damage to specific national security interests.</td>
<td>- Review the HRP Implementation Plan to determine what positions have been identified for enrollment, and compare these positions to those held by HRP incumbents.</td>
<td>- Review recent clearance downgrades to determine if the issued badge reflects the new clearance level.</td>
</tr>
</tbody>
</table>

- Compare CPCI list of recent “for cause” security clearance terminations to site badge records to verify that access is now prohibited.

- Compare a list of recent classified visits with site access control data to determine if access was provided before approval of the classified visit.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documented completion of all annual re-certification requirements</td>
<td>- If all of the re-certification requirements are not completed and documented, an incumbent could be allowed to continue to perform HRP duties with unidentified or unresolved disqualifying safety or security concerns.</td>
</tr>
<tr>
<td>Supervisor, management official, or certifying official action to remove an incumbent based on the identification of a potentially disqualifying safety or security concern</td>
<td>- HRP officials must immediately remove employees when warranted to prevent employees occupying HRP positions from performing HRP duties in a less than reliable and safe manner.</td>
</tr>
<tr>
<td>Medical assessments are designed to ensure that incumbents are medically and psychologically capable of performing their HRP duties.</td>
<td>- Medical officials are expected to determine if incumbents are medically and psychologically capable of performing their HRP duties, and to report to the management official when an incumbent is no longer able to do so to ensure that these incumbents are removed from the HRP until resolution of the medical or psychological concern.</td>
</tr>
<tr>
<td>- Review requests for Category 4 positions to determine if they are adequately justified and approved by the appropriate official.</td>
<td>- Review recent material access area (MAA) access records to identify frequent visitors and determine if the site considered them for enrollment.</td>
</tr>
<tr>
<td>- Review a random selection of HRP files to ensure that all re-certification requirements have been completed as required.</td>
<td>- Request in the data call a list of all individuals who have been temporarily removed (during the assessment period) as a result of the supervisor.</td>
</tr>
<tr>
<td>- Review a randomly selected group of HRP files for timely and appropriate notification and documentation.</td>
<td>- Determine if access (even under escort) was denied to the MAA after removal.</td>
</tr>
<tr>
<td>- Review medical and psychological files and compare the information to the HRP file to determine if information is being shared and actions taken if an individual must be temporarily removed from the program.</td>
<td></td>
</tr>
<tr>
<td>- Reinstatement action by the management official ensures that reinstatement is fully supported by appropriate recommendations and facts.</td>
<td>- The improper resolution of a safety or security concern and reinstatement of an incumbent who still does not meet certification requirements could permit an unqualified employee to perform HRP duties.</td>
</tr>
<tr>
<td>- Implementation of the eight-hour alcohol exclusion rule for unscheduled work</td>
<td>- Supervisor questioning and action of employees reporting for unscheduled work could prevent a potentially impaired employee from performing nuclear explosives duties.</td>
</tr>
<tr>
<td>- For cause and incident drug and alcohol testing: supervisor or management official action to conduct testing after an incident or based on reasonable suspicion</td>
<td>- Drug and alcohol testing for HRP incumbents for occurrences, incidents, and unsafe practices are key components in the HRP process. If testing is not performed as prescribed, there may not be sufficient deterrence to the use of illegal drugs or the abuse of drugs and/or alcohol. HRP employees who are under the influence of drugs or alcohol represent a reliability, safety, and/or security concern that could lead to unacceptable damage to specific national security interests.</td>
</tr>
<tr>
<td></td>
<td>- Request a list of employees who have performed unscheduled nuclear explosives duties and interview the applicable supervisor.</td>
</tr>
<tr>
<td></td>
<td>- Review incident and HRP records to determine if drug or alcohol tests were administered.</td>
</tr>
<tr>
<td>SUBTOPIC: FOREIGN VISITS AND ASSIGNMENTS (FV&amp;As)</td>
<td>DIRECT SUBTOPIC ELEMENTS*</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>- Sensitive FV&amp;A requests must be submitted: ensures that a visit or assignment does not commence or occur before the eligibility for access by a foreign national has been verified and validated</td>
<td>- The FV&amp;A program must be designed to prevent or mitigate unauthorized access to or unintentional disclosure of classified information, sensitive unclassified information, and/or SNM.</td>
</tr>
<tr>
<td>- Review and approval of sensitive FV&amp;A requests: process for authorizing access to site computing systems does not permit improper access to or use of computing systems</td>
<td>- Because nearly all visiting foreign nationals are provided access to a site’s computing systems, care must be used to balance the visitor’s needs versus the need to protect information stored on these systems and the systems themselves from unauthorized use or modification.</td>
</tr>
<tr>
<td>- Hosts and escorts: improper action by a host or escort that allows for unauthorized access (including the failure to notify other employees of the access and work limitations placed on a foreign national)</td>
<td>- As DOE representatives responsible for the activities associated with a visit or assignment, hosts/escorts ensure compliance with the stipulations of the visit or assignee to ensure that there is no unauthorized access.</td>
</tr>
<tr>
<td>- The FV&amp;A program must be designed to prevent or mitigate unauthorized access to or unintentional disclosure of classified information, sensitive unclassified information, and/or SNM.</td>
<td>- Review security incident reports for any that involved unauthorized access or use of site computing systems by a foreign national.</td>
</tr>
<tr>
<td>- The FV&amp;A program must be designed to prevent or mitigate unauthorized access to or unintentional disclosure of classified information, sensitive unclassified information, and/or SNM.</td>
<td>- Review security incident reports to see if any involved unauthorized access by a foreign national visitor or assignee.</td>
</tr>
<tr>
<td>- Compare FACTS data to site badge records for sensitive FV&amp;As.</td>
<td>- Conduct a walking tour of the areas where sensitive FV&amp;As have been conducted to determine if adequate controls or mitigating measures have been taken.</td>
</tr>
</tbody>
</table>

*The essential subtopic elements are directly related to preventing unauthorized access.

