Department of Homeland Security
Office of Inspector General

The DHS Personnel Security Process

OIG-09-65

May 2009

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

May 7, 2009

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of the department's personnel security program. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents

Appendixes

Table of Contents

Acronyms and Abbreviations

CBP	Customs and Border Protection
CFR	Code of Federal Regulation
CHCO	Chief Human Capital Office
OCSO	Office of the Chief Security Officer
DAE	disaster assistance employee
DHS	Department of Homeland Security
DNI	Director of National Intelligence
EOD	entry-on-duty
e-QIP	*electronic* Questionnaire for Investigative Processing
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FTE	full-time equivalent
HR	human resources
ICE	Immigration and Customs Enforcement
IRTPA	*Intelligence Reform and Terrorism Prevention Act of 2004*
ISMS	Integrated Security Management System
JRT	Joint Reform Team
MD	Management Directive
NAC	National Agency Check
NACI	National Agency Check with Inquiries
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PAC	Performance Accountability Council
PD	position description
PerSec	Personnel Security Office
PO	Program Office
PSD	Personnel Security Division
SECCEN	United States Coast Guard Security Center
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

This report assesses the effectiveness and efficiency of the Department of Homeland Security's personnel security programs. At the creation of the Department of Homeland Security, the Office of Security was given oversight of component personnel security programs. In 2005, the Office of Security, Personnel Security Division, was instructed to develop departmental personnel security policies and procedures. Department of Homeland Security Management Directive 11080 requires components to collaborate, participate, and recognize the shared, related, and interdependent responsibility to provide effective and efficient personnel security services to the department.

Department of Homeland Security personnel security offices are performing similar functions but use different policies throughout the personnel security process. Across the department, components strive to provide quality results in a timely manner but often are delayed by applicants, overwhelmed by customer service requests, restricted by database functions, and limited by information availability. The personnel security process is complicated. Application of reciprocity requires unification of Department of Homeland Security financial criteria, combination of temporary hiring requirements, and standardization of adjudication training. Further, department personnel security programs would benefit if better relationships could be established between the Office of Personnel Management and the Department of Homeland Security Chief Human Capital Office. The Department of Homeland Security personnel security program could be made more efficient and effective by consolidating the personnel security intake process, standardizing personnel security policies, and establishing better relationships.

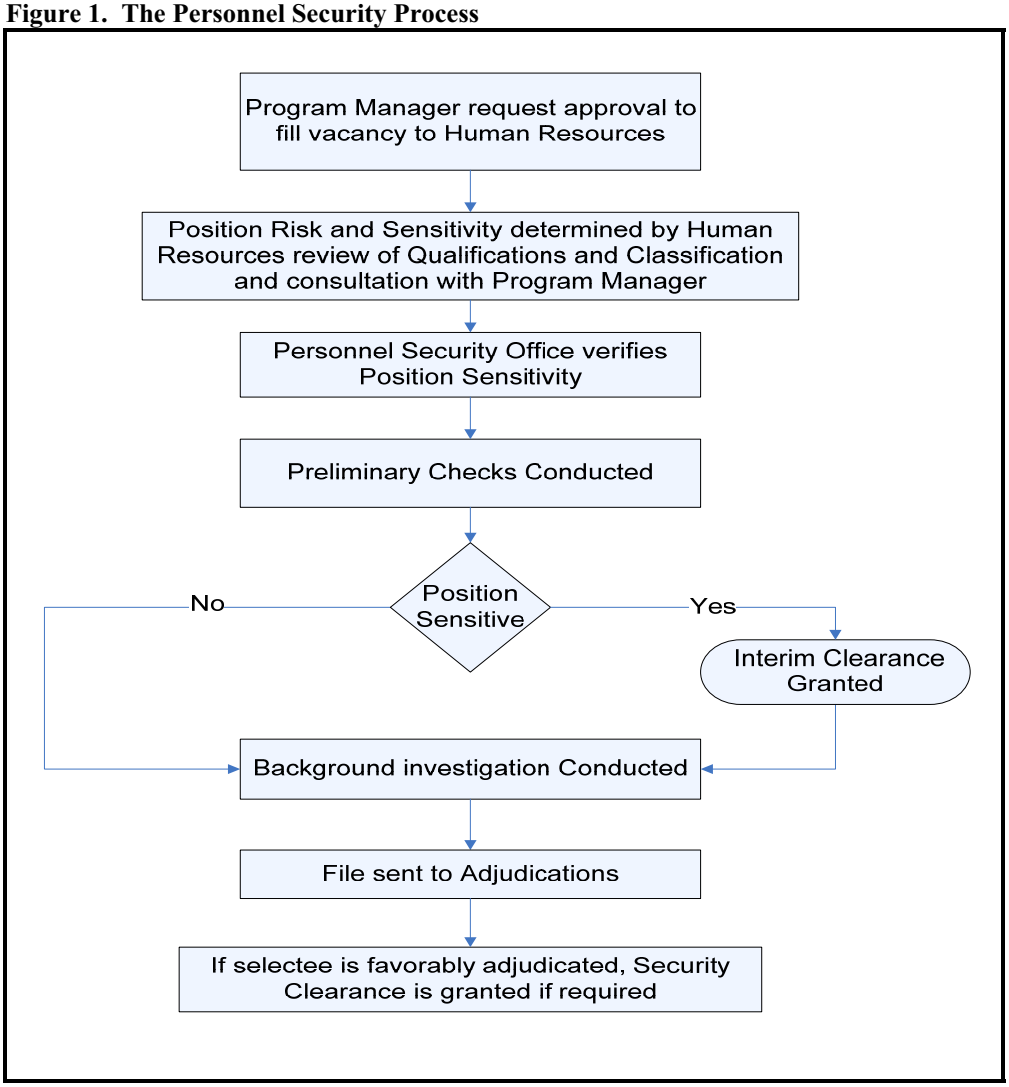
We are making 20 recommendations to improve the Department of Homeland Security's personnel security process.

Background

Overview of Personnel Security

All federal government positions require a risk and sensitivity designation. The highest level of risk or sensitivity determines the type of background investigation required. The greater the risk or sensitivity inherent in the position, the more extensive a background investigation is required. Once designations are made, the background investigation can be initiated and reviewed for suitability. With a favorable suitability determination, an applicant can be hired. Figure 1 illustrates the general personnel security process.

Figure 1. The Personnel Security Process



Source: OIG, derived from multiple sources.

Risk Designation

Risk designation is based on an evaluation of the potential adverse effect that a position may have on an agency. As a result, position risk designation guides the personnel security process. Personnel security specialists closely review the position description (PD), a written statement of the major duties, responsibilities, and supervisory relationships of the position. Human resource (HR) offices designate the level of position risk as the low, moderate, or high. The risk level corresponds to the appropriate type of background investigation, as shown in Figure 2.

Figure 2. Position Risk and Background Investigation

Position Risk and Background Investigation	
Low Risk	**National Agency Check with Inquiries**
Moderate Risk	**Minimum Background Investigation**
High Risk	**Background Investigation**

Source: OIG, derived from multiple sources.

Position Sensitivity

As shown in Figure 3, position sensitivity determines whether access to classified information is required. Sensitivity is reviewed in addition to risk designation. There are two types of federal government positions: Public Trust and National Security. Public Trust positions may involve policy making, law enforcement duties, or control of financial records, or may demand a significant degree of public confidence in the employee.[1] National Security positions are those in which the employee needs access to classified national security information to perform the duties of the position.[2]

[1] Title 5 Code of Federal Regulations 731.106(b).
[2] Title 5 Code of Federal Regulations 732.102.

Figure 3. The Sensitivity Level Designation

Sensitivity Level Designation	
Non-Sensitive	**No access to classified information**
Noncritical Sensitive	**Access to Secret or Confidential information and may adversely affect overall operations of DHS**
Critical Sensitive	**Access to Top Secret information; investigative duties, involvement with personnel security clearances or boards; or other national security positions that may adversely affect the overall operations of DHS and national security**
Special Sensitive	**Access to intelligence-related Sensitive Compartmented Information, the misuse of which may gravely affect overall DHS operations and national security**

Source: OIG, derived from multiple sources.

The risk and sensitivity designation determines the type of background investigation required. The Office of Personnel Management (OPM) developed the minimum requirements for the scope of the investigations used to grant access to classified information.[3] At any time, if the initial background investigation has not been done at the required level, a new investigation will be required. With approval, an agency may do more than what is required for a basic background investigation on a position, but not less.

Suitability

Risk and sensitivity designations are specific to each position, not to an employee. In contrast, suitability is an evaluation of the fitness the character and trustworthiness of the individual for the position. Suitability adjudication considers *only* an individual's personal conduct. OPM defines suitability as:

> *Identifiable character traits and conduct sufficient to decide whether an individual is likely or not likely to be able to carry out the duties of a federal job with appropriate integrity, efficiency, and effectiveness.*[4]

The suitability determination is a process that subjects employees' personal conduct to evaluation throughout their careers. Suitability is often confused with position qualifications. Qualification determinations are based on the individual's experience, education, knowledge, skills, and abilities, while suitability involves an assessment of past and present conduct. The assessment is

[3] OPM Federal Investigative Notice Letter No. 97-02, July 29, 1997.
[4] OPM Suitability Primer, 2007. www.archives.gov/isoo/oversight-groups/nisp/opm-suitability-primer.pdf.

intended to establish a reasonable expectation that the individual will protect the integrity or promote the efficiency of the agency.

An initial suitability determination includes a preliminary check of credit, name, address, education, and fingerprints to establish whether the applicant can perform the duties without compromising national security or public trust. If an individual successfully clears preliminary checks, the applicant is eligible for an interim security clearance. Interim clearances can be granted pending the completion of the full background investigation and adjudication for the final clearance. If unfavorable information is identified on the application form or during the background investigation, the interim clearance may not be issued or can be revoked. In some agencies, applicants are reviewed multiple times during their probationary period. The full adjudication process examines a sufficient period of a person's life to affirm that the individual is an acceptable risk. Each agency, after reviewing all available information, determines the degree of acceptable risk and judges each case on its own merits. Final determinations remain the responsibility of the hiring agency.

The suitability determination recognizes that there may be adverse elements in an individual's past conduct that would not be relevant to the federal position to which the individual is applying. Incidents of previous bad conduct, such as driving while intoxicated, possessing or using marijuana, or experiencing indebtedness, do not automatically disqualify an applicant for federal employment. These types of incidents may be assessed to determine whether they are sufficient in nature and gravity to result in an unsuitable determination for federal employment in a *particular* position. In fact, even individuals with a criminal conviction can be hired as long as they meet the specific suitability requirements for the particular position. For example, an applicant convicted of battery could be deemed suitable for a clerical position. However, the same applicant might be unsuitable for a law enforcement position that requires the employee to carry a firearm. Adjudicators carefully analyze factors that may mitigate the conduct. The nexus between the conduct and the position is the determinant.

Title 5, Code of Federal Regulation (CFR) Part 731, established factors that are used to make a determination of suitability. Part 732 set forth requirements to determine national security positions. Issues discovered during a background investigation are the basis for disqualification. Adjudicators consider types of conduct that could be incompatible with the core duties of a position. The 10

types of conduct issues shown in Figure 4 can be used to screen candidates.[5]

Figure 4. Type of Conduct Issues

Type of Conduct Issues
Intoxicants
Drug use
Financial irresponsibility
Criminal and immoral conduct
Dishonesty
Disruptive or violent behavior
Employment misconduct, negligence
Firearms and weapons violations
Statutory debarment
Miscellaneous agency-specific requirements

Source: OPM Suitability Referral Chart.

Each issue identified by an adjudicator is assigned a grade between A and D based on seriousness, as shown in Figure 5. Any gradable issue may be considered a basis for determining an individual unsuitable.

Figure 5. Seriousness of Issues

Issue Level	Seriousness	Issue Description
A	**Minor**	**Conduct or issue, standing alone, would not be disqualifying under suitability for any position**
B	**Moderate**	**Conduct or issue, standing alone, would probably not be disqualifying under suitability for any position**
C	**Substantial**	**Conduct or issue, standing alone, may probably be disqualifying under suitability for any position**
D	**Major**	**Conduct or issue, standing alone, would be disqualifying under suitability for any position**

Source: OPM; U.S. Department of Agriculture Graduate School, Suitability Adjudication, Version 2.1.

Suitability determinations are reevaluated periodically. This process is especially important for individuals who have been issued security clearances at the Secret or Top Secret level, as the investigation determines their trustworthiness for continued access to classified information. An updated Standard Form 86 must be completed for the adjudication process. If adverse information,

[5] Some DHS components have additional congressional mandated requirements that must also be considered.

such as excessive bad debt, is discovered in the reevaluation, the adjudicator can make an unfavorable suitability determination. Continuous reevaluation of individuals employed by the federal government ensures that only the most qualified and trustworthy individuals remain employed.

Security Clearance

A security clearance is a determination that a person can access classified information.[6] The decision to grant a security clearance can be made after the final suitability determination. Security clearance determinations are based on the information from preliminary checks, gathered from the background investigation, and evaluated by an adjudicator.[7] Figure 6 lists the three security clearance levels.

Figure 6. Security Clearance Levels

Level	Access to Information	Reinvestigated
Confidential	**Information that reasonably could be expected to cause damage to the national security if disclosed to unauthorized sources**	**Reinvestigation conducted every 15 years**
Secret	**Information that reasonably could be expected to cause serious damage to the national security if disclosed to unauthorized sources**	**Reinvestigation conducted every 10 years[8]**
Top Secret	**Information that reasonably could be expected to cause exceptionally grave damage to the national security if disclosed to unauthorized sources**	**Reinvestigation conducted every 5 years**

Source: OIG, derived from multiple sources.

Employees do not own their security clearance. A security clearance is a privilege granted by the federal government, and it can be revoked at any time if unfavorable information about the employee is discovered. Employees who remain employed but no longer require access to classified information can have their clearances administratively downgraded or withdrawn. If classified access is required again, the clearance can be reissued

[6] Executive Order 12598, Classified National Security Information, April 17, 1995; OPM Federal Investigative Notice Letter No. 97-02, July 29, 1997.
[7] Security clearance eligibility is based on information related to foreign influence, foreign preference, sexual behavior, psychological conditions, or other outside activities.
[8] These requirements may change based on work being conducted at the federal level by the Joint Security and Suitability Reform Team.

provided the background investigation has not expired. Agency clearances are terminated when an employee permanently leaves the agency; however, the new agency may use the background investigation already performed by the former agency to issue a security clearance.

Reciprocity

Reciprocity occurs when an agency accepts a security clearance granted to an individual by a former agency.[9] The concept of security clearance reciprocity has existed for decades. However, because agencies have specific missions, reciprocity can be difficult to achieve. Reciprocity is especially complicated for defense, intelligence, and law enforcement agencies.

Mandated Requirements

Personnel security programs were established in 1953 by Executive Order 10450 and enhanced in 1995 by Executive Order 12968. These orders set the standards for suitability and security clearance processes for the federal government, and the processes were reformed in 2008 by Executive Order 13467. In addition, Title 5 CFR Part 731 and Part 732, as amended, define specific suitability factors that must be considered when adjudicating applicants. The *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) sets goals and timelines for granting clearances, ensuring reciprocity, and establishing an integrated database for completed background investigations.[10] DHS has also developed management directives to implement federal requirements across the department.

Executive Orders Governing Personnel Security

Executive Order 10450 required agency heads to establish effective security programs and set minimum background investigation requirements for federal employment based on risk designation. Executive Order 12958 ensured that certain information related to national interest is maintained through a classification system. Executive

[9] OMB Memorandum, Reciprocal Recognition of Existing Personnel Security Clearances, December 12, 2005.
[10] Public Law 108-458.

Order 13467 reformed the use of reciprocity across the government to ensure cost-effective, timely, and efficient protection of national interests. Exceptions to the reciprocity standard are allowed for certain highly sensitive programs.

United States Code of Federal Regulations

OPM has oversight of federal personnel security programs, including background investigation programs. Its authority is delegated primarily through regulations contained in Title 5 CFR Part 731, "Suitability," and Part 732, as amended, "National Security Positions." Part 731 established the process and procedures for determining suitability eligibility for federal employment, and Part 732 established both the requirements for national security positions and the criteria for adjudicating them.

The Intelligence Reform and Terrorism Prevention Act of 2004

Following the events of September 11, 2001, Congress criticized the amount of time it took to hire federal employees. IRTPA contained specific processing deadlines for completing the personnel security investigation and adjudicatory phases. OPM was designated the central depository for all federal government background investigations and adjudications. OPM developed the electronic Questionnaires for Investigations Processing (*e*-QIP) to manage applicant personnel security information across the federal government.

e-QIP allows federal job applicants to electronically enter, update, and transmit their personal investigative data to the hiring agency. Applicants complete personnel security forms, including the Standard Forms 85 Questionnaire for Non-Sensitive Positions, 85P Questionnaire for Public Trust Positions, and 86 Questionnaire for National Security Positions, through *e*-QIP. Figure 7 describes IRTPA processing requirements.

Figure 7. The 2004 IRTPA Processing Requirements

Phase	December 2006	December 2009
Investigation Completed	**90 days**	**40 days**
Adjudication Completed	**30 days**	**20 days**
Total	**120 days on 80% of all applications**	**60 days on 90% of all applications**

Source: OIG, derived from IRTPA.

Since the implementation of IRTPA, OPM has made two other improvements to background investigation processes: the Clearance Verification System, which shares clearance records among agencies, and Imaging, an electronic document project to reduce paper use. With *e*-QIP,

the three new programs comprise OPM's "*e*-Clearance initiative." As of March 2007, all federal government agencies had signed agreements with OPM to use *e*-QIP for national security clearance investigation requests.

Department of Homeland Security Management Directives

On June 30, 2008, DHS Management Directive (MD) 121-01 assigned authority for DHS security programs to the Office of the Chief Security Officer (OCSO). The directive requires the OCSO to oversee DHS personnel security policies, programs, and standards; deliver security training and education to DHS; and provide personnel security support to DHS components. The directive also established a CSO Council responsible for the development of a departmental security strategic plan, establishment of priorities for the security program, and integration of department-wide security programs.

MD 11050.2 set DHS procedures for designating sensitivity, investigative standards for security clearances, and suitability determinations. The directive defined minimum standards, but did not prohibit additional requirements based on mission criticality. The directive made the DHS OCSO responsible for ensuring the issuance, implementation, and compliance of written policies.

MD 11080 required that component heads support and collaborate with the OCSO. The directive set three procedural guidelines for DHS' security functional integration:

1. Standardization of security policies and appropriate procedures;

2. Continued consolidation and integration of systems supporting DHS' security functions; and

3. Consolidation of organizations that perform the same function.[11]

The DHS Personnel Security Division (PSD) has drafted an *Instruction Handbook on Personnel Suitability and Security Program*. The publication establishes procedures, program responsibilities, minimum standards, and reporting protocols for the department personnel security programs. The instruction also provides information on personnel security authorities and responsibilities, requirements for background investigations, and adjudications.

[11] DHS Management Directive Number 11080.

Results of Review

All full-time DHS employees receive a background investigation and adjudication. Approximately 70,000 of the 208,000 DHS employees occupy positions requiring access to classified information. Some components are responsible for conducting their agency's personnel security functions, but must report to the OCSO. Many components have developed similar processes for initiating the personnel security process, resulting in duplicative efforts throughout the department. The key difference occurs in the application of mission-specific suitability standards during adjudication. A number of personnel security processes throughout DHS could be combined to create a more efficient and effective process. DHS PSD, as part of the OCSO, has the authority to make significant changes to the personnel security process across the department. The establishment of a consolidated DHS personnel security intake process would align personnel security policies and better coordinate key DHS operations.