NOTE: The assessor may also use additional Data Collection and Analysis Tools from the Personnel Security Assessment Guide to determine why certain negative conditions were identified.
### PERSONNEL SECURITY PROGRAM LINES OF INQUIRY
**PERFORMANCE MEASURE**
**CRITICAL CRITERIA/LINES OF INQUIRY**

**MANAGEMENT:** Does management ensure that the personnel security program represents a logical and cost-effective approach to protecting against the insider threat?

Is senior management support evidenced by proper funding and personnel security program resources, and by support for recommendation to suspend or revoke clearances?

**IMPACT:** Since the human element may represent the weakest link in any protection program and the greatest threat, it is important that management recognizes the significance of an effective personnel security program. This threat is realized through an insider who has authorized access that effectively bypasses some elements of protection systems and who may have extensive knowledge of a facility.

**Management:** Line management responsibility for safeguards and security is exhibited by management’s recognition of the significance of an effective personnel security program.

1. Have self-assessments, surveys, and/or assessments identified systemic deficiencies concerning delays resulting from processing unnecessary clearance requests, minimal participation in the security awareness briefings, and/or lack of proper visitor control?
2. Are there sufficient personnel to avoid an excessive workload for the personnel security specialists?
3. Does the assignment of secondary duties impact 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?
5. Are there sufficient funds in the budget to support retention of adequate staff and for training?

**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 program, desk-side procedures, mentoring, etc.) for preparing new personnel for duties as a personnel security specialist?
### Management
Program direction, plans, and records are supported by personnel security program representatives’ involvement in the development of plans to analyze and mitigate the risk represented by insiders, and/or to determine the level of assumed risk.

Management ensures that personnel security plans, policies, and priorities are adjusted to meet changing threat situations.

<table>
<thead>
<tr>
<th>1. Are personnel security concerns adequately addressed in the site operational and security planning processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>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?</td>
</tr>
<tr>
<td>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?</td>
</tr>
</tbody>
</table>

### Management
Feedback and improvement is supported by effective self-assessment and corrective action programs.

<table>
<thead>
<tr>
<th>1. Has the self-assessment program identified significant program weaknesses that, when addressed, would materially enhance program implementation?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Does the corrective action process include all of 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?</td>
</tr>
</tbody>
</table>

### 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 SNM?

Is the process used to determine eligibility credible and timely?

**IMPACT:** Flaws in the process for determining reliability and trustworthiness undermine the first line of defense against the insider threat.
**Clearance:** The request process (type of clearance) ensures that the type of clearance is appropriate.

1. Is the system in place sufficient to ensure the proper and timely review of clearance requests?
2. Are all of the key elements in place to process requests?
   - Certification that the request is justified?
   - Adequate procedures to ensure that the requested type of clearance is appropriate?
   - A tracking system to ensure that access is terminated when it is no longer needed?
3. Is management support for this process evident?
4. Does the overall number of clearances indicate a lack of control and scrutiny?

**Clearance:** The contractor pre-screening program provides DOE with all identified derogatory information.

1. Does the contractor pre-screening program ensure that all paperwork is complete?
2. Does the contractor pre-screening program eliminate all errors?
3. Does the contractor forward all identified derogatory information to DOE?

**Clearance:** DOE screening and analysis support the action taken (grant, disapprove, or send to Office of Headquarters Personnel Security) concerning a request for clearance.

The contractor badge program ensures that badges are issued only after a clearance is granted and awareness requirements have been completed.

1. Are the results of investigations screened and analyzed in a timely manner?
2. Are the individuals who are charged with the task of completing 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 personnel security files (PSFs) organized in a consistent manner, accurate, and complete?
9. Are procedures in place to ensure that badges are issued only to properly cleared individuals?
| **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. Is there a significant backlog of cases (initial and re-investigations) requiring resolution?  
3. Are there any systemic deficiencies in the administrative review (AR) process?  
4. Are adjudication criteria and procedures consistently applied?  
5. Is the appropriate denial of access (including retrieval of badges) initiated upon notification of suspension of a clearance or notification that a clearance is no longer needed? |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clearance:</strong> DOE is responsible for the timely submission and completion of re-investigations.</td>
<td>1. Is a system in place for the selection of individuals for re-investigation and the completion of these re-investigations?</td>
</tr>
</tbody>
</table>
| **HUMAN RELIABILITY PROGRAM (HRP):** Is the program identifying and enrolling all positions identified in the Site Safeguards and Security Plan (SSSP) to mitigate the threat represented by insiders, thereby providing all of the intended benefits of an enhanced safeguards and security HRP? | Does the system of continuous evaluation identify those individuals who may represent a reliability, safety, and/or security concern?  
**IMPACT:** Weaknesses in this program could lead to unacceptable damage to specific national security interests. |
| **Human Reliability Program:** Plans, policies, and procedures are complete and up to date. | 1. Is there a systematic process for identifying HRP positions that is consistent with policy, and are these positions reflected in the SSSP?  
2. Does the site HRP ensure that individuals 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? |
| **Human Reliability Program:** Reviews and evaluations are completed as required and are comprehensive. | 1. Are all required reviews and evaluations completed before enrolling an individual into the HRP?  
2. Is there a process that ensures that all of the annual evaluations, assessments, and determinations are completed for each individual enrolled in the HRP? |
### 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?

### 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)?
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?

### 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?

### 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?

Has a method been developed to measure the effectiveness of the program?

**IMPACT:** The ultimate effectiveness of the site protection program depends on the actions of all employees. Consequently, a poorly designed and implemented SSAP can have a serious impact.
| Safeguards and Security Awareness Program: Administration and management supports program implementation. | 1. Do program procedures and documentation support full implementation?  
2. Do the parameters of the program include coverage for subcontractors? |
|---|---|
| Safeguards and Security Awareness Program: Briefings are comprehensive and are conducted as a precondition to initial and continuing access. | 1. Is the comprehensive briefing conducted after the clearance has been granted?  
2. Is a security badge permitting unescorted access to a security area issued only after attendance at the comprehensive briefing?  
3. Do briefings contain all required subjects and/or site-specific information, and is the briefing material accurate?  
4. Do all onsite and offsite personnel complete annual refresher briefings?  
5. Are required briefings given to personnel traveling abroad? |
| 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? |
| 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? |
| Safeguards and Security Awareness Program: Coordinator training is evident in the quality of the briefings. | 1. Do the individuals assigned the responsibility to coordinate and present safeguards and security awareness briefings possess the proper skills and knowledge? |
### Safeguards and Security Awareness Program:
Feedback is continuous and leads to program enhancements.

1. Does employee knowledge reflect an effective SSAP?
2. Which feedback mechanisms – e.g., surveys, self-assessments, operations security (OPSEC) programs, questionnaires, tests – provide data (written or verbal) to the program manager?
3. Are the results of these mechanisms analyzed to identify lessons learned or potential enhancements?

### 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 SNM?

**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.

### Foreign Visits and Assignments: Procedures provide a basis for an integrated approach.

1. Does management support of site procedures ensure that visits and assignments are requested in sufficient time to allow all precautions to be taken?
2. Are local policies clear and unambiguous about roles and responsibilities, and do they ensure proper integration and communication 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?

### Foreign Visits and Assignments: Indices checks are used to identify potential risks.

1. Are indices checks completed prior to all visits and assignments that involve foreign nationals from sensitive countries or terrorist countries, that are concerned with sensitive subjects, and/or that include access to security areas?
2. Are counterintelligence (CI) consultations used appropriately in lieu of indices checks?

### Foreign Visits and Assignments: Security plans and coordination ensure the consideration of all security factors.

1. Are all security plans (especially generic security plans) sufficiently detailed to ensure that an inadvertent compromise of security interests does not occur?
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?
3. Do security plans adequately address and control remote access to site computing assets?
4. Do FV&A officials coordinate requests with OPSEC, CI, and export control program officials/subject matter experts?
5. Are foreign nationals permitted access to or use of computing assets?
6. Are foreign nationals provided an appropriate DOE or site security badge?
### Foreign Visits and Assignments: Escort

Escort procedures and training ensure that escorts can effectively meet their responsibilities.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Are escorts sufficiently indoctrinated in their responsibilities, and is there a mechanism to remind them of these responsibilities, especially for long-term assignments?</td>
</tr>
<tr>
<td>2.</td>
<td>Is there a specific training program for escorts (and hosts)?</td>
</tr>
<tr>
<td>3.</td>
<td>Is there a quality assurance process?</td>
</tr>
</tbody>
</table>

### Foreign Visits and Assignments: Host

Host reports support enhancements to the program.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Are hosts fully knowledgeable of their responsibilities concerning submitting a host report at the end of a visit or assignment?</td>
</tr>
<tr>
<td>2.</td>
<td>Do host reports provide sufficient information to detect program weaknesses and to take appropriate action (identify enhancements, conduct investigations, issue infractions, etc.)?</td>
</tr>
<tr>
<td>3.</td>
<td>Are incidents of security infractions reported?</td>
</tr>
<tr>
<td>STEPS</td>
<td>COMPLETION DATE</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>PRE-PLANNING</td>
<td></td>
</tr>
<tr>
<td>Develop an overview of past personnel security program</td>
<td></td>
</tr>
<tr>
<td>issues and concerns by reviewing past assessment</td>
<td></td>
</tr>
<tr>
<td>results and discussing them with team members.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Deputy Assessment Chief and obtain the name</td>
<td></td>
</tr>
<tr>
<td>of the site office and contractor personnel security</td>
<td></td>
</tr>
<tr>
<td>program points of contact.</td>
<td></td>
</tr>
<tr>
<td>Develop the personnel security input for the assessment</td>
<td></td>
</tr>
<tr>
<td>plan topic focus, performance testing, management</td>
<td></td>
</tr>
<tr>
<td>interviews, and potential issues.</td>
<td></td>
</tr>
<tr>
<td>HEADQUARTERS PLANNING MEETING</td>
<td></td>
</tr>
<tr>
<td>In discussion with team members:</td>
<td></td>
</tr>
<tr>
<td>- Confirm topic and subtopic objectives and scope</td>
<td></td>
</tr>
<tr>
<td>- Assign personnel/resources to support data collection</td>
<td></td>
</tr>
<tr>
<td>activities</td>
<td></td>
</tr>
<tr>
<td>- Develop expectations regarding the completion of data</td>
<td></td>
</tr>
<tr>
<td>collection tasks.</td>
<td></td>
</tr>
<tr>
<td>Discuss proposed topic objectives and scope with</td>
<td></td>
</tr>
<tr>
<td>Office Director and Deputy Office Director.</td>
<td></td>
</tr>
<tr>
<td>Refine topic objectives and scope, and tailor the</td>
<td></td>
</tr>
<tr>
<td>document request list.</td>
<td></td>
</tr>
<tr>
<td>Develop topic team schedule. (The schedule is a</td>
<td></td>
</tr>
<tr>
<td>general forecast of activities, not a precise description</td>
<td></td>
</tr>
<tr>
<td>of each day’s activities.)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEPS</th>
<th>COMPLETION DATE</th>
<th>ACTION OFFICER(S)/REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact field points of contact; provide 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 the team will need at the site. Of special importance is that the document request list identifies the lists for PSF reviews, and site sensitive locations and operations to focus FV&amp;A data collection activities.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>Meet with Headquarters topic points of contact to gather information and to discuss data collection activities.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>Prepare a list of additional documentation needed from the site for use before or during the planning meeting and provide to Deputy Assessment Chief; email the request to points of contact.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>Verify initial schedule with team and points of contact.</td>
<td></td>
<td>Team Leader</td>
</tr>
</tbody>
</table>