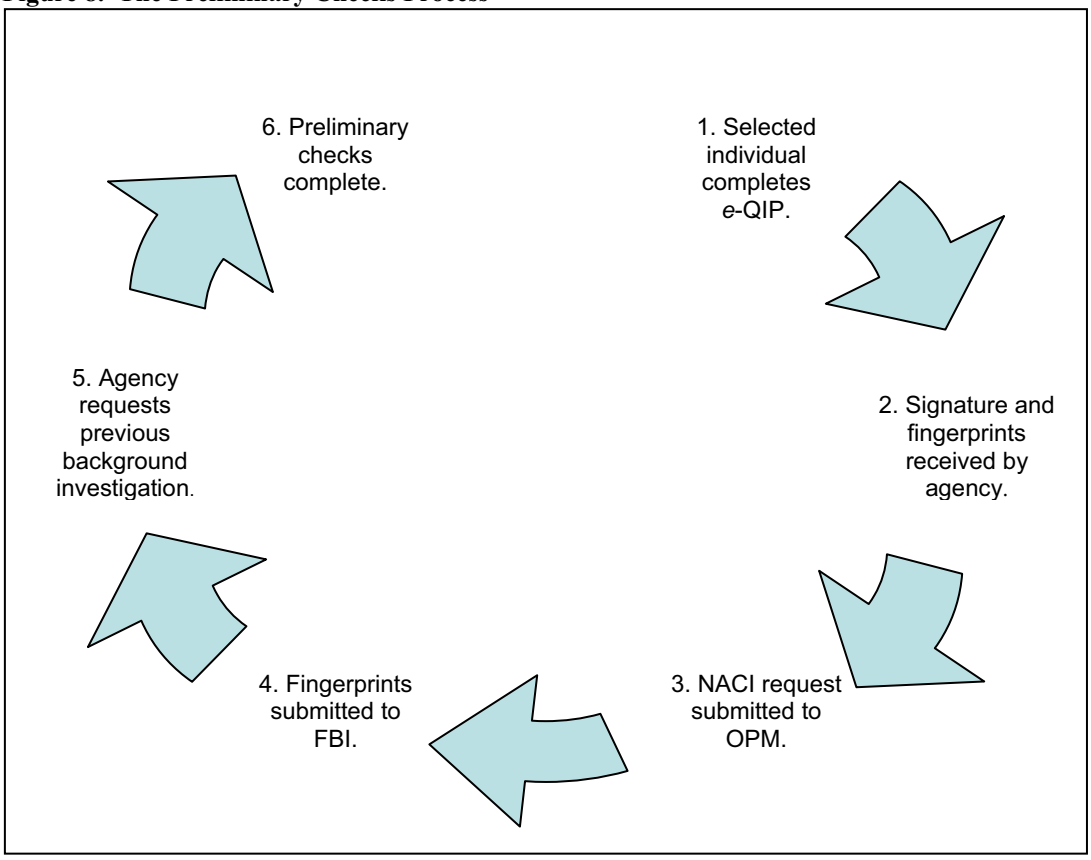
Consolidation of the Intake Process

Across DHS, individuals selected for positions are required to complete *e*-QIP. The *e*-QIP form has consent pages that require the applicant's signature. The pages must be mailed to the agency upon completion of *e*-QIP. Preliminary checks can be conducted once the hiring agency receives notification that *e*-QIP has been completed and receives all documentation.

Preliminary checks are the initial verifications done by an agency to determine whether an applicant meets the minimum hiring requirements. The agency may also conduct other checks if it has the capabilities. If not, the agency can request additional checks when submitting a National Agency Check with Inquiries (NACI) request to OPM. The NACI is a search of investigative files and other records held by federal agencies. The selectee's fingerprints are electronically submitted to the Federal Bureau of Investigation (FBI) for a criminal record check. Components can use the OPM FBI fingerprint check inquiry option, but most submit the fingerprint card directly to the FBI.[12] For applicants who have prior federal service and have had a background investigation conducted in the past 5 years, and whose break in service has not exceeded 2 years, the hiring agency will request the previous investigation. In most components, an interim clearance and entry-on-duty (EOD) date can be issued once a selectee has passed the preliminary checks. The component must be satisfied with results from the preliminary checks since the selectee's background investigation has not yet been fully vetted against the agency suitability standards. Figure 8 illustrates the preliminary checks process.

[12] Requests without an OPM FBI fingerprint inquiry are called National Agency Checks (NAC).

Figure 8. The Preliminary Checks Process



Source: OIG, derived from multiple sources.

Role of the Selectee

DHS personnel security offices agreed that the most time-consuming part of the initiation process involved the selectee. The selectee's responsiveness dictates when the security process can proceed. Some selectees respond immediately, but components noted that others have taken several weeks to respond or fail to respond at all. The average response time for selectees who do submit their forms in *e*-QIP is 10 days.

Some components have developed mitigating strategies to offset delays caused by the selectee. For example, in one component the hiring program manager is notified if the selectee has not completed *e*-QIP in 10 days. By keeping the program manager involved, the hiring agency can withdraw the tentative employment offer if the selectee does not complete *e*-QIP in a timely manner. In another component, the hiring process is discontinued if *e*-QIP is not completed within 30 days. Offices that have developed these types of selectee response strategies have reduced hiring delays.

We recommend that the Under Secretary for Management:

Recommendation #1: Establish a department wide requirement for selectees to complete *e*-QIP within a specified number of days, and develop strategies to manage selectees who do not meet the response requirement.

Customer Service

According to component officials, many selectees have difficulty accessing *e*-QIP or have questions regarding the online system. System access problems can result from technical or user issues. Six of the nine components included in our review have created a customer service group to address selectee questions. Some components have an 800 number, while others use an e-mail system to address customer service questions. *e*-QIP customer service groups answer questions daily about forgotten passwords or failed system access. *e*-QIP problems are not unique to applicants. Often HR offices have issues with *e*-QIP and cannot access the system.

United States Immigration and Customs Enforcement (ICE) has a customer service desk and intake unit responsible for handling customer questions, addressing *e*-QIP issues, filing, and managing training. In June 2008, the ICE intake unit responded to 1,268 phone calls, 2,024 e-mail messages, and 238 walk-in inquiries pertaining to the personnel security process. In the same month, the intake unit received 748 new cases requiring preliminary checks. The Transportation Security Administration (TSA) uses four units Customer Service, *e*-QIP Customer Service, Customer Review, and Scanning and Scheduling to handle internal and external customer questions on status updates or *e*-QIP, manage filing, and schedule investigations. TSA officials estimated that their customer service office receives more than 200 requests each day through e-mail, telephone, and fax. The United States Citizenship and Immigration Services (USCIS) answers all incoming inquiries via e-mail or phone. Inquiries are generally from program managers and selectees on the status of applications. In July 2008, USCIS received 252 calls regarding *e*-QIP, 107 regarding the security process, and 64 regarding applicants who were not selected.

We recommend that the Under Secretary for Management:

Recommendation #2: Delegate all customer service responsibilities to the DHS Personnel Security Division.

Preliminary Checks

Each component we reviewed has an internal division dedicated to processing and collecting selectee information to initiate the preliminary checks. Components with the highest volume of incoming cases were forced to develop intake groups or be overwhelmed. Only three components could determine the number of days it took to process intake functions. Some component officials said their components would benefit from an intake function; however, their organizations do not have the staff or funding to support an intake operation. Personnel security staffs with specialized adjudicator training are instead being used to perform basic clerical tasks such as filing documents, answering phones, and compiling selectee information.

Some components use a standardized intake process. DHS PSD recently reorganized its process to include a centralized intake function. The intake function was designed to initiate *e*-QIP, process forms, and conduct preliminary checks. ICE also aligned current staffing resources to form a standardized intake process. Many personnel security specialists noted that the standardized intake process reduced the time that was previously used to complete administrative tasks. Of all the personnel security offices we examined, ICE is uniquely structured to accomplish the IRTPA requirements.

According to DHS personnel security officials, implementing a consolidated intake function would require significant funding shifts. However, a centralized department-level personnel security intake processing center could also provide DHS PSD with a way to monitor customer service and intake issues across the department. This function could handle all *e*-QIP issues and initiate preliminary background checks (fingerprint submission, credit check, citizenship verification, employment, residency, and Selective Service checks). It could request previous investigative files from other agencies when appropriate. It would provide a complete prehire file to the components for their investigation and adjudication. This integrated customer service effort could improve the efficiency of the personnel security process by streamlining functions, eliminating duplication, improving transparency, and enhancing customer service.

We recommend that the Under Secretary for Management:

Recommendation #3: Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.

Database Functionality

Before 2008, components used individual databases to manage casework because DHS did not have a common data management system. Some components used legacy systems, often proprietary software, while others used commercial off-the-shelf software to build case-tracking capacity and meet individual needs. Figure 9 lists the different systems in use prior to 2008.

Figure 9. The Various DHS Personnel Security Databases

Component	Data System
CBP	Consolidated Tracking System: A proprietary database used to track clearance and investigation requests
FEMA	Automated Personnel Security System: A legacy system used to track background investigations and adjudication determinations
FLETC	Federal Law Enforcement Training Center Clearance Database: A Microsoft Access database used to track background investigation and clearance information. A separate Microsoft database is used to track investigations. Both are legacy databases
ICE	Security Activities Reporting System: A repository for more than 150,000 ICE cases that interfaces with some other DHS systems
PSD	Personnel Security Activities Management System: A system used to automate the tracking and status of security clearance checks and associated activities
TSA	Background Investigation Tracking System: A Microsoft Access database that records and tracks case processing actions
USCG	CHECKMATE: An off-the-shelf system that contains information on the status of all initiated and completed background investigations, to include level of clearance
USCIS	Personnel Security System: A combination of the ICE Security Activities Reporting System and the Security Operations Reporting and Tracking System
USSS	Clearances, Logistics, Employees, Applicants and Recruitment: A headquarters management system to track both human resources and personnel security case processing

Source: OIG, derived from multiple sources.

Increased reporting requirements and tightening timelines caused DHS PSD to develop the Integrated Security Management System

(ISMS).[13] ISMS is an integrated web-based software system that captures data related to all aspects of suitability determinations and security clearance processing. ISMS is an enterprise-wide system for the entire DHS personnel security operation, and has the ability to support administrative security cases, security violation tracking, and secure document tracking.

ISMS is planned to replace the components' separate data systems. As of November 2008, component conversion to ISMS was being completed in phases. ISMS will allow users to share personnel security information on individual cases and aggregate information for statistical and reporting requirements. ISMS will give users the capability to update information, view case status online, and submit case status inquiries, as well as the ability to report on the number of security clearances issued within the department. DHS PSD, under OCSO, will also be better able to monitor submissions under IRTPA. As of November 2008, DHS PSD was using ISMS, and pilot programs had been launched at United States Customs and Border Protection (CBP) and the Federal Emergency Management Agency (FEMA). The United States Secret Service (USSS) and TSA were discussing strategies to integrate their current systems into ISMS.

We recommend that the Under Secretary for Management:

Recommendation #4: Consolidate component security information into ISMS.

File Transfers

Executive orders and OPM regulations require agencies to accept investigations conducted by other federal departments reciprocally. Reciprocity is a process designed to enhance the cost effectiveness of background investigations. However, during fieldwork, DHS component officials complained about the amount of time it took to obtain investigative files within DHS and from other federal agencies. Opinion varied within DHS as to which components took the longest to provide previous background investigations. All components noted the difficulty of obtaining investigative files from law enforcement entities in other federal agencies.

ICE personnel security officials stated that they process most routine requests in 5 days. However, if a file had been archived, processing time could extend to 12 days. FEMA officials stated

[13] ISMS is not related to the Integrated Security Information Management System used by TSA.

that FEMA completes file transfer requests within 7 days. TSA indicated that most file transfers can be completed within hours upon request. USSS processes its file transfer requests in 30 days. The United States Coast Guard (USCG) transfers files within 17 days.

DHS PSD often processed file requests in 1 day. DHS PSD officials noted that the office does not have difficulty obtaining investigative files from other departments or DHS components. Because DHS PSD is part of headquarters and formally recognized by other federal agencies, information from other federal departments is easier to obtain. If DHS PSD was delegated intake responsibility for the entire department, there should be fewer delays in obtaining previous investigative files from other federal agencies and components.

We recommend that the Under Secretary for Management:

Recommendation #5: Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.

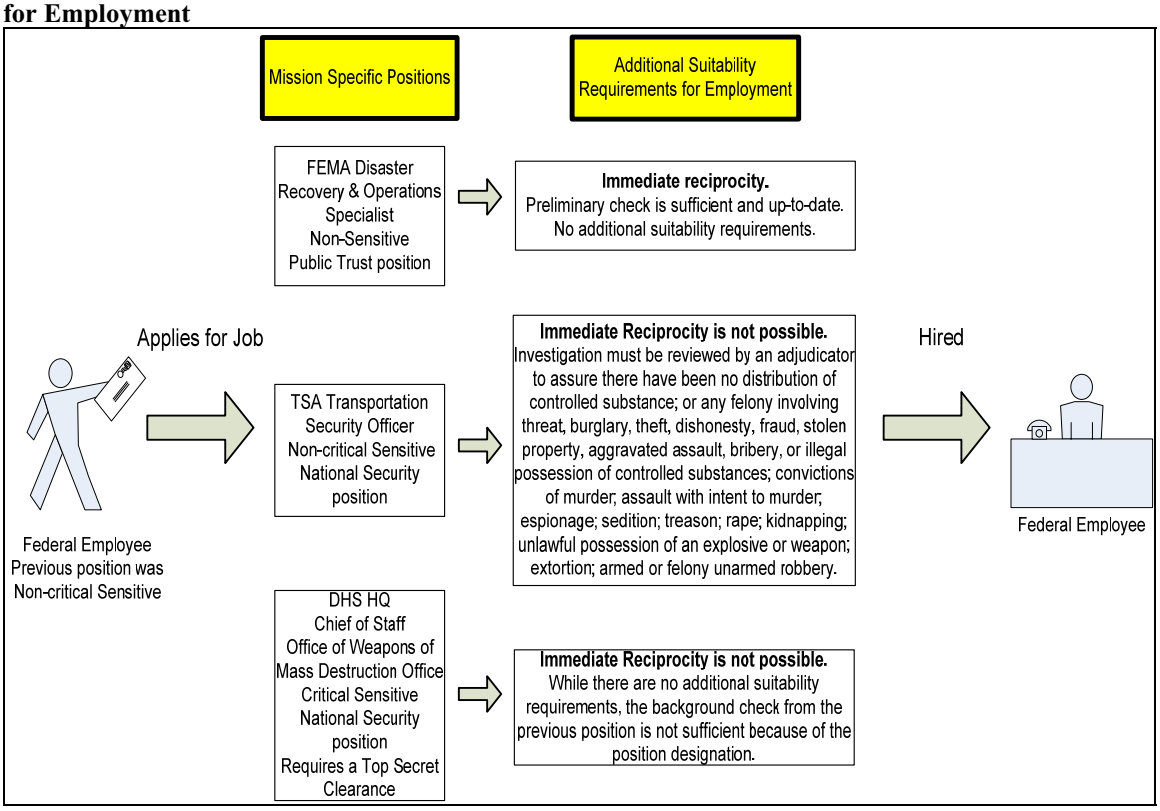
Alignment of Personnel Security Policies

DHS components have been using legacy personnel security policies developed prior to September 11, 2001. Because DHS has not been proactive in developing new security policies, components have developed supplemental guidelines. Component officials would like DHS to standardize several security policies across the department. The alignment of DHS personnel security policies on reciprocity, adjudicator training, bad debt minimums, and temporary employees would solidify the DHS personnel security processes.

Reciprocity Versus Suitability

Figure 10 illustrates three situations where mission-specific suitability requirements and reciprocity may be problematic factors. In the first situation, an employee is transferring to a new position much like the former position. In the second situation, the new position has very different suitability requirements owing to the nature of the work. In the third situation, the new position has higher criticality and sensitivity.

Figure 10. Examples of Mission-Specific Positions and Additional Suitability Requirements for Employment



Source: OIG, derived from multiple sources.

The application of reciprocity arises only in cases where an employee is moving from one federal position to another. Each position has its own risk designation and position sensitivity. The thoroughness of the previous background investigation was based on the risk and sensitivity of the original position. The previous background investigation may not meet the requirements of the new position if the new position has a higher risk or sensitivity level. Although some components do not have additional mission-specific requirements and could easily implement reciprocity, many components have very specific mission needs that must be met.

Applying Suitability Reciprocity

A September 18, 2008, memorandum from the Under Secretary for Management formalized DHS' commitment to implement suitability reciprocity within headquarters. DHS PSD will honor clearances held by employees in DHS components and from other federal agencies when the requirements for position sensitivity and access to classified information are the same. As of October 2008,

DHS PSD was the only component to outline formally how suitability reciprocity was to be applied within its office.

Implementing suitability reciprocity within DHS components will be difficult. The selectee can be evaluated against the specific suitability requirements only once the background investigation is complete. DHS is a national security agency with multiple components, each with its own mission-specific suitability standards based on varied PDs. Following are examples of how suitability affects certain positions:

- CBP Border Patrol agents are responsible for stemming the flow of illegal drugs into the United States. The agency seized more than 800,000 kilograms of illegal drugs in FY 2007. The opportunity for a Border Patrol agent to engage in illegal drug activity is high. Therefore, applicants are considered unsuitable for Border Patrol employment if it is determined that they have ever had any illegal involvement in the cultivation, manufacturing, distribution, processing, or trafficking of any drug or controlled substance.

- USCIS employees administer immigration services and benefits, adjudicate asylum claims and petitions for nonimmigrant temporary workers, issue employment authorization documents, and adjudicate and grant lawful permanent resident status and citizenship. USCIS employees verify U.S. citizenship and status of any immediate family members or adults living with selectees and conduct checks on all foreign-born applicants, relatives, and close associates. The nature of USCIS duties makes it imperative that its employees have no association with illegal immigration activities.

- TSA Transportation Security Officers are responsible for administering airport checkpoints across the United States. Because of their involvement with the flying public, and document and baggage checks, it is imperative the officers have been vetted for theft, burglary, or any interpersonal issues.

- USSS special agents protect national leaders, visiting heads of state and government, and secure national security special events. It is imperative that USSS agents possess the utmost integrity. Although most background investigations do not require polygraph and medical

examinations, USSS requires its selectees to complete these examinations satisfactorily.

To bring efficiency to the personnel security process, Executive Order 13467 clarified suitability reciprocity. The Executive order requires a background investigation for new security clearances, for clearances when the previous investigation is more than 5 years old, or for clearances when the previous investigation is not consistent with the position sensitivity level of the new position. Agencies are permitted to use additional mission-specific suitability requirements, but they must have the approval of either the OPM Suitability Executive Agent or the Security Executive Agent, as appropriate.

We recommend that the Under Secretary for Management:

Recommendation #6: Develop departmental guidance to apply reciprocity as outlined in Executive Order 13467.

Recommendation #7: Designate the DHS Office of Security, Personnel Security Division as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements.

Understanding Suitability Reciprocity

Most program managers are unaware of additional suitability requirements for certain positions. Personnel security offices, especially those with law enforcement responsibilities, must consider additional suitability requirements. From the program manager perspective, a security clearance is simply a background investigation. However, personnel security standards for a component may require additional suitability criteria that cannot be evaluated until a full background investigation is completed.