**ONSITE DATA COLLECTION PHASE**

<table>
<thead>
<tr>
<th>STEPS</th>
<th>COMPLETION DATE</th>
<th>ACTION OFFICER(S)/REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assemble at badge office.</td>
<td></td>
<td>Team</td>
</tr>
<tr>
<td>Attend site security and safety training.</td>
<td></td>
<td>Team</td>
</tr>
<tr>
<td>Attend in-briefing.</td>
<td></td>
<td>Team</td>
</tr>
<tr>
<td>Meet field points of contact, confirm/refine schedule after in-brief.</td>
<td></td>
<td>Team</td>
</tr>
<tr>
<td>Assemble at workspace to conduct topic team meeting to discuss matters as appropriate before the initiation of planning/data collection activities.</td>
<td></td>
<td>Team</td>
</tr>
<tr>
<td>Verify receipt of all requested documents.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>STEPS</td>
<td>COMPLETION DATE</td>
<td>ACTION OFFICER(S)/REMARKS</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
| Collect data  
- Interviews  
- File reviews  
- Performance tests. | | Team |
<p>| Validate data (team will be split, so each team member will validate data as it is collected and then summarize with attending field points of contact when a data collection activity is completed). | | Team |
| Keep Team Leader informed of location and phone number (may be done via admin support personnel). | | Team |
| <strong>Daily</strong>, prepare notes or data collection forms. Notes or data collected on the forms should represent a rollup and <strong>not a verbatim transcription</strong> of an individual’s notes. In this way, the analysis process will be initiated and it should ease preparation of Issue Forms (when required) and the assessment report. | | Team |
| Distribute to Deputy Assessment Chief and Admin Coordinator. | | Team Leader |
| Topic team discusses results of data collection and confirms/revises schedule (should occur briefly before the daily meeting, over the phone if necessary). | | Team Leader |
| As necessary, draft evening bullets. | | |
| *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>
<table>
<thead>
<tr>
<th>STEPS</th>
<th>COMPLETION DATE</th>
<th>ACTION OFFICER(S)/REMARKS</th>
</tr>
</thead>
</table>
| *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  
- Assessment team management has been informed off-line (no surprises). | | |
| Attend daily team meeting. | | Team Leader (team members may be excused) |
| When necessary, finalize evening bullets and provide to Deputy Assessment Chief during the evening meeting. | | Team Leader |
| Conduct end-of-the-day security checks. | | Team |
| Throughout data collection, the team works to:  
- Identify the key results to date  
- Determine the facts that support the key results  
- Revise data collection plan and adjust resources to collect this data. | | Team |
<p>| Subtopic assessors turn in draft sections of the report input to the principal writer. | | Team members |
| Review the draft report input for content and readability and respond to principal writer’s comments. | | Team |
| Identify documents for return to Germantown; return room keys, dosimeters, and pagers; destroy unwanted documents; return supplies; return site documents. | | Team Leader |
| Conduct topic team lessons-learned meeting. | | Team Leader |</p>
<table>
<thead>
<tr>
<th>STEPS</th>
<th>COMPLETION DATE</th>
<th>ACTION OFFICER(S)/REMARKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADDITIONAL ONSITE DATA COLLECTION PHASES, IF REQUIRED</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct topic team meeting on first day of data collection to confirm/refine schedule.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>Collect data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Validate data.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Issues that could impact the topic rating should normally be discussed in the evening meeting only after:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Topic team has reached agreement on the importance of the issue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Integration with other topic teams has been completed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Assessment team management has been informed off-line (“no surprises”).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Same steps as above.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>POST-ASSESSMENT ACTIVITIES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review site factual accuracy comments and incorporate as appropriate.</td>
<td></td>
<td>Team Leader</td>
</tr>
<tr>
<td>Revise Topic Assessment Process Matrix and distribute.</td>
<td></td>
<td>Team Leader</td>
</tr>
</tbody>
</table>
OVERALL PERSONNEL SECURITY TOPIC

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), foreign visits and assignments (FV&A) program, and safeguards and security awareness program (SSAP). This information is to be made available by all appropriate organizations, including the DOE or NNSA site 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 email (address as appropriate).

The following documents and/or information are 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, Office of Security Assessments (EA-22)). If necessary, an alternative method of transmission is an attached file to an email message to: email address as appropriate. Any classified information must be sent to EA-22 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)

Provide 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 (a six-month period—the same six-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 identify 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 access to (site) facilities (including visiting foreign nationals) and from employees who no longer do work that requires access to 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 was initially required by Secretarial memorandum, Decisions regarding drug testing for Department of Energy positions that require access authorizations (Security Clearances), dated September 14, 2007, and is now required in accordance with 48 Code of Federal Regulations (CFR) 952.204-2(h)(2).

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, security area, Protected Area, or non-security area) where the individual’s workspace resides.

3. 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 six-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 Area, Exclusion, or Protected Areas).

b. Separate alphabetized (last name first) listings or computer printouts of FV&As that have occurred between (an appropriate six-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 property protection area, Limited Area, Protected Area, or material access area (MAA)

(4) FV&As involving foreign nationals from terrorist countries

(5) 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

(6) 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

(7) A listing of all visiting foreign nationals who have been granted after duty hours access to any (site) facility

(8) A listing of all security incidents and inquiries that involved either visiting foreign nationals or their hosts/escorts

(9) A list of the most frequently visited site facilities (building or areas) and program organizations.
4. 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 locations.

c. The following separate, alphabetized (last name first) lists for personnel with a Q access authorization. The timeframe for all lists is (an appropriate six-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: (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 the 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 six-month period). If at all possible, the listing should group all of 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 are deemed to be subject to the counterintelligence 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 six-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 scheduled 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 assessment worksite on (specific date of first day of the assessment).

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, 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 corrective action plans.

2. FV&A

a. Procedures and/or protocols used to process and approve all FV&As

b. 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 assessment.

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, Standard Form 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. Local FACTS terminal
   d. Site Safeguards and Security Plan or Site Security Plan as applicable.
SERVICING PERSONNEL SECURITY ORGANIZATION

Personnel Security Clearance Program

The information below is requested to support the personnel security topic team in the subtopical area of the personnel security clearance program. This information is to be made available by all applicable DOE and NNSA personnel security organizations.

Questions should be addressed to (topic team leader), at (301) (as appropriate) or email (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, EA-22). If necessary, an alternative method of transmission is an attached file to an email message to: email address as appropriate. Any classified information must be sent to EA-22 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.)

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

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 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 (letter of interrogatory or LOI, personnel security interview or 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 that resulted in a clear case file determination and required no additional adjudicative actions prior to granting or continuing a clearance.

3. A listing of all re-investigation 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, Occurrence Reporting and Processing System, 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.

7. 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.

8. Intelligence Reform and Terrorism Prevention Act statistical reports for the last six months.
(9) A copy of Office of Personnel Management (OPM) Closed Case Reports (OPM Form 79A) for the previous two quarters.

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

**Personnel Security Clearance Program**

(1) Local/desk-side procedures  
(2) Personnel security files.
# PRE-EMPLOYMENT CHECK DATA COLLECTION FORM

Name: ___________________________ Employer: ___________________________

<table>
<thead>
<tr>
<th>Type of Clearance: DOE Q / L</th>
<th>Other Agency</th>
<th>Prior/Same Employer</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-employment checks completed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Check</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>References Contacted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employers Contacted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Law Enforcement Checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence of US Citizenship</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Birth Certificate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Derogatory Information</td>
<td>DATE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarded to DOE/NNSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Pre-employment Check</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Clearance Request</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forwarded to DOE/NNSA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Comments: ____________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
__________________________________________________________________________________________
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  □ National Security Information (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 (SNM)?
   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 SNM: □ Cat I  □ Cat II  □ Cat III  □ Cat IV

   Identify the **primary** location (building/facility) where you handle 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 the next page of this guide) that is filed in the individual’s personnel security file. The review is intended to determine whether there is consistency between the actual work being performed and the clearance justification/request.]
<table>
<thead>
<tr>
<th>Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Contract Number:</td>
<td></td>
</tr>
<tr>
<td>Last Clearance Justification/Request Date:</td>
<td></td>
</tr>
<tr>
<td>Clearance Level Requested:</td>
<td>Q L</td>
</tr>
<tr>
<td>Requested Clearance Justification Based On Access To:</td>
<td></td>
</tr>
<tr>
<td>Protected Area: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>Material Access Area: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>SNM: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>highest Category: □Cat I □Cat II □Cat III □Cat IV</td>
<td></td>
</tr>
<tr>
<td>Limited Area: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>Security/Exclusion Area: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>Classified Information: □Yes □No</td>
<td></td>
</tr>
<tr>
<td>highest Level: □TS □S □C</td>
<td></td>
</tr>
<tr>
<td>Category(s): □RD □FRD □NSI</td>
<td></td>
</tr>
<tr>
<td>PSYCH</td>
<td>MEDICAL</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>Date(s) of Last Assessment: Initial □ Re-cert □</td>
<td>Date(s) of Last Assessment: Initial □ Re-cert □</td>
</tr>
<tr>
<td>Evidence of access to JTA? □ Yes □ No</td>
<td>Evidence of access to JTA? □ Yes □ No</td>
</tr>
<tr>
<td>Reported Restrictions/Removals?(dates/info)</td>
<td>Evidence of Psych Integration? □ Yes □ No □ NA</td>
</tr>
<tr>
<td>Notifications made:</td>
<td>Current Prescription Medications noted? □ Yes □ No</td>
</tr>
<tr>
<td>Unreported Restrictions/Removals?(dates/info)</td>
<td>Reported Restrictions/Removals?(dates/info)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sec. Concerns? Date Reported?

Notifications made:

Unreported Restrictions/Removals?(dates/info)

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? □ Yes □ No

Is Section C always signed after drug and alcohol testing? □ Yes □ No

Reported Restrictions/Removals?(dates/info)

Notifications made:

Unreported Restrictions/Removals?(dates/info)
**HRP BREATH ALCOHOL TEST CHECKLIST**

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

Name:

<table>
<thead>
<tr>
<th>Name:</th>
<th>Location:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EQUIPMENT AND CHECKS**

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

   (Does the technician know that evidential breath testing (EBT) devices as listed **without** an “*” on the conforming products list must be used?)

2. Does the breath alcohol technician (BAT) 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 one is used.)

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 National Highway Transportation Safety Administration (NHTSA) for approval.]

4. Does the BAT/screening test technician (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 assessment, 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 know what two regulations govern HRP breath alcohol testing? (10 CFR 712 HRP and DOT 49 CFR, Part 40)

   Yes| | No| |

---

PS-84

Appendix A
TESTING PROCESS

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

7. Does the BAT explain the process and complete DOE alcohol testing form (ATF) Step 1?  
   Yes|   | No|   |   |   | [40.241(e) & (f)]

8. If the test result is less than 0.02, are these steps then taken by the BAT/STT?  
   Yes|   | No|   |   |   | [40.247(a)(1)-(2)] Circles “BAT” and “breath” at top of Step 3 on ATF
   Signs and dates the bottom of Step 3 on ATF  
   Transmits ATF original, gives a copy to the employee, and retains a copy.