The personnel security offices understand the program managers' desire to bring selectees on quickly but feel they are being asked to place national security at risk simply to meet hiring requirements. Across components, it was evident that the personnel security offices were committed to ensuring that only fully vetted selectees received a favorable final adjudication.

Component personnel security offices said it would be helpful to train program managers on the personnel security process. A training program that provided an overview of what personnel security is, how suitability is applied, and why extra processing

time is needed in some cases would increase program managers' understanding of the personnel security process. Program manager training on the personnel security process should also reduce the number of customer service inquiries.

We recommend that the Under Secretary for Management:

Recommendation #8: Develop a training program for program managers on the personnel security process.

Financial Disqualifiers

As part of the application process, selectees are asked about their financial record. This includes whether they have had wages garnished or property repossessed, have filed for bankruptcy, or have other unpaid debts. Selectees must explain any delinquencies arising from federal taxes, loans, overpayment of benefits, and other debts to the federal government. They must also report defaults on federally guaranteed or insured loans such as student and home mortgage loans. The standards of ethical conduct for employees of the executive branch states:

> *…employees shall satisfy in good faith their obligations as citizens, including all just financial obligations…especially those such as federal, state or local taxes…that are imposed by law.*[14]

Adjudicators must consider the nexus between the debt, the agency's mission, and the position duties. Life events such as divorce or serious medical conditions that resulted in the accumulation of bad debt can be mitigated. Adjudicators are looking for a demonstrated intent by the selectee to rectify the debt. If the effort is not evident, an adjudicator can determine the selectee to be unsuitable strictly on the presence of the bad debt. The decision is based on the level of risk to national security and possibility that the selectee could be blackmailed or tempted to engage in illegal acts to generate funds.

In setting bad debt criteria, some components linked the financial criteria to specific positions within the agency. Other components established debt ceilings and set a number of months or years after which the selectee must be debt free. These ceilings depended on the sensitivity of the position and included consideration of the security clearance.

[14] Title 5 CFR 2635.

Components use different non-risk based benchmarks to assess a selectee's financial status. For example, CBP reviews individuals with past due debts of $5,000 or more, unpaid judgments, or court-ordered obligations. USCG has established its outstanding debt threshold at $3,000. TSA uses a cumulative delinquent debt of $5,000 or more. Delinquent debt can be (1) any past due accounts that have been sent from a creditor to a collection agency or attorney for action; (2) any unpaid balance that has been reported as a loss to a creditor; (3) a repossession; (4) a court judgment that has not been satisfied; (5) a foreclosure on property or assets; or (6) any debts that have not been dismissed through a bankruptcy agreement. However, the amount of bad debt is not an automatic disqualifier since components use all available information to adjudicate a case. Figure 11 illustrates particular financial debt thresholds required by specific components.

Both FEMA and USCIS want to qualify more applicants. FEMA has increased its acceptable debt limit to $10,000 if the debt is 3 or more years old or $5,000 if the debt is fewer than 3 years old. USCIS raised its debt ceiling from $1,000 to $3,000.

Figure 11. Financial Threshold by Component

Component	Maximum Bad Debt
CBP	**$5,000**
FEMA	**Fewer than 3 years old: $5,000** **Three or more years old: $10,000**
FLETC	**$3,000**
ICE	**120 days or more delinquent: $5,000**
PSD	**$3,500**
TSA	**$5,000**
USCG	**$3,000**
USCIS	**$3,000**
USSS	**All bad debt must be mitigated**

Source: OIG, derived from multiple sources.

Component officials expressed an interest in having a common maximum bad debt threshold across the department. Except for FEMA, the components' maximum bad debt limits are similar. Components should have the latitude to increase the maximum bad debt requirement for their agency. Setting a common financial threshold across the department would facilitate reciprocity for intra-DHS assignments when the selectee's job series and clearance level match the position's requirements.

We recommend that the Under Secretary for Management:

Recommendation #9: Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount.

Temporary Staff and Interns

Temporary DHS employees and interns are generally subjected to less stringent background investigation requirements. There were no DHS standards for processing temporary or intern employees, so components have developed their own standards. Many DHS temporary employees and interns transition to full-time equivalent (FTE) employees at agencies. Inconsistent hiring processes for temporary or intern positions can add time to the hiring process.

While most components require only preliminary checks for interns, some components process interns for secret clearances. The Federal Law Enforcement Training Center (FLETC) processes its student interns and summer hire program employees using a NAC. Requirements for FEMA's disaster assistance employees (DAEs), a category of nonpermanent excepted service employees who are deployed during disasters, are legislated. DAEs do not hold security clearances because of the temporary nature of their disaster relief duties. FEMA vetting requirements for its temporary disaster workers were based on the length of the deployment period. DAEs with service of 180 days or more are vetted in the same manner as full-time federal civilian employees at FEMA. TSA performs a prehire suitability determination on all interns, summer hires, or volunteer personnel. Only if the individual will be returning to TSA for further assignment is the appropriate background investigation conducted. USSS not only conducts a limited background investigation on its student interns but also requires a favorable suitability and security clearance adjudication.

We recommend that the Under Secretary for Management:

Recommendation #10: Set minimum personnel security processing standards for temporary employees in DHS, to include student interns and summer hire program employees.

Adjudication Training

Personnel security adjudicators review the completed background investigation and use appropriate suitability requirements to make a final determination on the character of the selectee. To make a final determination and issue a clearance, the adjudicator must be confident that the selectee does not pose a threat to national security. The ability to make a determination that is sustainable in court is vital to the adjudication position.

The emphasis on adjudication training differs by component. DHS adjudicators receive training online, on the job, or in a classroom. The adjudication courses review adjudication guidelines and personnel investigations, and provide instruction on resolving cases with complex issues.

Each component personnel security office has developed individual adjudicator training requirements. For example, FEMA adjudicators take 24 hours of training online through DHS and other sources. As of July 2008, FLETC requires adjudicators to take a class on fraudulent document detection and complete external training courses. In contrast, ICE has an internal training program that it augments with several external training resources. ICE hosts on-site training sessions for adjudicators and sends adjudicators to the United States Department of Agriculture Graduate School of Management, OPM training sessions, and a 4-hour PSD class. TSA has also developed an in-house adjudication training program. Federal adjudication staff at TSA is required to attend beginning and advanced adjudication training on-site as well as that conducted by OPM. USCIS adjudicators receive training developed and taught by USCIS adjudication supervisors immediately upon assignment to the position. To ensure that those who provide customer services understand the adjudication process, USCIS provides an overview to its administrative support employees.

Since adjudication determinations are subject to review or appeal and may be overturned in legal proceedings, the components must ensure that adjudications are made according to statutory and agency mandates. Unfavorable decisions are made to promote the efficiency of government service, and only after giving the individual due process rights. Unfavorable suitability decisions may be appealed to the Merit Systems Protection Board. Properly documented unsuitable determinations must meet legal standards in order to sustain denial. Many components conduct internal reviews on all denials and other adjudicative decisions to identify

areas where training or procedural changes would enhance adjudication decisions. These reviews usually include staff attorney examinations for legal sufficiency of the adjudicator's written decision to deny the selectee.

DHS OCSO has directed the DHS Training and Operations Security Division to provide training and awareness on mission-based security policies and procedures. The training office has dedicated one FTE to produce personnel security-related training courses for personnel security staffs. Using instruction developed in PSD by adjudicators, the training office has developed courses to address issues such as foreign influence, suitability, types of security clearances, and basic personnel security.

Components provide their adjudicators with the tools necessary to make sound determinations. Several components told us that they had expressed to PSD a desire for a DHS adjudicator training certification program. In light of the Executive order requirements for reciprocity, a formal DHS adjudicator training program would provide assurance to components that DHS adjudicators have been trained to the same standard.

We recommend that the Under Secretary for Management:

Recommendation #11: Develop a formal DHS adjudicator training and certification program.

Coordination of Key Operations

Consolidating the intake function and aligning policies within the personnel security programs would give DHS an identifiable entity to coordinate actions with other federal agency and component personnel security offices. The coordination of key personnel security operations by DHS PSD would give components a single liaison for interaction with OPM. DHS PSD would be better able to work with the DHS Chief Human Capital Office (CHCO) on position designations and staffing needs.

Interaction with the Office of Personnel Management

OPM is the federal government's human resource agency.[15] OPM classifies federal positions according to job duties and

[15] Executive Order 12107, December 28, 1978; *Civil Service Reform Act of 1978* and Section 403 of Reorganization Plan Number 2 of 1978.

responsibilities and contracts with nongovernment providers for background investigations. OPM is responsible for the development of the *e*-QIP program and provides approximately 90% of the investigative services used by all federal agencies.

Delegation of Investigative Authority

In June 2005, OMB assigned OPM responsibility to develop and implement uniform policies for timely completion of background investigations. In turn, OPM authorized a number of federal entities to administer the background investigation process. Currently, DHS components requesting investigative authority must annually submit requests through DHS PSD. DHS PSD consolidates the requests and submits them to OPM. As of September 23, 2008, CBP, PSD, USCG, and USSS were delegated background investigative authority by OMB.[16] ICE, however, has legislated authority to conduct its own background investigations.[17] CBP and ICE contracted background investigations with several private companies. USCG and PSD use a mix of contractor and OPM investigative services. USSS uses internal resources to conduct background investigations, including administering polygraph examinations.

Recommendation #12: Retracted.

The e-QIP *System*

The electronic Questionnaire for Investigations Processing system (*e*-QIP) was designed to electronically capture and transmit personnel security information. The system transmits information that is immediately accessible to eligible users, including the applicant. *e*-QIP eliminates mailing paper forms, and simplifies and automates record keeping. The system was created as one of OPM's early steps in automating the personnel security process. Under *e*-QIP, agencies agreed to submit data and forms for background investigations electronically within 14 days.

Although in existence since 2003, *e*-QIP was not widely used by agencies until 2006, when IRTPA mandated the initial reporting phase for collecting timeliness processing information. In December 2005, DHS was using *e*-QIP to transmit only 6% of its investigations. One year later, DHS transmitted 64% of its background investigations through *e*-QIP. DHS is currently one

[16] OMB Letter to OPM, October 29, 2007.
[17] Public Law 109-90, House Report Number 109-79.

component away from being 100% compliant in *e*-QIP usage. At the time of our fieldwork, that component was negotiating with OPM on system security enhancements.

The *e*-QIP system provides information on the timeliness and accuracy of submissions. DHS components use the information to measure progress and make procedural improvements. DHS security officials said that *e*-QIP improved the overall application process. However, components identified areas of persistent problems with *e*-QIP. For example:

- *e*-QIP data fields are sensitive to small inconsistencies or errors.
- Reportedly, the system frequently returns applications to the applicant without notifying the component.
- *e*-QIP times out and erases applicant records. Some applicants have had to start their application over.
- Contractors do not have access to *e*-QIP, and components using contracted investigators have to print paper copies for investigation.
- Prior to *e*-QIP, the Standard Form 86 was 12 pages. With *e*-QIP, Standard Form 86 is more than 40 pages.
- Errors detected in *e*-QIP are time consuming for components to correct. Neither the applicant nor HR can correct erroneous birthdates or the spelling of a last name.

OPM electronically rejects or returns inaccurate *e*-QIP transmissions to the selectee. When an *e*-QIP submission is rejected, the file images are not viewable and the applicant must reinitiate the process. In some cases components do not have sufficient time to correct an error before *e*-QIP rejects the case. Some components received 10 to 15 rejections each week. Problems with an *e*-QIP submission must be resolved before the investigative phase can commence. When components do not understand the reason for the rejection, they call the *e*-QIP help desk. Component officials told us that they suspect that OPM is inundated with *e*-QIP support requests, but did not know for sure. Some component officials consider the *e*-QIP help desk staff unresponsive. According to these officials, *e*-QIP help desk staff could not explain why a form had been returned. The help desk is manned by contractors and, because of frequent contractor

rotation, it is difficult for components to follow up on cases. The time required to resolve discrepancies results in delays in initiation of the personnel security process.

We recommend that the Under Secretary for Management:

Recommendation #13: Develop a list of department concerns regarding *e*-QIP to share with OPM for resolution.

Investigations

IRTPA required that by 2006, 80% of personnel security investigation requests be completed within 90 days, and that by 2009, 90% be completed within 40 days. Figure 12 shows the average number of days it took the components to complete investigation requirements in 2007 and 2008. Few DHS components meet the IRTPA requirements. We observed that DHS' own contract investigations generally take 90 days or less, but those done for DHS by OPM usually take longer. Figure 12 compares investigation processing times between contractors and OPM by component.

Figure 12. Investigation Processing Times in Days

Contractors			OPM		
Component	**2007**	**2008**	**Component**	**2007**	**2008**
CBP	**97**	**59**	**PSD**	**101**	**67**
ICE	**52**	**39**	**FEMA**	**121**	**94**
USSS	**30–45**	**30–45**	**FLETC**	**Not Available**[18]	
			TSA	**130**	**96**
			USCIS	**110**	**82**
			USCG	**122**	**80**

Source: OIG, derived from multiple sources.

There are mixed opinions among component officials regarding the adequacy and quality of OPM investigations. Some officials said that OPM investigators are inexperienced and may not know the proper questions to ask. Other officials, however, expressed complete satisfaction with OPM investigations. A determination regarding the sufficiency of OPM investigations was not within the scope of our review.

[18] FLETC data are not available because the FLETC Personnel Security Office was not staffed until early 2008.

Components that use contracted background investigation services have stated that the investigations are complete and very thorough. There were few instances when a product was returned for further work; however, products were usually returned within 1 week. Components pay for all investigative services, OPM or contracted.

A number of components expressed interest in negotiating with OPM on the type of information covered in a background investigation. Allowing a single entity like DHS PSD to liaise with OPM on personnel security issues would ensure a balanced approach to issue resolution. Placing DHS PSD in a direct liaison role with OPM would facilitate the delegation of investigative authority and faster resolution of *e*-QIP issues.

We recommend that the Under Secretary for Management:

Recommendation #14: Develop a list of department concerns regarding background investigations to share with OPM for resolution.

Recommendation #15: Designate DHS Office of Security, Personnel Security Division, as the sole representatives to OPM for the components.

Connection to DHS Chief Human Capital Office

DHS CHCO is responsible for all DHS' human resources issues, which include developing performance measures and enterprise human resource systems, training, and recruiting. Component officials described the relationship between the CHCO and DHS components as consultative. Component HR offices noted that the CHCO is understaffed and at a disadvantage in providing needed service. To date, the CHCO Recruitment and Staffing office has not been involved with position designation and classification at the component level. The CHCO does not have the federal staff necessary to coordinate component actions on position designation, a PD library, or workforce projections. Until CHCO can to provide appropriate position designations, a PD library, and workforce projections across the department, personnel security offices cannot function effectively.

Verification of Position Designations

The personnel security process starts when the program manager prepares the PD. In addition to containing a description of job duties, the PD states the sensitivity level of the position. The type

of background investigation that will be required must always correspond to the sensitivity level in the PD. Background investigations for sensitive positions those that require security clearances are usually both costly and time consuming. It is important that the sensitivity levels correctly reflect the duties of the job and be consistent with national security clearance access criteria.

Inaccurate sensitivity levels compromise the personnel security program, increase costs, and lengthen investigation times. On the one hand, if a position's sensitivity is understated, the selectee will be given a less complete investigation. This will result in issuance of an insufficient security clearance, prohibiting the selectee from performing the duties of the position. On the other hand, if a position's sensitivity is overstated, the selectee will undergo a more expensive and protracted investigation than necessary and will receive a security clearance beyond what is required for the position.

HR classifiers determine final position risk and sensitivity designation. Of the components included in our review, only three had classifiers. USSS has a classification branch with five classifiers. USCG has nine classifiers assigned to its HR offices. TSA had multiple classifiers to review position sensitivity. The CHCO has one classifier on staff. USSS, USCG, and TSA use their classifiers to review and validate position sensitivity. Components with classifiers on staff deem the role critical to ensure the proper designation of positions. DHS CHCO officials expressed concern about the absence of department grading standards and instructions for classification of PDs. We were told by the CHCO that a class on how to make position designations was offered to classifiers but only one individual attended.

HR offices without classifiers rely on program managers to certify the accuracy of the position classification. One HR manager said that the classification occupation is perceived as less important than other HR areas. According to personnel security and HR officials, qualified classifiers are difficult to find and were described as a "dying breed." Components without HR classifiers are uncertain who has responsibility for PDs. Personnel security and HR offices observed that program managers frequently do not understand the value of position designation. Many DHS component officials rely on their knowledge of position designation as it applied in legacy organizations. For example, as of August 2008, one component was using criteria developed by the National Aeronautics and Space Administration to establish

position risk and sensitivity designations. Another component was using a Department of Treasury form to classify positions. Others were using the Department of Treasury manual to make position risk and sensitivity designations.

Personnel security officials said that some program managers want to adjust position clearance levels. To hire an employee, some program managers request a low designation, hire the individual, and then resubmit the position for an upgraded security clearance level. Other program managers insist on a higher clearance level to attract or retain an already cleared individual. Personnel security officials said that discussions take place with HR regarding the inappropriate designation levels. The HR office then discusses the matter with the program manager for resolution.

Requests by program managers to upgrade clearance levels without full justification compelled TSA to develop a position sensitivity policy. The policy requires that TSA HR make the final decision. The TSA guidance supplements a DHS personnel security directive, which authorizes the program manager to designate position sensitivity. The DHS management directive states that sensitivity designations are subject to final approval by the organizational element's respective Personnel Security Office.[19] However, the directive does not clearly state the role of the human resource classifier.

DHS CHCO has placed the OPM requirements for position designation online. Some components, like USCIS and TSA, have developed and augmented their websites with information on the position designation and sensitivity process. Component officials would like clarification on making the final position designation.

We recommend that the Under Secretary for Management:

Recommendation #16: Direct component human resource offices to use a qualified classifier as the final decision maker in position designations.

DHS Position Description Library

A PD is the source document that lists the sensitivity designation and indicates to the personnel security officer the level of the security clearance to process. Many HR officials stated that DHS CHCO has not emphasized consistent application of federal

[19] DHS Management Directive 11050.2.

regulations or developed department policies on writing PDs for the components.

The development and use of PDs vary among components. Some HR offices were using legacy PDs to fill vacancies. In other HR offices, program managers would identify a particular individual and then ask HR to write a PD to fit the position. Of all the components, only TSA classifiers reviewed positions whenever there were significant changes in duties or when employees were promoted. Although DHS CHCO has not required components to review old PDs, a departmental review of PDs would more accurately reflect security requirements of DHS' positions. The CHCO should consider a 100% validation of PDs to ensure that sensitivity levels are appropriately designated. The HR community could conduct this task in cooperation with program managers and in coordination with personnel security offices.

Unlike many federal departments, DHS does not have a PD library. A PD library is a collection of description templates and sample standardized PDs that program managers can download, use, and edit. A DHS PD library would simplify the classification process as it would contain standard description of duties, grading, and sensitivity designations for positions or series. A DHS PD library would also enable program managers to review existing PDs.

We recommend that the Under Secretary for Management:

Recommendation #17: Establish and maintain a department position description library of properly designated positions.

Workforce Projections

The CHCO and component personnel security offices need better information about future DHS hiring plans to staff their own offices properly. Personnel security offices cannot determine the appropriate size of their own staff without knowing the demand for services in the coming year. Inadequate staffing at personnel security offices often results in staffing shortages throughout the department. Because DHS CHCO does not collect workforce projections, some components conducted independent studies to determine security office staffing levels.

TSA conducted an internal staffing assessment to identify the best possible realignment of FTEs and contractors. From July to October 2008, TSA's backlog of cases to be adjudicated had grown from 2,000 to 5,000 cases. The average number of days to

adjudicate a case increased from 95 to 147 days. TSA implemented a night surge team and requested the transition of contractor adjudicator slots to full-time federal positions. In 2008, based on the results of the staffing assessment, TSA leadership agreed to provide 11 adjudicative and administrative FTEs to support the workload.

ICE personnel security also conducted a review of the resources needed to meet agency hiring requirements. The personnel security officer required agency offices to submit their projected hiring needs. These projections were reconciled against the agency's attrition rates, and ICE personnel security officials met with agency officials to discuss the cost of processing new hires. Agency leaders were willing to pay for contracted services if new hires could be on board within 60 days. Therefore, ICE personnel security negotiated four contracts for background investigations. Under these contracts, ICE background investigations are completed in approximately 37 days. The quick completion of the contractor-led investigations has allowed ICE adjudicators to issue final determinations more quickly. As of October 2008, ICE can have an individual investigated, adjudicated, and working in as few as 45 days if a case has no significant suitability issues. ICE was the only component that was confident that it could meet IRTPA requirements.

FEMA also completed an internal staffing review to determine the number of additional adjudicators it needed to comply with the 30-day IRTPA requirement. The study validated a need for three additional full-time adjudicators. Although initial funding was not available, as of October 2008, FEMA was in the process of developing a contract to provide administrative support for adjudicators so their primary workload could be adjudications.

Only federal adjudicators can make final determinations. Adjudicator recruiting should be a priority as personnel security adjudication functions are understaffed. Adding contract staff support will expedite some support functions, but only federal employees have the right to adjudicate suitability. Any backlogs caused by caseload exceeding adjudicative capacity can only be relieved by hiring more federal adjudicators. Figure 13 shows the average adjudication processing time among DHS components.

Figure 13. Average Adjudication Processing Time in Days

Component	2007	2008
PSD	37	37
CBP	62	79
FEMA	Not Available	
FLETC	55	37
ICE	45	35
TSA	95	147
USCG	90	17
USCIS	50	59
USSS	Continual Basis	

Source: OIG, derived from multiple sources

Some components' adjudication processing times have increased in the past year due to increased workloads. In June 2008, FEMA had five adjudicators and a backlog of 1,430 cases. By October 2008, FEMA had only three adjudicators, and the number of FEMA cases awaiting adjudication grew to more than 1,900. Since May 2008, PSD has had the capacity to adjudicate 575 cases a month but received an average of 725 cases each month. In October 2008, TSA completed 2,000 cases in 1 month but, because of incoming cases, the backlog remained at 5,000.

Both IRTPA requirements and expectations from program managers have forced personnel security officers to become better organized. However, not all personnel security offices have access to the workforce projections necessary to justify additional personnel security staff. Without accurate projections on FTEs, personnel security offices have a difficult time predicting future workloads or justifying the need for additional staff.

DHS CHCO does not collect workforce projection numbers, which affects components' ability to determine appropriate staffing levels for their own HR and Personnel Security units. With shorter IRTPA timeline standards, personnel security offices must have fully staffed offices. The department's personnel security program cannot be fully successful without CHCO involvement.

We recommend that the Under Secretary for Management:

Recommendation #18: Direct DHS component HR offices to submit workforce projections to the Chief Human Capital Office annually.

Support of DHS Components

At times, components need help with adjudications or guidance on how to meet federal requirements. DHS PSD informally provides adjudicator support to components and consults with components on program changes, and components keep DHS PSD apprised of developing personnel security situations. Further, DHS PSD can provide additional services to the components. Establishing an intake function would help accelerate the administrative processing of cases and would better enable DHS PSD to assist components with unexpected hiring surges and reinvestigation requirements.

Surge Capacity

DHS has experienced some significant yet unforeseen workload increases that may result from new programs or mandated requirements. Program surges significantly affect component personnel security offices. To assist components, DHS PSD provides vital surge capacity.

The President's FY 2008 budget proposal requested $647.8 million to hire 3,000 CBP Border Patrol agents. Subsequently, CBP was inundated with applicants seeking Border Patrol agent positions. To help with the influx, CBP enlisted DHS PSD and USCG's help with adjudicating the investigations. DHS PSD and USCG adjudicators assisted with the CBP workload through voluntary overtime.

FEMA has also used adjudicator resources from DHS PSD. When natural disasters occur, FEMA is responsible for getting a number of temporary employees cleared and to the disaster site in a short time. FEMA has sought and DHS PSD has provided adjudicative assistance in these situations.

In 2008, the National Protection and Programs Directorate was directed to hire an additional 200 employees by the end of the fiscal year. As of September 2008, the directorate was attempting to coordinate hiring efforts with the CHCO to meet the mandate. At the time we concluded our fieldwork in October 2008, DHS PSD had not yet received any of the 200 applications.

Currently, components must develop an agreement with PSD to obtain surge assistance. It is often time-consuming to negotiate the agreements. If PSD had a formal surge adjudicator capacity, it could offer adjudication more quickly through the intake office as a support feature.

We recommend that the Under Secretary for Management:

Recommendation #19: Instruct DHS Office of Security, Personnel Security Division to formalize its provision to components of adjudicator surge capacity.

Reinvestigations

Periodic reinvestigations to assess an employee's continued eligibility for access to classified information are critical to the personnel security process. The type of security clearance held by the employee determines when a reinvestigation is required.

A periodic reinvestigation requires that the employee complete the same forms collected for the initial investigation. Either HR or the personnel security office notifies the employee that a reinvestigation of personnel security is required. Typically, the notification is accompanied by a request that the employee update Standard Form 86 via *e*-QIP. Employees who delay submitting the requested forms delay their readjudication, jeopardizing their continued access to classified information.

With full implementation of ISMS, DHS PSD could oversee the department's reinvestigation process. With more than 75,000 employees maintaining security clearances and the need to reinvestigate every 5 to 10 years, many DHS employees need readjudication. The reinvestigation requirement increases the workload of the components. Under a centralized intake function, DHS PSD could initiate and consolidate component surge requests and reinvestigations.

We recommend that the Under Secretary for Management:

Recommendation #20: Require DHS Office of Security, Personnel Security Division to use ISMS to initiate and track reinvestigation needs for components.

Management Comments and OIG Analysis

The recommendations in this report are made to the Under Secretary for Management. Compliance will require action by the Office of the Chief Security Officer on recommendations 1 11, 13, 14, 15, 19, and 20, and action by the Chief Human Capital Officer on recommendations 16, 17, and 18.

Department management provided a complete and detailed response to our draft report, which we have attached as Appendix B. Though not required, the response includes not only the reply from the OCSO but also comments submitted to that office by USSS, USCIS, CBP, and ICE. Technical comments and corrections were received from CBP, FLETC, ICE, PSD, TSA, USCG, and USCIS. Where appropriate, we made changes to ensure the accuracy of information. As a result of these exchanges of updated information, we removed the recommendation that appeared in our draft report as recommendation number 12. To preserve the sense of the management comments, which were written to respond to the draft, we have not renumbered recommendations 13 20.

We recommend that DHS OCSO exercise the full range of authorities it has been given under MD 121-01 and MD 11050.2. Fulfilling its role will cause PSD, as part of the OCSO, to serve as both a departmental personnel security processing center and a representative for all DHS personnel security issues. PSD should have full awareness of how each component processes personnel security requests and serve as a resource to the OCSO on personnel security operations across the department. This would include standardizing, consolidating, and integrating DHS personnel security functions. We understand that component-level personnel security offices are reluctant to cede to the department many tasks and responsibilities they now perform for themselves, some of which are not substantially component-specific. Nevertheless, components' willingness to continue to perform individually tasks that could effectively be centralized is not, in our opinion, a persuasive reason to accept continuing fragmentation of the department's personnel security customer service processes.

We also identified a number of HR functions the CHCO has not completed that significantly hinder the personnel security process. As these functions are essential to ensuring national security, we encourage the CHCO to undertake remedial action.

Recommendation #1: Establish a department-wide requirement for selectees to complete *e*-QIP within a specified number of days, and develop strategies to manage selectees who do not meet the response requirement.

OCSO Response: OCSO concurred with recommendation #1. In its response, OCSO management said that the CHCO allows each applicant 10 days to complete *e*-QIP after making a tentative job offer. OCSO said that if the

applicant fails to complete *e*-QIP within the required timeframe, the CHCO has the authority to rescind the offer of employment.

OIG Analysis: This recommendation is resolved, open. Managers in components with more qualified applicants than vacancies can feel frustrated when an individual selected for a vacancy fails to complete the *e*-QIP process within the allotted time. Conversely, managers in components with more vacancies than qualified applicants are willing to tolerate such delays. Therefore, we are not recommending that the department arbitrarily impose a 10-day *e*-QIP completion deadline on selectees. We do recommend that the department develop an acceptable baseline, communicate it to selectees, and develop a strategy for dealing with selectee-caused delays. We understand that components need to be able to manage exemptions related to hard-to-fill positions. However, a baseline is important to maintaining efficiency in the personnel security process. The recommendation will remain open pending the receipt of a department-wide policy establishing a baseline for *e*-QIP completion.

Recommendation #2: Delegate all customer service responsibilities to the DHS Personnel Security Division.

OCSO Response: OCSO concurred in part with recommendation #2. In its response, OCSO management said each component has unique characteristics and operating requirements that would make a central customer service office impractical. Furthermore, OCSO management said a central customer service office to address *e*-QIP questions, such as password and golden questions resets, could be a viable alternative following a resource and process analysis.

OIG Analysis: This recommendation is resolved, open. Our report provides a general resource and process analysis that could be used to initiate a department-wide personnel security customer service office administered by PSD. We did not include specific details on implementation of this recommendation, but are concerned that personnel security offices do not fully understand our intent.

We considered several of the component customer service functions as best practices from which the entire department would greatly benefit if uniformly applied. It is possible to use documents already developed by components to implement a customer service function at the department level. It is important that DHS provide consistent customer service on personnel security issues not only to applicants but also to program managers. The recommendation will remain open pending receipt of documentation of implementation plans to develop a department-wide personnel security customer service function for all *e*-QIP responsibilities.

Recommendation #3: Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.

OCSO Response: OCSO concurred in part with recommendation #3. In its response, OCSO management said implementation of this recommendation would require a significant reallocation of resources and space, and a comprehensive study should be conducted to determine feasibility. In addition, input would be needed from the chief information officer and information technology support offices. OCSO noted in its comments that some components did not believe that a centralized intake processing and customer service center would yield the efficiencies cited in the report.

OIG Analysis: This recommendation is unresolved, open. A few components have concerns that implementation of our recommendation could result in a loss of control and initial processing delays. These components have developed their own capable personnel security programs incorporating prehire customer service tasks. Elevating their skills and best practices to a department-wide level would benefit all of DHS. Many smaller components need the resources to address their customer service needs thoroughly. When the tools, documents, and procedures already optimized by some large components are exported to a new, vitalized customer service function at the department level, the smaller components can be among the first to benefit. After the office is established, larger components can incorporate their customer service tasks. The potential value of providing consistent customer service on personnel security issues not only to applicants, but also to DHS program managers, should not be understated. We do not envision removing components' ability to apply mission-specific requirements to their process. We encourage OCSO to consult component processes to develop a department-level personnel security intake processing center. The recommendation will remain open pending receipt of the results of a comprehensive study to determine the feasibility of implementing this recommendation.

Recommendation #4: Consolidate component security information into ISMS.

OCSO Response: OCSO concurred, stating that it is currently merging FEMA and CBP security information into ISMS. FLETC, ICE, and USCG are scheduled for future rollout.

OIG Analysis: This recommendation is resolved, open. We will close the recommendation upon receipt of documentation on the integration of TSA and USSS personnel security information to ISMS and proposed timeframe for completion.

Recommendation #5: Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.

OCSO Response: OCSO concurred with recommendation #5. In its response, OCSO management said the recommendation is being mandated by the Repository Working Group, a subgroup of the Joint Reform Team, which consists of personnel security experts from the Director of National Intelligence (DNI), OPM, OMB, and Department of Defense. The mandate requires all records created by December 15, 2009to be stored in an approved electronic format. The OCSO said that it has taken the appropriate steps to implement the mandate.

OIG Analysis: This recommendation is resolved, open. The Joint Reform Team is working to address issues regarding existing investigative files kept by other agencies. We encourage OCSO to take the lead on this important department-wide issue, and incorporate the responsibility for transferring previous investigation files into the centralized intake processing center. The recommendation will remain open pending the receipt of documentation of a DHS policy to obtain and coordinate interagency and federal department requests for previous investigations.

Recommendation #6: Develop departmental guidance to apply reciprocity as outlined in Executive Order 13467.

OCSO Response: OCSO concurred with recommendation #6. In its response, OCSO noted the Joint Reform Team is developing guidance on application of reciprocity.

OIG Analysis: This recommendation is resolved, open. The Joint Reform Team is working to address this recommendation. We encourage OCSO to develop a department-wide policy on reciprocity. DHS PSD has already developed a policy that could be applied department-wide. The recommendation will remain open pending receipt of documentation of a DHS policy for application of reciprocity.

Recommendation #7: Designate the DHS Office of Security, Personnel Security Division as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements.

OCSO Response: OCSO concurred in part with recommendation #7. In its response, OCSO management said the DHS Chief Security Officer represents all DHS components on personnel security-related issues.

OIG Analysis: This recommendation is resolved, open. In practice, OMB and OPM consider OCSO as the DHS personnel security representative. However, we were not provided any documentation recognizing OCSO as the DHS Suitability Executive Agent or Security Executive Agent. Further consideration

could also be given to designating PSD as the OCSO component liaison on all personnel security-related issues. The recommendation will remain open pending the receipt of documentation indicating that OCSO is the DHS representative authority for personnel security-related issues.

Recommendation #8: Develop a training program for program managers on the personnel security process.

OCSO Response: OCSO concurred with recommendation #8. In its response, OCSO management said the OMB Performance Accountability Council (PAC) has created a subcommittee to address the need to establish standardized training. The OMB PAC will mandate training and certification for all investigators and adjudicators.

OIG Analysis: This recommendation is resolved, open. The OCSO response related to the development of training programs for investigators and adjudicators. In discussion with OCSO managers, we clarified that our recommendation was to develop a training program for program managers the supervisors whose staff vacancies were being filled by the new hires. Some personnel security officials told us that responding to repeated inquiries from managers eager to fill their vacancies was as burdensome as repeat inquiries from selectees. The recommendation remains open pending documentation indicating development of an informational module for program managers.

Recommendation #9: Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount.

OCSO Response: OCSO concurred with recommendation #9. In its response, OCSO management said OCSO is reviewing debt levels in order to develop a proposed ceiling that is acceptable to the department.

OIG Analysis: This recommendation is resolved, open. In discussion, OCSO noted that a memorandum was recently signed implementing this recommendation. We agree that the action OCSO plans to take will satisfy the intent of this recommendation. The recommendation will remain open pending the receipt of the signed memorandum documenting the department-wide bad debt maximum.

Recommendation #10: Set minimum personnel security processing standards for temporary employees in DHS, to include student interns and summer hire program employees.

OCSO Response: OCSO did not concur with recommendation #10. In its response, OCSO management said every agency vets its temporary employees and interns differently. OCSO noted that Title 5, CFR, Section 732 requires an

investigation only after 180 days of employment. Further, OCSO questions the value added to the personnel security process if this recommendation is implemented.

OIG Analysis: This recommendation is unresolved, open. We understand that only employees who serve for more than 180 days are required to be vetted in the same manner as full-time federal civilian employees. However, under the management directives cited in this report, it is the responsibility of OCSO to issue, implement, and ensure compliance with written personnel security policies throughout the department. Our fieldwork identified component personnel security offices that were uncertain what the department required as a minimum for temporary employees. We encourage OCSO to consider using Homeland Security Presidential Directive 12 requirements to establish minimum processing requirements for temporary DHS employees. The recommendation will remain open pending receipt of documentation indicating that a department-wide minimum for temporary employees has been developed.

Recommendation #11: Develop a formal DHS adjudicator training and certification program.

OCSO Response: OCSO concurred with recommendation #11. In its response, OCSO said it provides adjudicator training at an annual security conference and quarterly at DHS adjudicator roundtable meetings. OCSO envisions developing additional adjudicator training to enhance OPM government-wide standards for adjudicator and investigator training and certification.

OIG Analysis: This recommendation is resolved, open. Many components have developed adjudicator training programs that could be modified and certified at the department level. Some components indicated a willingness to assist with development, host a session, or serve as a pilot for such a program. The recommendation remains open pending receipt of documentation indicating that a DHS adjudicator training and certification program is being developed.

Recommendation #12: Retracted.

This recommendation was removed from the final report. DHS officials stated that OPM annually delegates investigative authority to DHS, and DHS is satisfied with OPM's decisions with respect to delegated investigative authority.

Recommendation #13: Develop a list of department concerns regarding *e*-QIP to share with OPM for resolution.

OCSO Response: OCSO did not concur with recommendation #13. In its response, OCSO management said that it had no information suggesting *e*-QIP is not operating smoothly.

OIG Analysis: This recommendation is unresolved, open. As we reported, some selectees and DHS employees have experienced difficulties using the *e*-QIP system. OCSO should validate its assertion that *e*-QIP is operating smoothly by surveying DHS users to identify whether *e*-QIP issues exist within the department. Any issues noted should be conveyed to OPM. The recommendation will remain open pending the receipt of documentation on action taken by OCSO to bring department-wide *e*-QIP issues to OPM's attention.

Recommendation #14: Develop a list of department concerns regarding background investigations to share with OPM for resolution.

OCSO Response: OCSO concurred with recommendation #14. In its response, OCSO management said the office, as part of a working group, is addressing the concerns of this recommendation. As a result, a survey and statistical analysis has been completed.

OIG Analysis: The recommendation is resolved, open. We recognize that OCSO represents DHS regarding personnel security-related issues. However, our fieldwork identified a number of issues at the component level regarding background investigations. As noted in recommendation #3, the department's fragmented approach to personnel security prevents OCSO from always being aware of department-wide issues. The recommendation will remain open pending the receipt of documentation of the survey and statistical analysis conducted, as well as documentation on action taken by OCSO to resolve department-wide background investigation issues.

Recommendation #15: Designate DHS Office of Security, Personnel Security Division, as the sole representative to OPM for the components.

OCSO Response: OCSO did not concur with recommendation #15. In its response, OCSO management said OCSO is a member of OMB PAC and of the DNI Special Security Center, and represents all DHS components on personnel security-related issues. OCSO and the components reported, however, that because each component has unique operational requirements, each must deal directly with OPM on specific case issues. The components want to retain their ability to deal directly with OPM on matters they consider specific to their organizations.

OIG Analysis: This recommendation is unresolved, open. OCSO indicates that it uses various intergovernmental memberships to represent components on personnel security-related issues. Our fieldwork demonstrated that components contact OPM on the same issues. We recognize that components and OPM can quickly resolve some small, day-to-day issues , but the intent of this recommendation was to ensure a balanced approach to issue resolution. OCSO PSD has experienced fewer issues requiring OPM resolution than components. Our fieldwork indicated that the authority of OCSO has enabled PSD to resolve

issues more quickly than components. Designating PSD as the sole representative to OPM for the components could lend additional legitimacy to issues experienced by components and result in quicker resolution. The recommendation will remain open pending the receipt of a memorandum delegating authority to OCSO PSD as the sole representative for components on personnel security-related OPM issues.