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

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

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

10. Does the BAT 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)  
    Yes|   | No|   |   |   | [40.243(f)]

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

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

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

ACTIONS FOLLOWING A POSITIVE ALCOHOL TEST

Waiting period

13. Does the BAT instruct the donor that a waiting period of at least 15 minutes is required?  
    Yes|   | No|   |   |   | [40.251.(a)(1)]

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

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

14. Does the BAT inform the donor of the following?  
    During the waiting period, they cannot put anything into their mouth or belch.  
    Yes|   | No|   |   |   | [40.251.(a)(2)(i)]
The reason for the waiting period is 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 |
|-----|----------------|

15. Is the donor observed by the BAT or another employee throughout the entire waiting period?

\[40.251(a)(1)(iii)\]

| Yes | | No |
|-----|----------------|

**Conduct of confirmation test**

16. Does the BAT conduct an air blank in the presence of the employee and show the employee the reading?

\[40.253(a)\]

| Yes | | No |
|-----|----------------|

17. Does the BAT open a new individually wrapped mouthpiece in view of the employee and insert it into the device?

\[40.253(b)\]

| Yes | | No |
|-----|----------------|

18. Does the BAT ensure that the employee reads the unique test number displayed on the device?

\[40.253(c)\]

| Yes | | No |
|-----|----------------|

19. Does the BAT 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 |
|-----|----------------|

20. Does the BAT show the employee the result displayed on the device?

\[40.253(e)\]

| Yes | | No |
|-----|----------------|

21. Does the BAT 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 |
|-----|----------------|

22. If the device does not print the result directly onto the ATF, but on a separate printout, does the BAT 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**

23. Does the BAT sign and date Step 3 of the ATF?

\[40.255(a)(1)\]

| Yes | | No |
|-----|----------------|

24. If the confirmation test was positive, does the BAT direct the employee to sign and date Step 4 of the ATF?

\[40.255(a)(3)\]

| Yes | | No |
|-----|----------------|

25. Does the BAT immediately inform the site HRP management official of the result in a confidential manner?

\[40.255(a)(5)\]

| Yes | | No |
|-----|----------------|

26. Have the BAT and the site 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 |
|-----|----------------|

27. 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: __________________________ 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 that 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 the 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 representative? [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 collection form? [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 remain 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 have no access to any water fountain, faucet, soap dispenser, cleaning agent, or any other materials, which may be used to adulterate the specimen? [8.3(i)]
   Yes |   | No |   |

16. Is a new specimen collection container 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-ounce 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 collection form, notifies the designated representative, and sends copies of the collection form to the medical review official (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 temperature is in the acceptable range (90-100 degrees), the specimen is discarded and a second specimen is collected. The donor is given a reasonable amount of liquid (8-ounce glass of water every 30 min - not to exceed 40 ounces over a period of 3 hours). If the 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 collection form to the MRO and the site HRP management official.

NOTE: Whenever a donor is unable to provide a sufficient amount of urine, a medical examination must be performed to determine whether 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)?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

Does the collector understand that both specimens must be forwarded for analysis?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

21. After a good specimen has been provided and submitted, is the donor instructed to wash his/her hands?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

22. Do the donor and the collector keep the specimen bottle in view at all times prior to it being sealed and labeled?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

23. Does the collection site person securely place a tamper-evident seal/label on the specimen bottle with the date?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

24. Does the donor initial the tamper-evident seal/label on the specimen bottle?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

25. Is the donor asked to read and sign a statement on the collection form certifying the specimens identified were collected from him or her?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

Does the collector understand that if the donor refuses to sign this statement that the refusal must be documented on the collection form?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

26. Does the collector ensure that the required information is entered on the Federal chain of custody form?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

27. Does the collector seal the specimens (bottle A and bottle B) and chain of custody form in a package as specified on the collection form?

<table>
<thead>
<tr>
<th>Yes</th>
<th></th>
<th>No</th>
<th></th>
</tr>
</thead>
</table>

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?
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 the right side (first volume) of the file; use the date stamped on the 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 OPM Form 79A was removed and returned after completion of clearance actions related to a BI for Federal employees.
## PERSONNEL SECURITY FILE DATA COLLECTION FORM: DEROGATORY INFORMATION

<table>
<thead>
<tr>
<th>1. Name/File Number</th>
<th>2. Site/Employer &amp; Work Location</th>
<th>3. Job Title/Position</th>
<th>4. AA Status</th>
<th>5. High-risk Program Status</th>
<th>6. Pre-employment Check Documented</th>
<th>7. Justification Adequate</th>
<th>8. Date Most Recent BI or partial BI (if last investigation) received</th>
<th>9. Most Recent BI Screened</th>
<th>10. Identification and Resolution of Derogatory Information [beginning with the most recent issue(s)]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CRITERIA OF ALL DEROGATORY INFORMATION

**CASE EVALUATION SHEET (CES) IDENTIFYING the MOST RECENT issue(s) Date: Analyst:**

<table>
<thead>
<tr>
<th>Criteria:</th>
<th>Criteria:</th>
</tr>
</thead>
<tbody>
<tr>
<td>↑ (major) or ↓ (minor)</td>
<td>↑ or ↓</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>≤ 5 years or ≥ 5 years</td>
</tr>
</tbody>
</table>

**Initial Additional Adjudicative Action:**

- LOI
- PSI
- PE
- CI
- AR

**Date Recommended:**

**Date Approved:**

**Date Completed:**

**ACTION TAKEN AND DATE OF ACTION**

<table>
<thead>
<tr>
<th>G</th>
<th>C</th>
<th>S</th>
<th>D</th>
<th>N</th>
</tr>
</thead>
</table>

**Second Additional Adjudicative Action**

**CES date:**

**Analyst:**

**Date Recommended:**

**Date Approved:**

**Date Completed:**

**ACTION TAKEN AND DATE OF ACTION**

<table>
<thead>
<tr>
<th>G</th>
<th>C</th>
<th>S</th>
<th>D</th>
<th>N</th>
</tr>
</thead>
</table>