Recommendation #16: Direct component human resource offices to use a qualified classifier as the final decision maker in position designations.

OCSO Response: OCSO reports that the CHCO concurred in part with recommendation #16. Its response said that the CHCO would need to establish FTE classifier positions in order to fulfill this recommendation and ensure continuity of operations.

OIG Analysis: This recommendation is unresolved, open. The OCSO response addressed only the matter of adding qualified position classification specialists at the department level, not in the components. Our fieldwork has identified a significant need for qualified classifiers throughout the department to ensure the efficiency of the personnel security process. Without classifiers, positions can be filled using incorrect risk or sensitivity designations. Until this need is met, OCSO should assist in expediting the reallocation of department resources to include detailing experienced classifiers to components without classifiers. The recommendation will remain open pending our receipt of documentation that identifies the number of classifiers required department-wide, the proposed timeline for hiring new classifiers, and acknowledgment that classifiers have been placed in the components.

Recommendation #17: Establish and maintain a department position description library of properly designated positions.

OCSO Response: CHCO concurred in part with recommendation #17. In its response, OCSO management said that at least two teams need to be established to fulfill this recommendation. OCSO proposed an initial team of two classifiers to handle classification of position descriptions, ensuring that OPM guidance is followed. An undetermined number of classifiers on another team would identify the number of PDs to be reviewed and the timeframe of the review. Contractors could be used for administrative support between the two teams and to enter documentation into the newly developed CHCO PD library.

OIG Analysis: This recommendation is unresolved, open. As noted in our report, we determined that some components use classifiers to review PDs. The CHCO should be able to request validated PDs from those components. Further, with implementation of recommendation #16, more components should be able to provide the CHCO with PDs that have been verified by detailed classifiers. These PDs could serve as the beginning of the DHS PD library and should be updated as

components make changes. This approach would reduce workload and use existing departmental resources. More important, it would facilitate quick startup of the PD library. We encourage the CHCO to work with component HR offices and to compile already validated PDs produced by qualified position classifiers. The recommendation will remain open pending receipt of PD templates with clear notation that the classification has been validated.

Recommendation #18: Direct DHS component human resources offices to submit workforce projections to the Chief Human Capital Office annually.

OCSO Response: OCSO concurred with recommendation #18. In its response, OCSO management said the CHCO needs to create a manning roster for each Directorate, by position. In addition, only vacant positions can be filled. It is expected that this will reduce unconstrained hiring.

OIG Analysis: This recommendation is unresolved, open. While we encourage the CHCO to develop and maintain an electronic manning roster for the directorates, the CHCO's proposed action would address only a portion of our concern. Workforce projections need to be obtained for all components, not just the headquarters directorates, and then shared with all personnel security offices. This will aid the department in acquiring sufficient qualified classifiers, adjudicators, and other staff to deal with future hiring activity.

Implementation of this recommendation is essential to ensure appropriate planning and use of resources throughout the department. As the department's human capital office, the CHCO has the authority to plan and execute department-wide policies. We understand that the CHCO has experienced staffing limitations, but our fieldwork indicated that inadequate execution of HR policies can have a detrimental effect on other department programs. We saw this clearly in the personnel security programs. The recommendation will remain open pending documentation that describes the CHCO's efforts to collect workforce projections from the department.

Recommendation #19: Instruct DHS Office of Security, Personnel Security Division to formalize its provision to components of adjudicator surge capacity.

OCSO Response: OCSO concurred with recommendation #19. In its response, OCSO management said that provision for a surge adjudication team was included in the FY 2010 budget but the funding had been dropped. DHS was in the process of appealing the decision.

OIG Analysis: This recommendation is resolved, open. In discussion, OCSO said that the OMB decision to cut funding for a surge adjudication team was being appealed. The OCSO response did not indicate what the surge capacity would be, or how OCSO will overcome budget and operational requirements to implement this recommendation. We endorse the critical need for a surge adjudication team

to vet cleared selectees in a timely manner when department hiring initiatives overwhelm existing personnel security capacity. The recommendation will remain open pending receipt of documentation indicating the final appeal decision.

Recommendation #20: Require DHS Office of Security, Personnel Security Division to use ISMS to initiate and track reinvestigation needs for components.

OCSO Response: OCSO concurred with recommendation #20. In its response, OCSO management said implementation of this recommendation is under way. The first component is scheduled to begin using ISMS to track reinvestigations in April 2009.

OIG Analysis: This recommendation is resolved, open. The action OCSO plans to take will satisfy the intent of this recommendation. OCSO should provide a timeline for inclusion of all components' security information in ISMS, and a consolidated list of projected reinvestigations by component for FY 2010.

Appendix A
Purpose, Scope, and Methodology

The purpose of our review was to examine the department's internal processes and standards for background investigations. This review did not evaluate the DHS personnel security clearance screening process for contractors, appointees, or nonfederal DHS employees. We measured DHS' processing requirements, security clearance investigative authority, agency suitability requirements, clearance update requirements, and the application of reciprocity. Our report is based on interviews with key personnel security officials, human resources employees, and senior DHS officials.

We conducted our fieldwork from June to August 2008. During this period, we received briefings from officials at the Office of Personnel Management and DHS Chief Human Capital Office, and conducted numerous interviews, including interviews with senior DHS Office of Security officials. We met with officials from PSD (which services all but eight of the DHS components) and spoke to officials from the following eight legacy personnel security offices within DHS: (1) United States Customs and Border Protection, (2) United States Citizenship and Immigration Services, (3) the Federal Emergency Management Agency, (4) the Federal Law Enforcement Training Center, (5) United States Immigration and Customs Enforcement, (6) the Transportation Security Administration, (7) the United States Coast Guard, and (8) the United States Secret Service. These offices provided insights into the effectiveness of the DHS personnel security process. We also interviewed department human resources officials and field office staff to learn about classification and hiring processes, and completed a Suitability Adjudications training course offered by the U.S. Department of Agriculture Graduate School.

We studied related laws, regulations, Executive orders, and DHS management directives. We reviewed DHS guidelines and procedures, and analyzed DHS personnel security documents. In addition, we examined Government Accountability Office reports, relevant speeches, congressional testimony, and news articles.

This review was conducted under the authority of the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency.

Office of Security
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 5, 2009

MEMORANDUM FOR: Richard L. Skinner
Inspector General

FROM: Jerry Williams
Chief Security Officer

SUBJECT: Response to Department of Homeland Security, Office of Inspector General Draft Report titled: "The DHS Personnel Security Process – For Official Use Only (FOUO)"

Purpose

This memorandum provides the response to the Department of Homeland Security (DHS) Office of Inspector General (OIG) draft report, "The DHS Personnel Security Process – For Official Use Only (FOUO), January 2009."

Background

The OIG examined the department's personnel security program as part of its overall mandate to "promote economy, efficiency, and effectiveness within the department." It studied this program by conducting interviews with employees and officials, making observations, and reviewing all applicable documents.

The OIG made 20 recommendations designed to enhance the department's personnel security process.

Discussion

The Management Directorate appreciates having the opportunity to review and comment on this draft report. While the report offers some interesting suggestions to modify mental operations, we have noted that there are several inaccuracies when it comes to interpreting established policies, processes and procedures. As one example, on page 2, there is the following statement: "All federal government positions require a risk and sensitivity designation for national security." This is not accurate in that not all positions require a security clearance. The basis for this misconception is likely the confusion between *suitability investigations* and *security clearances*. While these two terms are often thought to be synonymous, they are not. All federal and contract employees must be found *suitable* for employment with DHS. *Security clearances* (i.e., Confidential, Secret, Top Secret) are granted only to employees who have a need to access classified information; the clearance is granted upon completion of an appropriate investigation.

Additional security training is required before the access to classified information is permitted.

As noted in the Background section, the OIG made 20 recommendations that it believed would make the department's personnel security processes operate more effectively and efficiently. The Office of the Chief Security Officer has prepared a set of responses to each of the recommendations. In addition, some components responded with their own set of comments to the recommendations which address their unique circumstances; these responses are attached. These comments can be used as the basis of our conversation on inaccuracies and misunderstandings in the draft report.

The Department would like the opportunity to meet to discuss these items and discuss any misunderstandings. If there are any questions, or to arrange a meeting regarding this report, please contact Mr. Elie D'Amico at (202) 447-5821.

Attachments

cc: Carlton I. Mann
Assistant Inspector General for Inspections

Attachment A

IG Report on DHS Personnel Security Process Recommendations
Personnel Security Division, Office of Security Responses

1. **Establish a requirement for selectees to complete e-QIP within a specified number of days, and develop strategies to manage selectees who do not meet the response requirement.**

   This recommendation has already been implemented. Presently, the Chief Human Capital Office (CHCO) allows each applicant 10 days to complete e-QIP after making a tentative job offer. If the applicant does not complete e-QIP within the required timeframe, CHCO has the authority to rescind the offer of employment.

2. **Delegate all customer service responsibilities to DHS Personnel Security Division.**

   Each component has unique characteristics and operating requirements that would make a central customer service office impracticable. It would be next to impossible for centralized customer service operators to accurately address questions about unique operating requirements and processes of each component.

   However, a central customer service office to address e-QIP questions, password resets, golden questions reset, etc. could be a viable alternative. A thorough resource and process analysis must be conducted before a final decision can be made.

3. **Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.**

   A centralized intake processing center would require a significant re-allocation of resources and space. Before an accurate assessment can be made regarding this recommendation, a comprehensive study should be conducted, addressing current processes of each component, resources allocated for the intake process, budget, and space issues. In addition, a collaborative effort with CIO to provide training and allow IT support to assist all components would be required.

   Various components in DHS have provided the Office of the Chief Security Officer (OCSO) with their own responses to these recommendations. Many do not believe that a centralized intake processing and customer service center would yield the efficiencies cited in the report. Please see attached documents for their individual responses.

4. **Consolidate component security information into ISMS.**

   This is underway; FEMA and CBP are scheduled for implementation in April 2009, and additional components have met with the project team for gap analysis during the past six months. FLETC, ICE, and USCG are scheduled for the next rollout.

5. **Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.**

   This recommendation has already been mandated by the Repository Working Group (RWG), which is a sub-group of the Joint Reform Team (JRT), a team consisting of DNI, OPM, OMB, and DOD, with input from the personnel security community government-wide. The mandate requires that all records created by December 15, 2009, and thereafter, must be stored in approved electronic format. Furthermore, all requests for security files must be sent via electronic format within 15 calendar days. The OCSO has taken the appropriate steps to implement the RWG mandate.

6. **Develop departmental guidance to apply reciprocity as outlined in Executive Order 13381.**

   Executive Order (EO) 13381 has been revoked by EO 13467 "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information" and the new EO 13488 "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvesting in Individuals in Positions of Public Trust."

   These EOs provide general guidance on reciprocity. As a result, implementation guidance is currently being developed at the federal level through the JRT.

7. **Designate the DHS Office of Security, Personnel Security Division, as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements.**

- The DHS Chief Security Officer (CSO) is a member of Office of Management and Budget/ Performance Accountability Council (OMB/PAC) and a member of the Director of National Intelligence (DNI) Special Security Center. The DHS CSO uses these memberships to represent all DHS components on personnel security-related issues. In addition, the Personnel Security Division (PSD) of the OCSO also represents the department as a member of the PAC, and several other working groups. Some of these groups include: Training and Certification Sub-committee; Repository Working Group; Repository Reform Implementation Group; Background Investigations Stakeholders Group; eApp Requirements Working Group; Investigations Working Group; Personnel Security Working Group; and the Requirements Working Group

8. **Develop a training program for program managers on the personnel security process.**

   The OMB/PAC has created a sub-committee to address the need to establish standardized training. It is anticipated that the end result will be to mandate training and certification

for all investigators and adjudicators. PSD participates fully in this effort and ensures that all personnel security matters of DHS are brought to the forefront for consideration.

9. **Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount.**

   This is currently being addressed by the JRT. The OCSO participates in this effort and ensures that all department concerns are fully represented.

   The OCSO Personnel Security Division is reviewing debt levels established for headquarters components and will develop a proposed ceiling that is acceptable to the department. This proposal will be offered for consideration when a mandatory threshold will be set government-wide – a threshold that is called for under the new investigative standards.

10. **Set minimum personnel security processing standards for temporary employees in DHS to include student interns and summer hire program employees.**

    Every agency vets its temporary employees and interns differently; it is up to each agency to determine what is appropriate for its mission. In addition, Title 5, CFR, section 732 requires an investigation be conducted *after* 180 days of employment. Reciprocity does not extend to these positions unless they convert to permanent employment after 180 days. It is not clear that the establishment of minimum standards for temporary employees would add value to the personnel security process.

11. **Develop a formal DHS Adjudicator training and certification program.**

    The OCSO currently provides adjudicator training at the annual Security Conference, as well as through quarterly meetings of the DHS Adjudicator Roundtable. To supplement these efforts, the OCSO Training and Operations Security (OPSEC) Division is developing additional adjudicator training. Lastly, the PAC is developing government-wide standards for adjudicator and investigator training and certification.

12. **Negotiate with the Office of Personnel Management for investigative authority to be delegated to DHS Office of Security.**

    The Office of Management and Budget issued a memorandum on October 29, 2007, which instructed OPM to inform the OCSO, among other agencies, that it had received delegated investigative authority. OCSO is currently exercising that authority by using a contract administered by Customs and Border Protection to conduct investigations.

13. **Develop a list of concerns regarding e-QIP to share with OPM for resolution.**

    According to all the statistical information available to us at this time, e-QIP is operating smoothly.

14. Develop a list of concerns regarding background investigations to share with OPM for resolution.

OCSO, together with other agencies such as DOD, DNI and PERSEREC, are addressing concerns that have been expressed. Surveys have been completed, as well as several statistical analyses, that are designed to yield information on background investigations.

15. Designate DHS Office of Security, Personnel Security Division, as the sole representatives to OPM for the components.

As discussed in the response to question 7, the DHS Chief Security Officer is a member of the OMB/PAC and a member of the DNI Special Security Center. As such, the DHS CSO represents all DHS Components on personnel security-related issues.

However, because each component has unique operational requirements, it must deal directly with OPM on specific case issues. Adding a new layer of authority would likely result in inefficient and burdensome processes.

16. Direct component human resource offices to use qualified classifier as the final decision maker in position designations.

CHCO will need to establish a number of FTE classifiers (that is, a classification team to consist of a yet-to-be determined number of positions) in order to fulfill this recommendation and ensure continuity of operations that cannot be provided by contract support. It is important to point out that this number is subject to change depending on the contract involved.

17. Establish and maintain department Position Description Library of properly designated positions.

As stated above, a need exists to establish at least two teams to fulfill this recommendation. The first team would likely consist of two FTEs to handle classification of position descriptions (PDs), ensuring that OPM guidance is followed. For the second team of FTE classifiers, the number required would be determined by the number of PDs that need to be reviewed and what timeline must be met. This team would be designated to review all approved PDs to date to ensure proper classification. Contractors could be used for administrative support between the two teams and to enter documentation into the newly-developed CHCO PD library.

18. Direct DHS component HR offices to submit workforce projections to the Chief Human Capital Office annually.

Working with each Directorate, DHS CHCO needs to create manning rosters for each Directorate, by position. Position would have a line number, with the following to correlate to each line: position title; series; grade; and PD number. To better control the federal work flow, only vacant positions – or those additional positions approved by the

approving authority for that Directorate – can be filled. It is expected that this will reduce the surge mentality of hiring with no constraints.

19. Instruct DHS Office of Security, Personnel Security Division, to formalize its provision to components for adjudicator surge capacity.

OCSO recognizes the requirement for adjudicator surge capacity to assist components during hiring initiatives. In the past, OCSO has been able to provide this surge capacity; however, budget and operational requirements have reduced this capacity. Accordingly, provisions for a surge adjudication team were formerly included in the FY 2010 budget. Although OMB has cut the funding for this initiative, DHS has appealed the decision.

20. Require DHS Office of Security, Personnel Security Division, to use ISMS to initiate and track reinvestigation needs for components.

Implementation of this recommendation is underway. The first component is scheduled to begin using ISMS to track reinvestigation in April 2009. Additional components have begun taking steps for their inclusion at a later date.

Attachment B

USCIS DHS OIG Report on DHS Personnel Security Process

Response to Recommendations

1. Establish a requirement for selectees to complete e-QIP within a specified number of days, and develop strategies to mange selectees who do not meet the response requirement.

Concur. USCIS currently requires that an applicant complete e-QIP within 10 days, and the hiring office is notified when a selectee has not completed e-QIP within the timeline, so HR can determine if the individual is still interested in the position.

2. Delegate all customer service responsibilities to DHS Personnel Security Division

Disagree. Moving this crucial process further from the accountability that comes from direct connection with component performance and goals would be ineffective. USCIS PSD has a customer service unit that responds to customer inquires within 2 hours on average. If this function were consolidated at DHS, response rates to the USCIS customers would be significantly impacted due to the volume of requests from all components. Close proximity to the USCIS applicant files, as well as the PSD personnel processing the applicants, enhances the ability to provide outstanding rapid responses to our customers and to USCIS Management.

Since a majority of the customers serviced by a component personnel security office are within the component, directing customer service responsibilities to the DHS Personnel Security Office would create a longer communication chain, when speed and accuracy are vital to meeting the customers' requirements. A DHS-level customer service function would increase the possibility for miscommunication between the components' personnel security offices, the program offices requesting services, and the applicants/appointees/employees, due to the involvement of another party that may not be familiar with a component's specific requirements.

USCIS recommends that each component establish a customer service unit commensurate with the volume of work that is processed by the component to address inquiries for support and information using an automated intake process such as an electronic mailbox. This approach has proven to be successful at USCIS and has been recognized as a best practice.

3. Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.

1

Disagree. USCIS PSD has established a concise set of procedures to include the receipt of applicant paperwork, creation of the personnel security files for each applicant and to conduct immediate credit and fingerprint checks utilizing direct lines to the FBI and the Equifax credit bureau. The USCIS PSD Intake Unit completes all initial work and assigns the case to a processing security assistant in less than 1 day. This efficient and comprehensive approach has reduced overall processing time and ensured that personnel hired to review and determine suitability of applicants are utilizing their specialized skills on analysis rather than clerical responsibilities. Should DHS establish an intake unit at the Department level to address all components initial processing, this would add unnecessary time delays while completed files are triaged by DHS PSD and delivered to the appropriate component. The USCIS PSD processing timeframes would be adversely impacted, reducing the component's ability to meet the OMB guidelines.

USCIS recommends that each component establish an intake unit to complete the clerical processing responsibilities of data entry into the electronic security databases and to create the applicant's files as needed.

4. Consolidate component security information into ISMS.

Concur. USCIS is currently working with DHS Office of Security on the deployment of ISMS.

5. Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.

Disagree. USCIS does agree that certain agencies take a long time to transfer background investigations. The Federal Strategy for Improving the Accessibility of Federal Investigative Records establishes the desired goal to be fully automated in processing record requests and record responses between agencies in optimal time. Once implemented, the initiative will improve timeliness of receipts of investigative files.

6. Develop departmental guidance to apply reciprocity as outlined in Executive Order 13381.

EO 13467 replaced 13381(revoked).

Concur. DHS-level guidance, if specific, would have to recognize each component's mission. Government-wide guidance relating to this Executive Order is currently being developed through the Joint Reform Team.

2

7. Designate the DHS Office of Security, Personnel Security Division as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements.

Concur.

8. Develop a training program for program managers on the personnel security process.

Concur. As part of the USCIS training program for supervisors, OSI currently conducts briefings during each course outlining the personnel security program. USCIS OSI provides an overview of personnel security within the security training sessions offered throughout the component. USCIS routinely provides PSD briefings to managers, covering all aspects of the security screening, adjudication, and security clearance processes. USCIS OSI PSD has created many outreach documents, brochures, and presentations to educate program managers on the personnel security process. Much of this information is available to USCIS employees through the OSI website.

9. Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount.

Concur. DHS is coordinating a financial Adjudicator Roundtable, scheduled for March 2009, for discussion of debt thresholds across the Department.

10. Set minimum personnel security processing standards for temporary employees in DHS to include student interns and summer hire program employees.

Concur. USCIS currently conducts a NACI investigation on all temporary employees (student interns, summer hires, etc.)

11. Develop a formal DHS Adjudicator training and certification program.

Concur. DHS is developing adjudicator training of all Personnel Security adjudicators. In addition, OPM is establishing a government-wide training and certification program required for all adjudicators.

12. Negotiate with the Office of Personnel Management for investigative authority to be delegated to DHS Office of Security.

Concur. If DHS negotiates agency-wide delegated authority this would expedite the process for

any individual component pursuing the authority.

13. Develop a list of concerns regarding e-QIP to share with OPM for resolution.

USCIS has not experienced the same persistent problems as outlined, and has few complaints or recommendations regarding e-QIP.

In response to the problems identified by other DHS components:

- E-QIP adequately outlines instructions for completing various fields. USCIS does not receive consistent complaints from applicants or users regarding sensitivities in the system.
- USCIS has no documented instances of applications being returned to applicants.
- USCIS has had no experience with e-QIP timing out and erasing applicant records. The applicant side of e-QIP saves data frequently, and no applicants have complained about having to start their applications over.
- e-QIP can be utilized by contract applicants. USCIS has established a child-parent agency hierarchy to accommodate this working relationship. USCIS uses OPM as their Investigation Service Provider (ISP), so the componennt has no knowledge of difficulties in transmitting investigation paperwork to contracted ISPs.
- USCIS concurs that the printed Archival Copy is lengthy.
- USCIS finds that their system administrators are able to correct errors (to include password resets) with ease and in a timely manner. OPM has provided several acceptable and efficient avenues for amending errors on applicant paperwork that present no significant problems.

USCIS began using e-QIP in April 2006. Since introducing this system at USCIS, the Personnel Security Division (PSD) has dedicated time and resources to developing in-house technical expertise, has created a Frequently Asked Questions outreach document, and has utilized their Customer Service Branch to assist users with questions. USCIS has found OPM to be consistent in rejections and helpful in providing information about using and developing the agency's e-QIP system.

USCIS concurs that e-QIP has improved the overall application process.

14. Develop a list of concerns regarding background investigations to share with OPM for resolution.

Concur. OPM provides an annual opportunity for individual components to respond to the quality of OPM services. USCIS agrees that a consolidated list of concerns would identify a consensus of issues requiring resolution.

DHS recently participated in an OPM Performance Accountability Council Investigation Quality review. DHS adjudicators conducted reviews of OPM investigations and provided written feedback indicating deficient reports of investigations in which the components were unable to make adjudicative determinations. OPM provided detailed responses, addressing the

Department's concerns and in some cases agreed with the identified deficiencies; in other instances OPM cited handbook procedures, justifying the quality of the results.

15. Designate DHS Office of Security, Personnel Security Division, as the sole representatives to OPM for the components.

Disagree. Each component should have the ability to directly liaison with OPM on questions and or concerns. Designating DHS as the sole representative would add an unnecessary layer and cause delays in resolving issues.

16. Direct component human resource offices to use qualified classifier as the final decision maker in position designations.

Disagree. In accordance with the DHS MD 11050.2, Personnel Security and Suitability Program, position designations will be subject to final approval by the Organizational Element's respective Personnel Security Office. On 1/5/09 OPM issued a Federal Investigation Notice announcing a New Position Designation System and Automated Tool. This tool provides agencies with an automated tool to accurately and consistently classify position risk and sensitivity. USCIS Personnel Security are accustomed to making position designation determinations. USCIS recommends that Personnel Security review every draft position description and identify the risk and sensitivity level, as well as the required background investigation.

17. Establish and maintain department Position Description Library of properly designated positions.

Concur. There is currently a CPB position description library however all PDs are not included in the library. A centralized library would make the process more efficient.

18. Direct DHS component HR offices to submit workforce projections to the Chief Human Capital Office annually.

Concur. USCIS leadership created a special unit responsible for monitoring overall growth, reporting on progress and setbacks, and facilitating dialogue on any issues that arise. This unit works closely with functional offices to coordinate support for the growth, including Human Resources, Personnel Security, IT, and Facilities. Close involvement by leadership adds accountability to the oversight process. The Chief of USCIS PSD attends bi-weekly hiring and training meetings with the growth management unit in which USCIS hiring projection are reported and tracked. This exchange of hiring information has allowed USCIS PSD to accurately project workload and justify positions.

5

#19 Instruct DHS Office of Security, Personnel Security Division to formalize its provision to components of adjudicator surge capacity.

Concur. DHS has developed a formal proposal for assisting with adjudication surges across the Department.

20. Require DHS Office of Security, Personnel Security Division to use ISMS to initiate and track reinvestigation needs for components.

Disagree. Recommend rewording this recommendation to direct DHS Personnel Security Division to facilitate and provide tools to the components enabling them to identify, track, and task reinvestigations ideally with ISMS. USCIS does not recommend that DHS oversee the reinvestigation program of each component.

6

IG Report on DHS Personnel Security Process Recommendations
Comments by
CBP Office of Internal Affairs

Attachment C

IG Report on DHS Personnel Security Process Recommendations
Customs and Border Protection Responses

CBP has addressed below each of the OIG's recommendations without having the benefit of analysis or studying the feasibility of such far reaching concepts. We recommend DHS spearhead a working group with representatives from each component to conduct an in-depth, comprehensive cost-benefit analysis prior to accepting any recommendations about the centralization of intake and customer service or any component process/function at the department level.

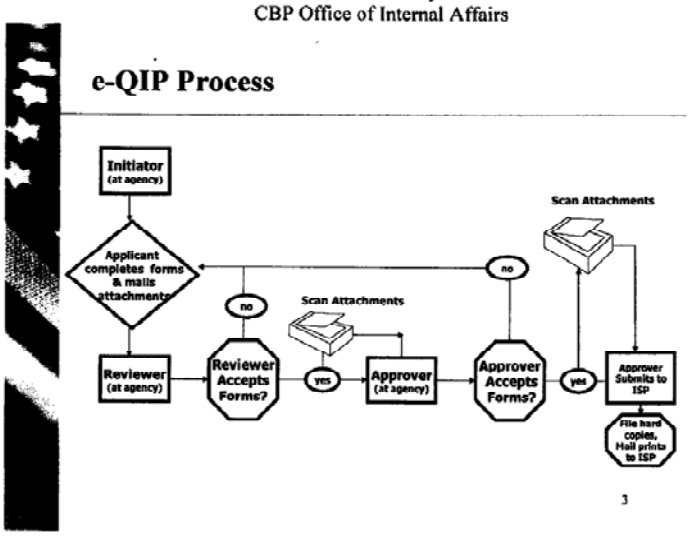
1. **Establish a requirement for selectees to complete e-QIP within a specified number of days, and develop strategies to manage selectees who do not meet the response requirement.**

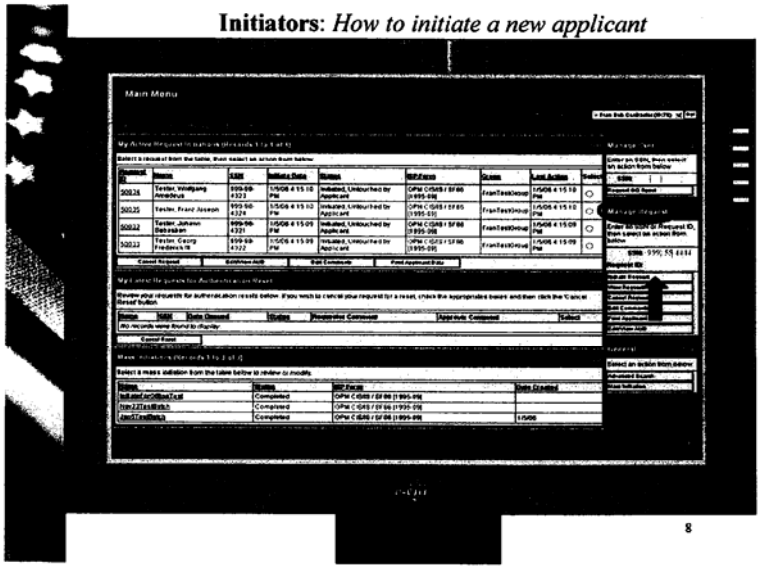
CBP Response: Agree to the extent that CBP PSD is able to control this part of the process. In CBP, the applicant (selectee) process related to timely preparation of e-QIP rests with the Office of Human Resources Management (HRM) and not the CBP Personnel Security Division (PSD). PSD will work with HRM to set response standards and develop strategies to manage selectees who do not meet the response requirements.

PSD does control the e-QIP process for CBP Periodic Reinvestigations (employees), from initiation to releasing completed forms back to the Office of Personnel Management (OPM). PSD will establish a timeliness requirement and develop strategies to manage employees who do not meet the response requirement.

The following diagrams were taken from an OPM e-QIP overview presentation:

IG Report on DHS Personnel Security Process Recommendations
Comments by
CBP Office of Internal Affairs





2. Delegate all customer service responsibilities to DHS Personnel Security Division

CBP Response: Disagree. The OIG report suggests that the need for centralization of customer service at the department level is to reduce the number of interruptions components experience to answer e-QIP related questions. The nature of e-QIP (explained in response to Recommendation 3) does not lend itself to department-level customer service. The most efficient customer service initiative is for each component to establish a help desk function for addressing e-QIP questions from its applicants and employees.

3. Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.

CBP Response: Disagree. Centralized intake is not practical and leaves room for confusion and breakdowns in communication. Based on the mandate received from the Administration to hire a significant number of Border Patrol Agents, CBP has the largest volume of investigations in DHS (more than 27,000 in 2008). Given this volume, CBP should maintain its own intake function for the foreseeable future.

IG Report on DHS Personnel Security Process Recommendations
Comments by
CBP Office of Internal Affairs

In addi ion to CBP's large intake volume, the nature of e-QIP does not lend itself to a centralized department-level intake process. OPM limits e-QIP access to applicants and authori zed agency user groups. Each user agency (i.e. DHS component) is provided a Sponsoring Organization Number (SON) or Sponsoring Organization Identifier (SOI). The SON and/or SOI is needed to access e-QIP forms applicable to each specific component. A centralized intake process would be too cumbersome, requiring management of all e-QIP forms for multiple components.

4. **Consolidate component security information into ISMS.**

CBP Response: Agree.

5. **Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.**

CBP Response: Disagree. As stated above, a department-level centralized intake processing center is impractical. CBP processes more background investigations than any other component within DHS.

6. **Develop departmental guidance to apply reciprocity as outlined in Executive Order (EO) 13381.**

CBP Response: Agree. Executive Order 13381 does not discuss reciprocity; agree to apply reciprocity as outlined in ***EO 13467***. Since all components are required to comply with reciprocity provisions outlined in EO 13467, departmental guidance would provide consistency across all components.

7. **Designate the DHS Office of Security, Personnel Security Division as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements.**

CBP Response: Disagree. This would only create an additional layer of bureaucracy and delay responses to component requests. New OPM Investigative Standards which discuss Suitability and Security Executive Agent positions are still in final draft status.

8. **Develop a training program for program managers on the personnel security process.**

CBP Response: Agree.

3

IG Report on DHS Personnel Security Process Recommendations
Comments by
CBP Office of Internal Affairs

9. **Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount.**

CBP Response: Agree.

10. **Set minimum personnel security processing standards for temporary employees in DHS to include student interns and summer hire program employees.**

CBP Response: Disagree. The same investigative standards that apply to permanent full time employees should also apply to temporary staff and interns. Investigative standards should be based on position sensitivity, not the duration of employment. If temporary staff and interns have the same level of access as full time employees, they should be required to undergo the same level investigation, and the same personnel security processing standards should apply.

11. **Develop a formal DHS Adjudicator training and certification program.**

CBP Response: Agree. DHS needs to develop an adjudicator training course consisting of two parts, one for suitability adjudication (including mission-specific criteria for DHS) and one for eligibility. All DHS adjudicators should be required to complete both courses.

12. **Negotiate with the Office of Personnel Management for investigative authority to be delegated to DHS Office of Security.**

CBP Response: Not applicable for CBP.

13. **Develop a list of concerns regarding e-QIP to share with OPM for resolution.**

CBP Response: Agree.

14. **Develop a list of concerns regarding background investigations to share with OPM for resolution.**

CBP Response: Not applicable to CBP.

15. **Designate DHS Office of Security, Personnel Security Division, as the sole representatives to OPM for the components.**

CBP Response: Disagree. OPM provides excellent support to CBP through assigned liaison personnel. There is no value added by having a sole DHS PSD department-level representative to OPM. This may even delay response to inquiries due to competing priorities across components.

IG Report on DHS Personnel Security Process Recommendations
Comments by
CBP Office of Internal Affairs

16. Direct component human resource offices to use qualified classifier as the final decision maker in position designations.

CBP Response: Agree, as per current practice in CBP.

17. Establish and maintain department Position Description Library of properly designated positions.

CBP Response: Agree.

18. Direct DHS component HR offices to submit workforce projections to the Chief Human Capital Office annually.

CBP Response: Agree.

19. Instruct DHS Office of Security, Personnel Security Division to formalize its provision to components of adjudicator surge capacity.

CBP Response: Agree.

20. Require DHS Office of Security, Personnel Security Division to use ISMS to initiate and track reinvestigation needs for components.

CBP Response: Agree; with clarification. The OIG report stated that ISMS can be used to initiate and track 5- and 10-year reinvestigations. Under the new OPM Investigative Standards final draft, all background investigations will be grouped into 3 "Tiers." Tiers 2 and 3 will require reinvestigations as follows:

> 20% of Tier 2 employees will be reinvestigated each year so that 100% will be reinvestigated within 5 years. Tier 3 employees will undergo continuous evaluation, meaning that 100% of these employees will be required to update their e-QIP form and undergo a Subject Interview annually, as well as have automated record checks conducted. In addition, any qualifying life event will require an e-QIP update and concurrent management notification.

DHS OIT must ensure that ISMS will be able the handle the large volume of information anticipated when all components are utilizing the system to initiate and track investigations and reinvestigations under the new OPM Investigative Standards.

5

U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE
Washington, D.C. 20223

February 19, 2009

MEMORANDUM

From: Robin L. DeProspero-Philpot
Chief – Security Clearance Division
U.S. Secret Service

To: Jerry Williams
Chief Security Officer
Department of Homeland Security

Subject: Response to Department of Homeland Security Office of Inspector General Report on Personnel Security Process

Reference is made to your e-mail, dated January 30, 2009, requesting all Department of Homeland Security (DHS) components to review and make any relevant comments pertaining to the DHS Office of Inspector General Report on Personnel Security Process (draft, dated January 2009).

Listed below is the U.S. Secret Service's position on several recommendations made by the DHS Office of Inspector General.

Recommendation #2: Delegate all customer service responsibilities to the DHS Personnel Security Division.

Recommendation #3: Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division.

The U.S. Secret Service (Secret Service) strongly opposes Recommendations 2 and 3 above. The Secret Service solely controls and conducts all facets of its personnel security process, and has a very unique applicant process (personal, hands-on) for both the Special Agent and Uniformed Division Officer positions. Utilizing the Department for a centralized customer service office and security intake-processing center for all DHS components would not be feasible for the Secret Service, as control and accountability of its hiring process, and the personal contact with its applicants would be greatly reduced.

Page 2

Recommendation #5: Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files.

The Secret Service opposes Recommendation #5. In compliance with the Joint Security and Suitability Reform Team and the Repository Working Group's Federal Strategy for Improving the Accessibility of Federal Investigative Records, the Secret Service is in the process of attempting to acquire the necessary equipment and resources to scan all personnel security investigations. The relevant Secret Service Headquarters offices are developing a concept of operations for the submission of investigations electronically to other federal departments and agencies in the mandated timeframe. Utilizing a centralized intake processing center for this responsibility would negate a component agency's ability for its control, handling, and accountability of their personnel security investigations.

Recommendation #20: Require DHS Office of Security, Personnel Security Division use ISMS to initiate and track reinvestigation needs for components.

The Secret Service strongly opposes this Recommendation. The Secret Service is in full compliance of the requirement for its employees' reinvestigation process. Presently, the Personnel Security office of the Secret Service is initiating reinvestigations on its employees every four (4) years. Due to "surges" in fiscal year hiring, applicant background investigations take precedence over reinvestigations. By initiating the reinvestigations every 4 years, additional time is allotted for the completion and adjudication of the updated investigation, ensuring completion at the 5-year mark.

If you have any questions, or need additional information, please contact me at 202/406-5433.

Office of the Assistant Secretary
U.S. Department of Homeland Security
500 12th Street, SW
Washington, DC 20536

U.S. Immigration and Customs Enforcement

March 17, 2009

MEMORANDUM FOR: Jerry Levine
Departmental Audit Liaison
U.S. Department of Homeland Security

FROM: John P. Torres
Assistant Secretary (Acting)

SUBJECT: ICE Response to OIG Draft Audit Report: "The DHS Personnel Security Process, January 2009"

U.S. Immigration and Customs Enforcement (ICE) provides the following response to the subject Office of the Inspector General (OIG) report. As this is an audit of the Department of Homeland Security (DHS), this response is provided to your office for inclusion in the DHS response to OIG.

OIG Recommendation 1: "Establish a requirement for selectees to complete *e*-QIP within a specified number of days, and develop strategies to manage selectees who do not meet the response requirement."

ICE Response to Recommendation 1: ICE concurs. It has been the experience of ICE that the applicant takes about 3 days to 3 weeks to complete electronic-Questionnaire for Investigations Processing (e-QIP). A reasonable time to complete the questionnaire is 10 days. Further, the responsibility for ensuring the applicant completes e-QIP should remain with the Office of Human Capital (OHC) as part of the application process. Submitting forms by an applicant is a condition of employment and should remain with OHC until the security packet is processed by OHC and then submitted to ICE Personnel Security.

OIG Recommendation 2: "Delegate all customer service responsibilities to the DHS Personnel Security Division."

ICE Response to Recommendation 2: ICE does not concur. To achieve the Secretary's "one DHS" goal in this area, ICE believes that it would be better for DHS to formulate policies and procedures to be followed by the components. The ICE Customer Service Desk is

www.ice.gov

operating extremely well. ICE concurs that DHS should create a centralized number dedicated to e-QIP questions.

OIG Recommendation 3: "Create a centralized department-level personnel security intake processing and customer service center within DHS, administered by the DHS Personnel Security Division."

ICE Response to Recommendation 3: ICE does not concur. The Secretary's goal of achieving a "one DHS" would not be accomplished by the proposed centralization. In terms of intake processing, efficiencies can best be achieved at the component level. The DHS-level centralized approach as suggested by OIG would create competition among the DHS components. Each would seek priority status from DHS in pursuit of their own priorities and interests. ICE prefers to perform this work using its own resources because it allows personnel security matters to be prioritized and addressed in accordance with hiring initiatives and priorities within ICE.