**Third Additional Adjudicative Action**

**CES date:**

**Analyst:**

**Date Recommended:**

**Date Approved:**

**Date Completed:**

**ACTION TAKEN AND DATE OF ACTION**

<table>
<thead>
<tr>
<th>G</th>
<th>C</th>
<th>S</th>
<th>D</th>
<th>N</th>
</tr>
</thead>
</table>

**Fourth Additional Adjudicative Action**

**CES date:**

**Analyst:**

**Date Recommended:**

**Date Approved:**

**Date Completed:**

**ACTION TAKEN AND DATE OF ACTION**

<table>
<thead>
<tr>
<th>G</th>
<th>C</th>
<th>S</th>
<th>D</th>
<th>N</th>
</tr>
</thead>
</table>

**Fifth Additional Adjudicative Action**

**CES date:**

**Analyst:**

**Date Recommended:**

**Date Approved:**

**Date Completed:**

**ACTION TAKEN AND DATE OF ACTION**

<table>
<thead>
<tr>
<th>G</th>
<th>C</th>
<th>S</th>
<th>D</th>
<th>N</th>
</tr>
</thead>
</table>

**Complete for each additional CES developed as a result of the adjudicative actions that were required to resolve this issue.**

---

**PS-91**

**Appendix A**
<table>
<thead>
<tr>
<th>CRITERIA:</th>
<th>RESOLUTION METHOD:</th>
<th>ACTION TAKEN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: Acts of Treason</td>
<td>LOI: Letter of Interrogatory</td>
<td>G: Grant</td>
</tr>
<tr>
<td>B: Association</td>
<td>PSI: Personnel Security Interview</td>
<td>C: Continue</td>
</tr>
<tr>
<td>C: Membership</td>
<td>PE: Psychiatric Evaluation</td>
<td>S: Suspend</td>
</tr>
<tr>
<td>D: Overthrow of Government</td>
<td>CI: Counterintelligence Review (when applicable)</td>
<td>D: Deny</td>
</tr>
<tr>
<td>E: Foreign Influence</td>
<td>AR: Administrative Review</td>
<td>N: None Taken</td>
</tr>
<tr>
<td>F: Falsification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G: Violation of Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H: Emotional, Mental Disorders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I: Refusal to Testify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>J: Alcohol Consumption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>K: Use of or Trafficking in Illegal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L: Personal Conduct/Finance</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11. Was consideration of applicable mitigating factors documented*?  
☐ Yes  ☐ No

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

12. For a Federal employee, was OPM Form 79A returned after completion of the security clearance determination?  
☐ Yes  ☐ No
**PERSONNEL SECURITY FILE DATA COLLECTION FORM: TERMINATIONS**

|-----------------|----------------|----------------------------------|---------------------------------|----------------------------|----------------------------------------|------------------------------------------------|------------------------------------------------|------------------------|

9. **Summary of Assessor’s Concern:**

10. **Site Response:**

**PSF Review Form**

|----------------|----------------------------------|---------------------------------|----------------------------|----------------------------------------|------------------------------------------------|------------------------------------------------|------------------------|

9. **Summary of Assessor’s Concern:**

10. **Site Response:**

**PSF Review Form**

|----------------|----------------------------------|---------------------------------|----------------------------|----------------------------------------|------------------------------------------------|------------------------------------------------|------------------------|

9. **Summary of Assessor’s Concern:**

10. **Site Response:**
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes___ No___</td>
<td>Yes___ No___</td>
<td></td>
</tr>
</tbody>
</table>

9. Summary of Assessor’s Concern:

10. Site Response:
# PERSONNEL SECURITY FILE DATA COLLECTION FORM: CLEAR CASES

<table>
<thead>
<tr>
<th>PSF REVIEW FORM FOR CLEAR FILES</th>
<th>1. File Number</th>
<th>2. Site/Employer &amp; Work Location</th>
<th>3. Job Title/Position</th>
<th>4. AA Status</th>
<th>5. Pre-employment Check Documented</th>
<th>6. AA Justification Adequate</th>
<th>7. High-risk Program Status</th>
<th>8. Date Most Recent BI or partial BI (if last investigation) received:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>□ Initial/Applicant</td>
<td>□ Yes Date:</td>
<td>□ Yes Date:</td>
<td>□ Yes □ No □ HRP □ SCI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>□ Incumbent</td>
<td>□ No Date:</td>
<td>□ No Date:</td>
<td>□ HRP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>□ Reinstate</td>
<td>□ NA Date:</td>
<td>□ NA Date:</td>
<td>□ SCI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>□ Other</td>
<td>□ NA Date:</td>
<td>□ NA Date:</td>
<td>□ SCI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>□ NA Date:</td>
<td>□ SCI</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Acts of Treason</th>
<th>Violation of Security Requirements</th>
<th>Grant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association</td>
<td>Emotional, Mental Disorders</td>
<td>Continue</td>
</tr>
<tr>
<td>Membership</td>
<td>Refusal to Testify</td>
<td>None Taken</td>
</tr>
<tr>
<td>Overthrow of Government</td>
<td>Alcohol Consumption</td>
<td></td>
</tr>
<tr>
<td>Foreign Influence</td>
<td>Use of or Trafficking in Illegal Drugs</td>
<td></td>
</tr>
<tr>
<td>Falsification</td>
<td>Personal Conduct/Finance</td>
<td></td>
</tr>
</tbody>
</table>

12. Was consideration of applicable mitigating factors documented*?

| ☐ Yes  ☐ No |

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

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

| ☐ Yes  ☐ No |

### Analyst Information

Analyst: Date:

---

PS-95
Appendix A
PERSONNEL SECURITY FILE DATA COLLECTION FORM: PENDING RE-INVESTIGATION

<table>
<thead>
<tr>
<th>PSF REVIEW FORM FOR PENDING RE-INVESTIGATIONS</th>
<th>1. File Number</th>
<th>2. Site/Employer &amp; Work Location</th>
<th>3. Job Title/Position</th>
<th>4. Pre-employment Check Documented? (☐ Yes ☐ No ☐ NA (if employment began more than 5 years ago))</th>
<th>5. AA Justification Adequate (☐ Yes ☐ No) Date: ☐ NA (if employment began more than 5 years ago)</th>
<th>6. High-risk Program Status (☐ Yes ☐ No ☐ HRP ☐ SCI)</th>
<th>7. Date Re-investigation Submitted Received</th>
<th>8. Date of EA-22 File Review</th>
<th>9. Date Next Most Recent Previous BI Screened Analyst: Date:</th>
</tr>
</thead>
</table>

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

12. Did the investigation report identify any new derogatory information? (☐ Yes ☐ No)

If so, indicate the applicable criteria: (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].)

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

PS-96
Appendix A
13. Site’s subsequent review (after identifying pending status in the data call) of the re-investigation report:

<table>
<thead>
<tr>
<th>Date Reviewed:</th>
<th>Analyst:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjudicative Action Taken:</td>
<td>LOI</td>
</tr>
<tr>
<td>Date Action Recommended:</td>
<td>Date Approved:</td>
</tr>
<tr>
<td>Final Action Taken:</td>
<td>Grant</td>
</tr>
<tr>
<td>Date Final Action Taken:</td>
<td></td>
</tr>
</tbody>
</table>

14. Summary of Assessor’s Concerns
### PERSONNEL SECURITY FILE DATA COLLECTION FORM: UNSCREENED FILES

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Identification of Derogatory Information Contained in Unscreened Report</td>
<td><strong>CRITERIA OF NEW/UNRESOLVED DEROGATORY INFORMATION CONTAINED IN THE UNSCREENED REPORT</strong></td>
<td><strong>CRITERIA OF PREVIOUSLY IDENTIFIED DEROGATORY INFORMATION CONTAINED IN THE UNSCREENED REPORT</strong></td>
<td><strong>RESOLUTION METHOD(s)</strong></td>
<td><strong>ACTION TAKEN AND DATE OF ACTION</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria A, Acts of Treason ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria A, Acts of Treason ↑ or ↓ ≤ 5 years or ≥ 5 years A:</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria B, Association ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria B, Association ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria C, Membership ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria C, Membership ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria D, Overthrow of Government ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria D, Overthrow of Government ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria E, Foreign Influence ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria E, Foreign Influence ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria F, Falsification ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria F, Falsification ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>□ Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ Criteria G, Violation of Security Requirements ↑ or ↓ ≤ 5 years or ≥ 5 years</td>
<td>□ LOI □ PSI □ PE □ CI □ AR</td>
<td>□ G □ C □ S □ R □ N</td>
<td>Date:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria H, Emotional, Mental Disorders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria I, Refusal to Testify</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria J, Alcohol Consumption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria K, Use of or Trafficking in Illegal Drugs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criteria L, Personal Conduct/Finances</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### B. NEW DEROGATORY INFORMATION IDENTIFIED DURING SITE REVIEW OF A PREVIOUSLY UNSCREENED REPORT

<table>
<thead>
<tr>
<th>CRITERIA OF NEW DEROGATORY INFORMATION CONTAINED IN THE PREVIOUSLY UNSCREENED REPORT</th>
<th>RESOLUTION METHOD(S)</th>
<th>ACTION TAKEN AND DATE OF ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria A, Acts of Treason</td>
<td>LOI [PE [CI [AR</td>
<td>N: None/Pending</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria B, Association</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria C, Membership</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria D, Overthrow of Government</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria E, Foreign Influence</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria F, Falsification</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria G, Violation of Security Requirements</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria H, Emotional, Mental Disorders</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria I, Refusal to Testify</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria J, Alcohol Consumption</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria K, Use of or Trafficking in Illegal Drugs</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
<tr>
<td>Criteria L, Personal Conduct/Finances</td>
<td>LOI [PE [CI [AR</td>
<td>G: Grant</td>
</tr>
<tr>
<td>≤ 5 years or ≥ 5 years</td>
<td>Date Approved: Date Completed: Date:</td>
<td></td>
</tr>
</tbody>
</table>

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

**ACTION TAKEN:**
- G: Grant
- S: Suspend
- N: None/Pending
- R: Revoke

---

**PS-100**

Appendix A
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 (e.g., PSC pre-employment checks, HRP supervisor, incumbent questionnaire), and provide a one-phrase or one-sentence conclusion.

(U) Results: (Bullet statements of strengths and weaknesses.)

Strengths: (U)

Weaknesses: (U)

Narrative: (U) (Briefly summarize all of the data collected on a subtopic or on an aspect of a subtopic. This is not a verbatim account of data collection results. Identify findings using the standard format and include the appropriate reference(s).)

System Description: (U) (Describe the organization [identification of organization(s), number of staff, and training] that has the responsibility to implement this subtopic or subtopical element, and all supporting procedures, including whether the procedures are up to date and comprehensive.)

Implementation: (U) (Assessment of effectiveness of each major subtopic process/element’s effectiveness.)

- (first major 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.
REPORT PREPARATION

Although the personnel security team currently only provides input to the protection program management team’s principal writer during physical security assessments, the following steps will be used when there is a need to prepare a separate 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, in the form of notes or 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 Data Collection Phase(s) (Report preparation will occur during the last 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 the introduction section and any sections that have completed data collection activities (work on the report may begin earlier in the week).

- Friday: All other subtopical inputs are due to the principal writer by close of business.

- Saturday: Finalize the draft report; team reviews report for content, and one team member proofreads the report.

- Monday: Conduct final proofreading and correction prior to submission to the Quality Review Board.