OIG Recommendation 4: "Consolidate component security information into Integrated Security Management System (ISMS)."

ICE Response to Recommendation 4: ICE concurs. The availability of a consolidated information system such as ISMS would be beneficial to the security clearance adjudication process.

OIG Recommendation 5: "Designate the centralized intake processing center responsibilities for obtaining and coordinating interagency and federal department requests for previous investigation files."

ICE Response to Recommendation 5: ICE concurs. We note that government-wide efforts are in motion to speed up the provision of requesting previous investigative files from agency to agency. If it is found that DHS has a higher success rate in getting investigations from other agencies, then DHS might serve as a central site for seeking investigation and clearance information on behalf of the components. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 goals require coordination and cooperation across the government, yet this recommendation does not address the issue of agencies that do not process these requests timely.

OIG Recommendation 6: "Develop departmental guidance to apply reciprocity as outlined in Executive Order 13381."

ICE Response to Recommendation 6: ICE concurs. We note that Executive Order 13381 is revoked and Executive Order 13467 is now in effect. Current federal or contract employees with existing investigations who are processing into DHS and its components should be identified more easily in the application process. If identified early, time would not be expended on requesting the completion of new and unnecessary security forms. This might also significantly reduce the processing time for these types of individuals.

OIG Recommendation 7: "Designate the DHS Office of Security, Personnel Security Division as the DHS representative to the Suitability or Security Executive Agent to facilitate approval of additional DHS component suitability requirements."

ICE Response to Recommendation 7: ICE concurs. A single, Department-level representative will be a valuable resource for the components.

OIG Recommendation 8: "Develop a training program for program managers on the personnel security process."

ICE Response to Recommendation 8: ICE concurs.

OIG Recommendation 9: "Establish a maximum bad debt amount for the department, and permit components to use less but not more than the maximum amount."

ICE Response to Recommendation 9: ICE does not concur. ICE makes a determination based upon the character, actions and history of the "whole" person rather than numerical threshold disqualifiers. Our concern is that a threshold of indebtedness would be used as a singular exclusionary factor, which is counter to our adjudications approach. ICE is reviewing its own procedure with the aim of helping adjudicators apply suitability factors or the adjudicative guideline to financial considerations.

Some adjudicators use thresholds as "stop measures," meaning an applicant is deemed unsuitable if their level of indebtedness reaches or surpasses the threshold. ICE prefers for its adjudicators to render their opinions based upon more than a single disqualifying factor.

OIG Recommendation 10: "Set minimum personnel security processing standards for temporary employees in DHS to include student interns and summer hire program employees."

ICE Response to Recommendation 10: ICE concurs. HSPD 12 is the minimum in government that must be met before physical access into facilities and logical access to Information Technology (IT) systems can be granted. Higher investigative requirements for access to sensitive law enforcement systems or access to classified information should remain in effect.

OIG Recommendation 11: "Develop a formal DHS adjudicator training and certification program."

ICE Response to Recommendation 11: ICE concurs and fully supports a formal training program for DHS adjudicators. ICE is willing to assist in the development of a training program and model, can host DHS training sessions, and can pilot any training program developed.

OIG Recommendation 12: "Negotiate with the Office of Personnel Management for investigative authority to be delegated to DHS Office of Security."

ICE Response to Recommendation 12: ICE concurs.

OIG Recommendation 13: "Develop a list of concerns regarding *e*-QIP to share with the OPM for resolution."

ICE Response to Recommendation 13: ICE concurs.

OIG Recommendation 14: "Develop a list of concerns regarding background investigations to share with OPM for resolution."

ICE Response to Recommendation 14: ICE concurs, in general. ICE does have investigative authority to conduct its own background investigations.

OIG Recommendation 15: "Designate DHS Office of Personnel Security Division, as the sole representatives to OPM for the components."

ICE Response to Recommendation 15: ICE does not concur. ICE prefers to coordinate with the Office of Personnel Management (OPM) directly to resolve or improve its own requirements. Adding another layer of coordination is unnecessary, results in interpretation and filtering of communications and information, and would adversely impact efficiency at ICE.

OIG Recommendation 16: "Direct component human resource offices to use a qualified classifier as the final decision maker in position designations."

ICE Response to Recommendation 16: ICE does not concur. ICE prefers to coordinate jointly with HR classification authorities, program offices and security personnel to determine position designations. This makes for a better product and reduces any risk to the agency by having a properly documented position designation.

OIG Recommendation 17: "Establish and maintain a department Position Description Library of properly designated positions."

ICE Response to Recommendation 17: ICE concurs with having an inventory of updated position designations placed into a repository accessible to the components.

OIG Recommendation 18: "Direct DHS component HR offices to submit workforce projections to the Chief Human Capital Office annually."

ICE Response to Recommendation 18: ICE concurs. Projections impact each personnel security office that supports the agency's hiring initiatives. ICE also encourages the inclusion of both federal employees and contract employees in the projections since the volume could be equal to or may even surpass federal hiring. The hiring projections are used to properly staff adjudication facilities to meet these hiring initiatives. Without good estimates, it places DHS and ICE at a disadvantage of not meeting government adjudication timelines because of improper staffing to support the workload.

OIG Recommendation 19: "Instruct DHS Office of Security, Personnel Security Division to formalize its provision to components of adjudicator surge capacity."

ICE Response to Recommendation 19: ICE concurs. This capability starts with the implementation of the recommendation above to establish a formal adjudicator-training program. DHS must establish a baseline training program to allow for consistent adjudication procedures

across the Department. This will help foster confidence in adjudicator decisions within DHS, regardless of the component.

OIG Recommendation 20: "Require DHS Office of Security, Personnel Security Division to use ISMS to initiate and track reinvestigation needs for components."

ICE Response to Recommendation 20: ICE does not concur. ICE effectively and efficiently manages its reinvestigations needs. This might be offered as a service for those components not possessing the resources to manage their own needs, but there is no value in establishing the DHS Office of Security, Personnel Security Division as a business unit to service components that already possess this capability and the necessary resources to manage it.

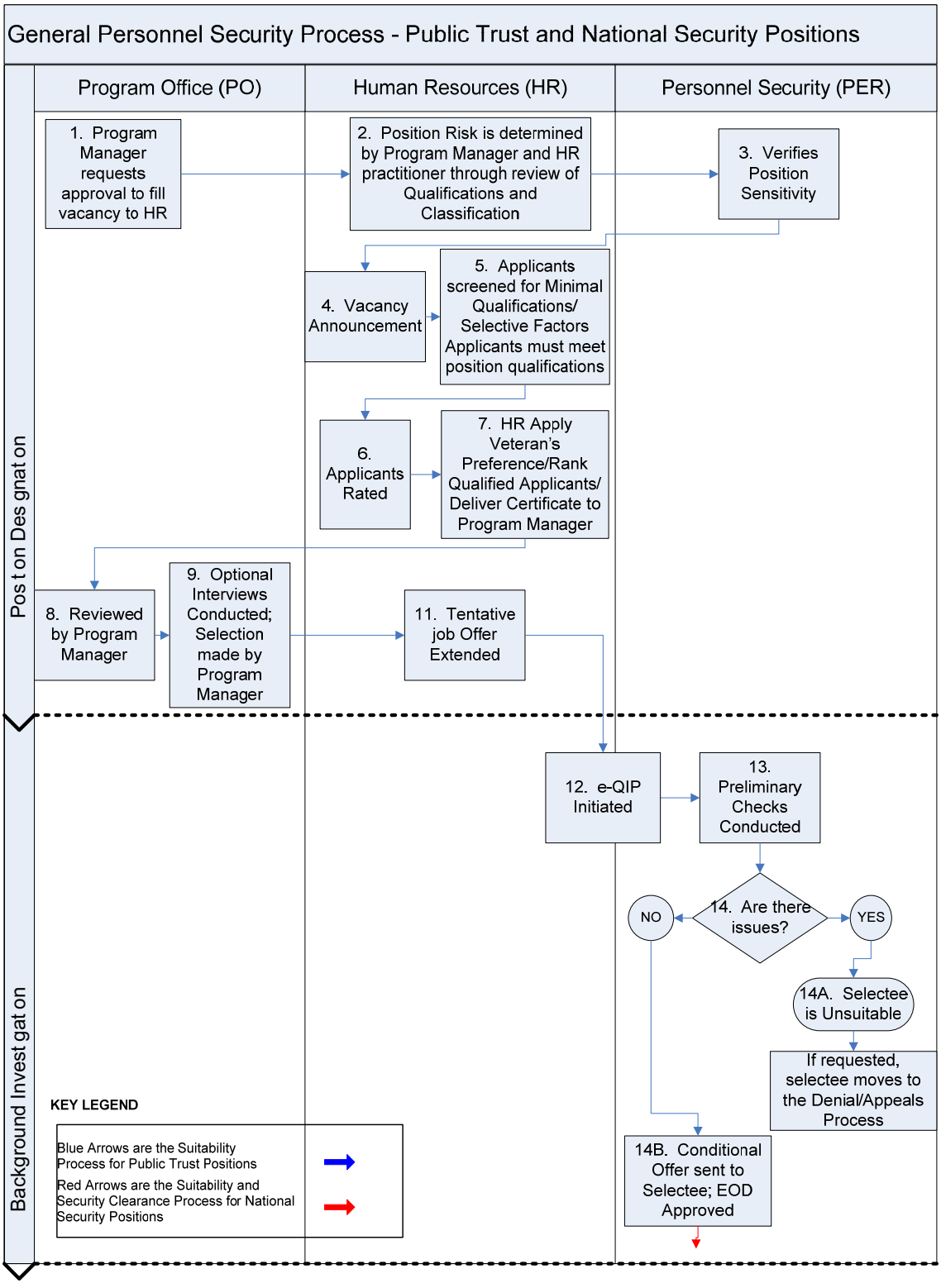
Should you have questions or concerns, please contact OIG Audit Portfolio Manager Margurite Barnes at (202) 732-4161 or by e-mail at Margurite.Barnes@dhs.gov.

Appendix C
Background Investigations

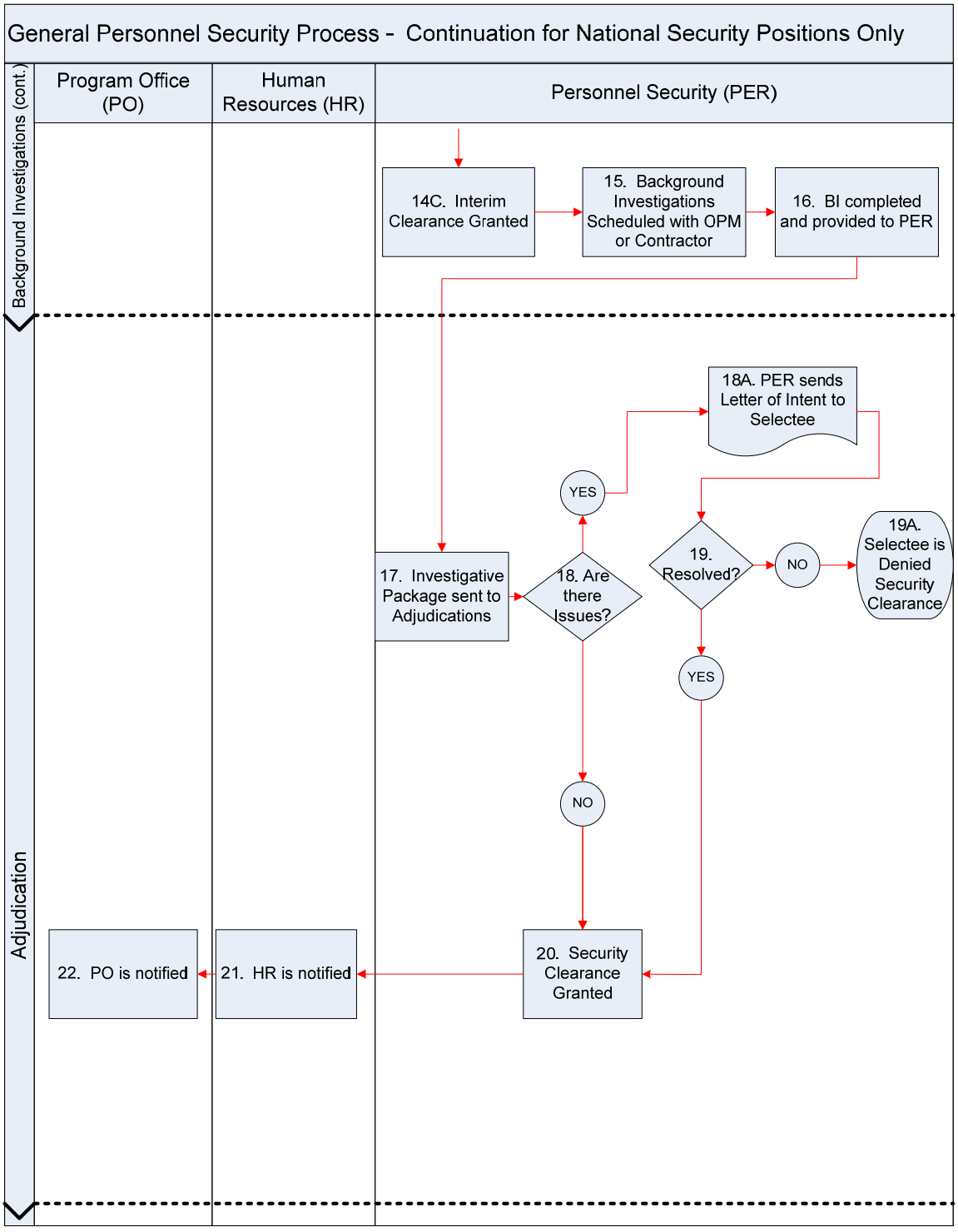
Position Sensitivity	National Security Information Access	Background Investigation Minimum Standard
National Security – Access to Classified Information		
Special Sensitive: **Any position designated at a level higher than Critical Sensitive requiring access to Sensitive Compartmented Information and other intelligence-related Special Sensitive Information.**	**Top Secret and more restricted Sensitive Compartmented Information.**	*Single Scope Background Investigation*: **NAC reviews previous background investigations and law enforcement and intelligence agency records. Includes a check of cohabitants, personal interview, and record searches for the past 10 years.**
Critical Sensitive: **Critical Sensitive positions have the potential for exceptionally grave damage to national security.**	**Top Secret national security information or materials, or other positions related to national security that require the same degree of trust.**	*Single Scope Background Investigation*
Non-Critical Sensitive: **Non-Critical Sensitive positions have the potential for serious damage to national security.**	**Access to Secret or Confidential national security information or materials, or duties that may directly or indirectly adversely affect national security operations.**	*Minimum Background Investigation*: **NACI includes a personal interview and reference, credit, law enforcement agency, residence, and employment checks.**
Public Trust Law Enforcement or Fiduciary Responsibility		
High Risk: **Potential for exceptionally serious consequences on the integrity and efficiency of a service. Duties especially critical to the agency or program mission with a broad scope of responsibility and authority.**	**None**	*Full Field Background Investigation:* **Minimum background investigation covering 5 years of employment, residential, and educational history.**
Moderate Risk: **Considers the potential for moderate to serious affect on the integrity and efficiency of the service. Duties considerably important to the agency or program mission with significant program responsibility or delivery of service.**	**None**	*Minimum Background Investigation*
Non-Sensitive/Low Risk: **Considers the potential for limited affect on the integrity and efficiency of the service. Duties and responsibilities of limited relation to an agency or program mission.**	**None**	*National Agency Check with Inquiries*: **NACI and employment, education, law enforcement agency, and personal reference checks.**

*Information in this chart was accurate as of March 2009. It is anticipated that changes will be made based on findings by the Joint Security and Suitability Reform Team.

Appendix D
General Personnel Security Clearance Process



Appendix D
General Personnel Security Clearance Process



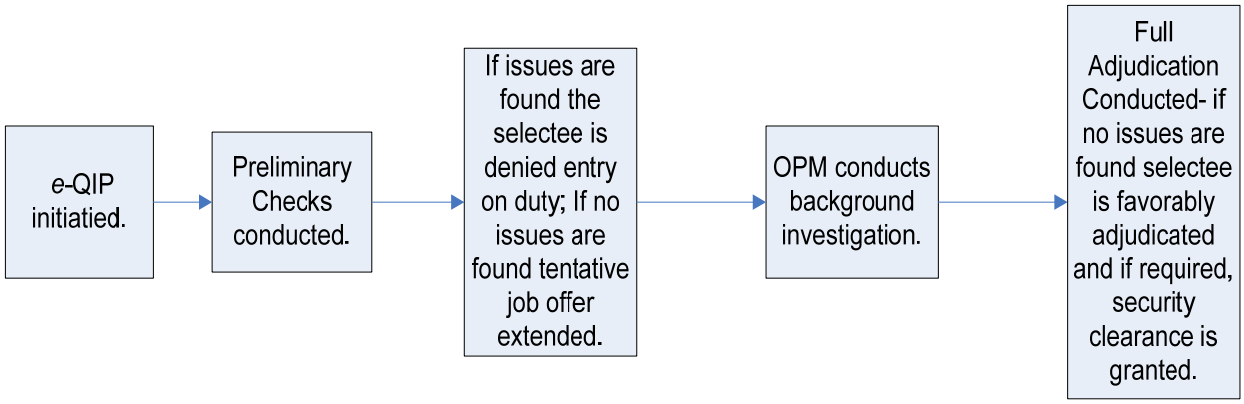
Appendix E
Component Specific Personnel Security Information

The following provides general information on the mission and role of component personnel security offices. The flowcharts do not include detailed decision points in the process nor variations applied for processing contractors. This information is current as of March 2009.

DHS Personnel Security Division

OCSO has oversight responsibilities for the DHS Personnel Security Program, to include issuing, implementing, and complying with policies and procedures. PSD is one of seven divisions under the DHS Office of Security. DHS PSD is responsible for developing and overseeing DHS personnel security policies governing background investigation and adjudications. PSD also manages and implements the employee suitability and security clearance program for all employees at headquarters. PSD develops department-wide security policies and assists the Administrative Security Division with compliance reviews. The Project Management Branch is responsible for developing enterprise systems and other special projects. Figure 17 describes the PSD workflow process.

Figure 17. The DHS PSD Personnel Security Process

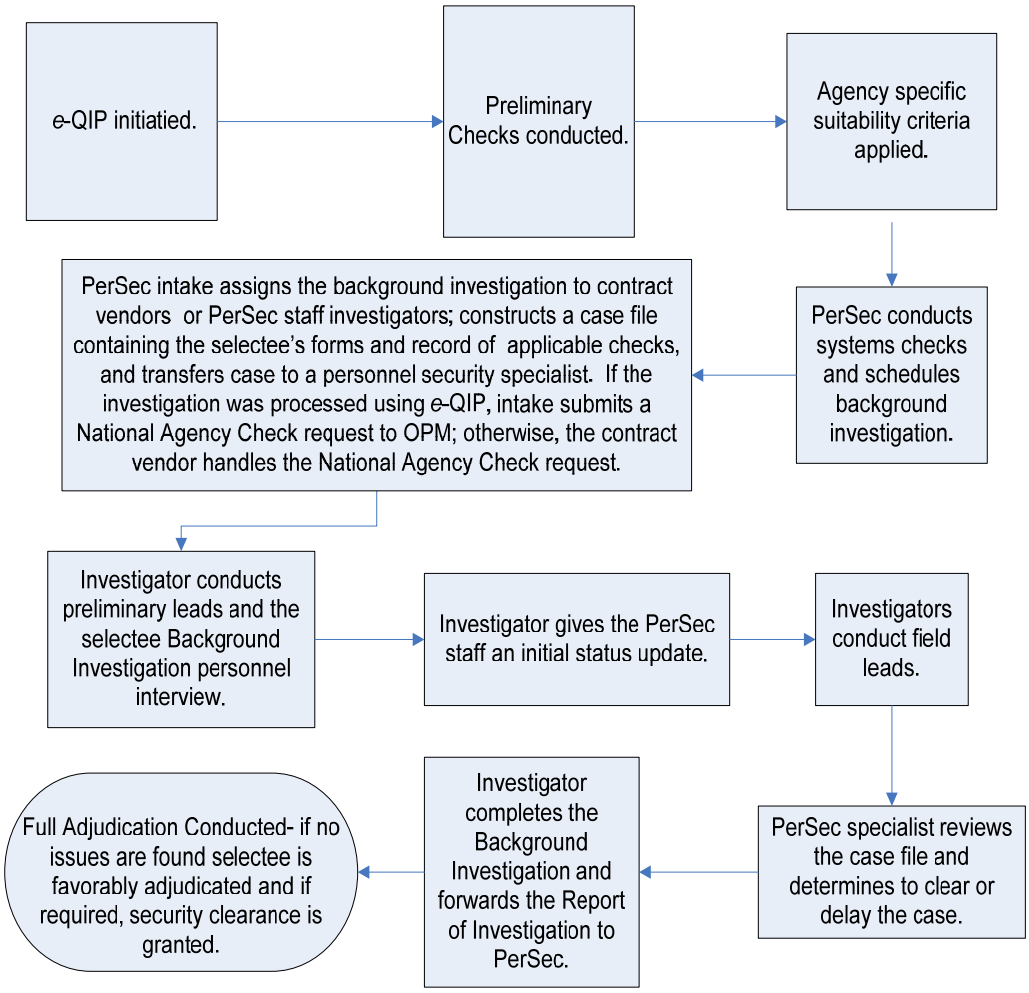


Source: Data derived from DHS PSD documents.

United States Customs and Border Protection

CBP is responsible for detecting and preventing illegal aliens, cargo, drugs, terrorists, and terrorist weapons from entering the United States. To achieve this goal, CBP Personnel Security Division (PerSec) is part of the Office of Internal Affairs and is responsible for the development of CBP policy and procedures, as well as the implementation and administration of all aspects of the Personnel Security Program. Figure 18 describes the CBP workflow process.

Figure 18. The CBP Personnel Security Process

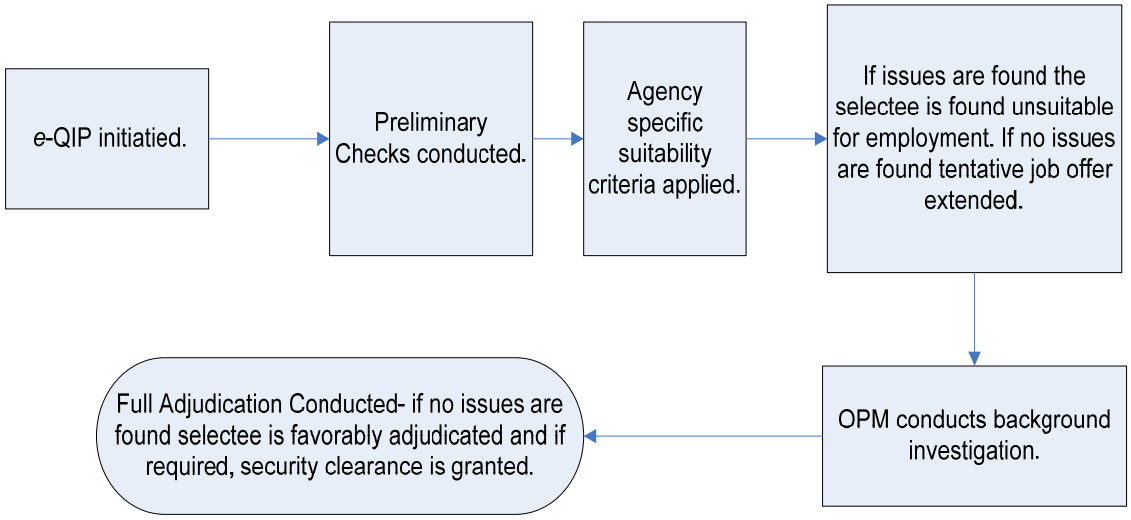


Source: Data derived from CBP documents.

Federal Emergency Management Agency

FEMA's primary mission is to provide disaster assistance and protect the Nation from all hazards. This includes natural disasters, acts of terrorism, and other manmade disasters. FEMA PerSec is part of the Human Resources Office and operates under the Customer Service Unit. Figure 20 describes the FEMA workflow process.

Figure 20. The FEMA Personnel Security Branch Process

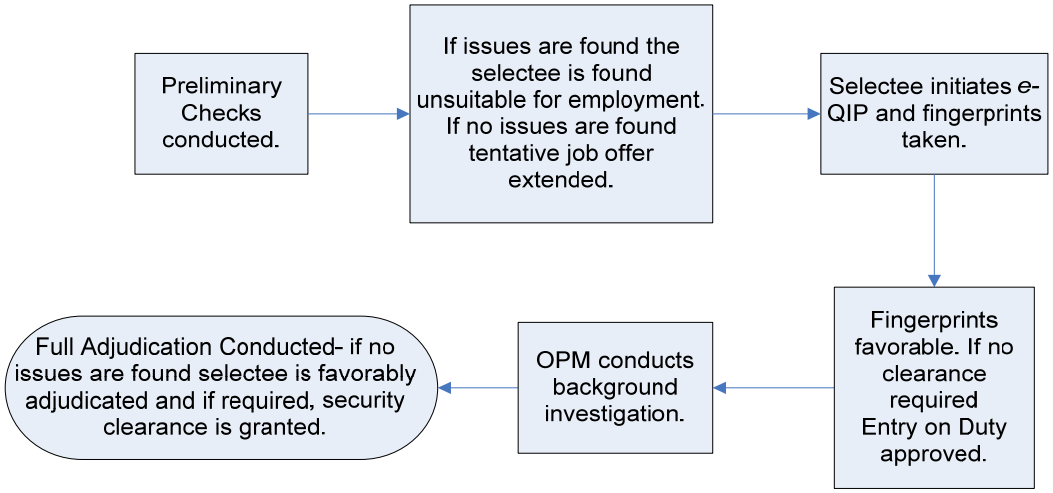


Source: Data derived from FEMA documents.

Federal Law Enforcement Training Center

FLETC is responsible for training employees who support the federal law enforcement community. FLETC also provides services to state, local, and international law enforcement agencies. FLETC PerSec is part of the Security and Emergency Management Division. The FLETC PerSec mission is to ensure that only authorized personnel have access to FLETC facilities and sensitive but unclassified and national security information. FLETC PerSec adjudicates all investigations on FLETC federal and contractor employees. The FLETC PerSec Branch is organized into two units, the Federal Employee Unit and the Contractors Unit. Figure 21 describes the FLETC workflow process.

Figure 21. The FLETC Personnel Security Process

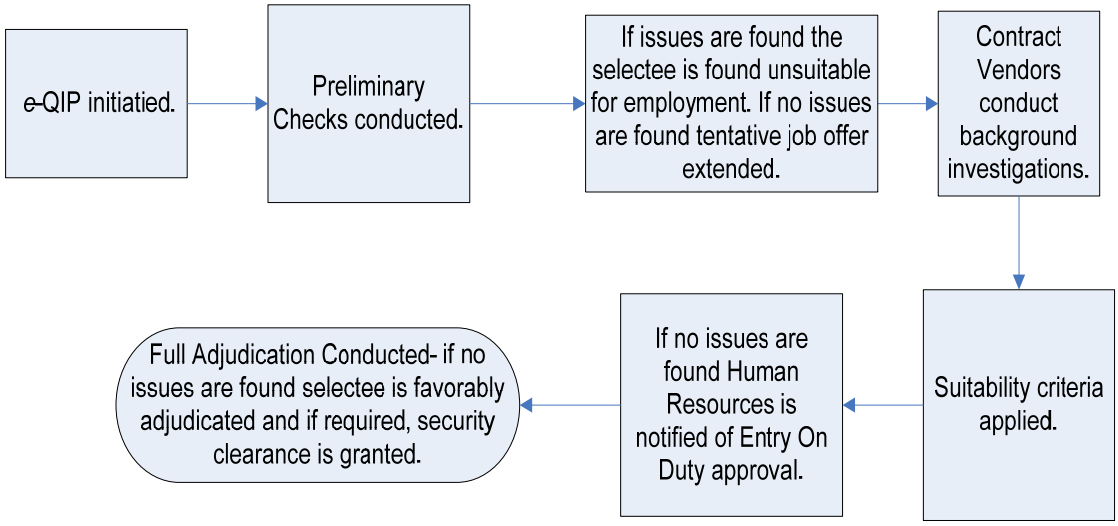


Source: Data derived from FLETC documents.

Immigration and Customs Enforcement

ICE is responsible for identifying criminal activities and eliminating vulnerabilities that pose a threat to the Nation's borders, as well as enforcing economic, transportation, and infrastructure security. ICE PerSec is responsible for processing personnel security investigations, adjudications, and reinvestigations on federal and contractor employees. PerSec has offices in Washington, DC; California; and Texas. Each ICE PerSec office is organized into the core four distinct functions for Intake, EOD, Investigations, and Adjudications. The DC office supports the entire investigative process. Figure 22 describes the ICE workflow process.

Figure 22. The ICE Personnel Security Unit Process

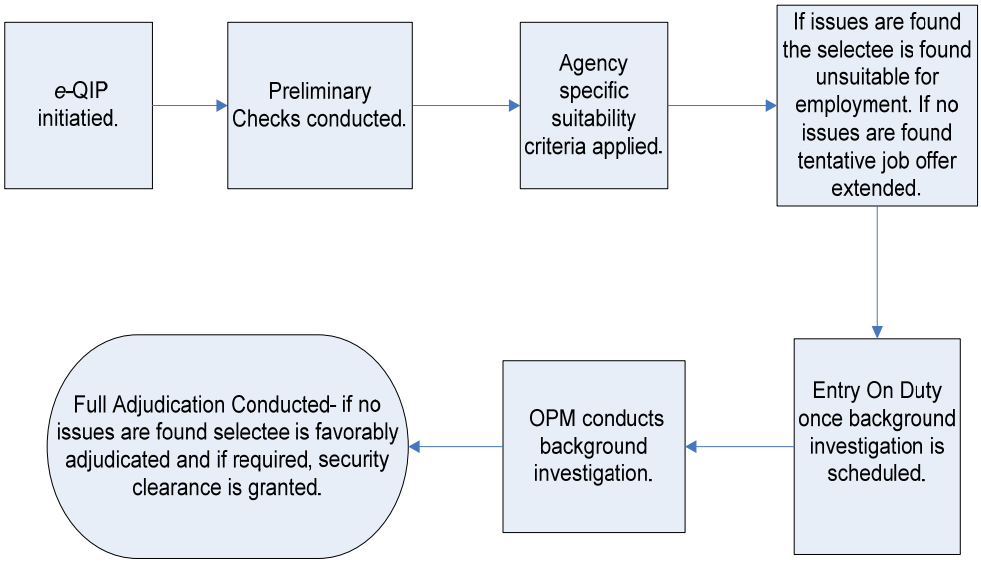


Source: Data derived from ICE documents.

Transportation Security Administration

TSA protects the Nation's transportation systems to ensure freedom of movement for people and commerce. With state, local, and regional partners, TSA oversees security for the highways, railroads, buses, mass transit systems, ports, and U.S airports. TSA PerSec is located under the Office of Security. TSA PerSec is organized into two branches, Adjudications and Operational Support. Figure 23 describes the TSA workflow process.

Figure 23. The TSA Personnel Security Process

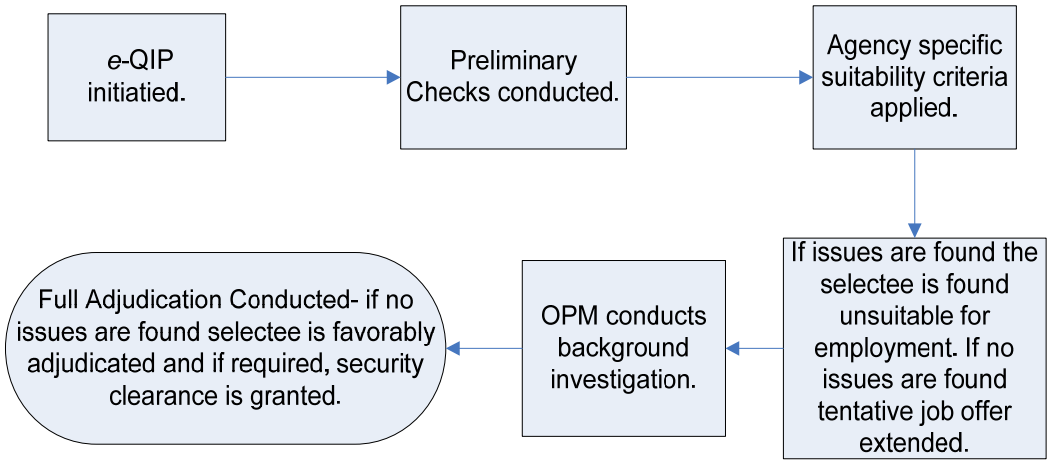


Source: Data derived from TSA documents.

United States Coast Guard

USCG is a branch of the United States Armed Forces. It is unique in that it is also a maritime law enforcement agency and a federal regulatory agency under DHS. The USCG mission is to protect the public, the environment, and U.S. economic and security interests in any maritime region. The Coast Guard Security Center (SECCEN) in Chesapeake, Virginia, is the central adjudicating facility for the processing and maintenance of all USCG personnel security files. SECCEN is an operational division under the USCG Office of Security Policy and Management. SECCEN is functionally organized into three branches for uniformed members, federal civilians, and technical security employees. Figure 24 describes the USCG workflow process.

Figure 24. The USCG Personnel Security Process

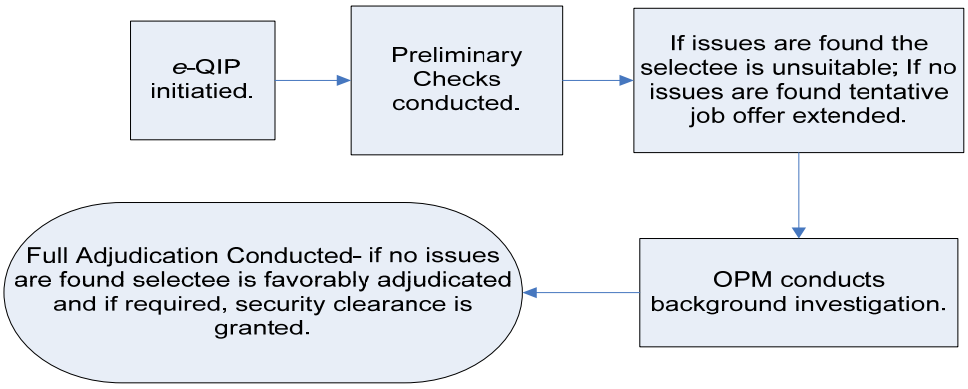


Source: Data derived from USCG documents.

United States Citizenship and Immigration Services

USCIS is charged with administering immigration services and benefits by processing immigrant visa petitions, naturalization petitions, and asylum and refugee applications. The USCIS PerSec, headquartered in Burlington, Vermont, is part of the Office of Security and Integrity. USCIS PerSec screening processes involve a security EOD and suitability determination for all federal and contractor applicants. USCIS PerSec also conducts internal selection, federal transfer approvals, and background investigation initiation. Figure 19 describes the USCIS workflow process.

Figure 19. The USCIS Personnel Security Division Process

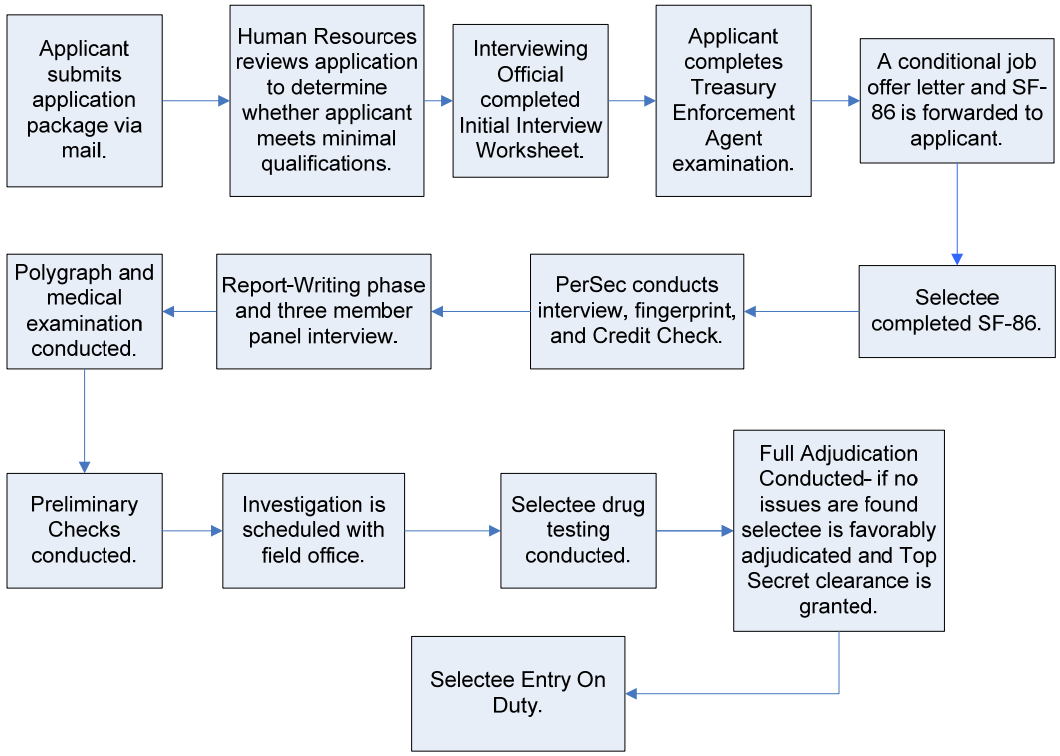


Source: Data derived from USCIS documents.

United States Secret Service

The USSS mission is to safeguard the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites, and national special security events. USSS PerSec is one of three branches in the Security Clearance Division under the Office of Human Resources and Training. Figure 25 describes the USSS workflow process.

Figure 25. The USSS Personnel Security Branch Process



USSS solely controls and conducts all facets of its hiring processes, adjudication of eligibility for a Top Secret clearance and suitability determinations are made throughout the entire process by the Security Clearance Division and Personnel. Once an applicant is found not suitable, or is adjudicated as not meeting the requirements for a Top Secret security clearance, the applicant process is immediately discontinued and correspondence is sent to notify the applicant.

Source: Data derived from USSS documents.

Appendix F
Major Contributors to This Report

Douglas Ellice, Chief Inspector
Megan McNeely Reedy, Lead Inspector
Susan Fischer, Inspector
Pharyn Smith, Inspector

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
Acting General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
DHS Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;
- Fax the complaint directly to us at (202) 254-4292;
- Email us at DHSOIGHOTLINE@dhs.gov; or
- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.