PERSEREC

Management Report 05-5
April 2005

Security Background Investigations and Clearance Procedures of the Federal Government

Eric L. Lang
Defense Personnel Security Research Center

Approved for Public Distribution:
Distribution Unlimited

Research Conducted by
Defense Personnel Security Research Center

Management Report 05-5 **April 2005**

Security Background Investigations and Clearance Procedures of the Federal Government

Eric L. Lang
Defense Personnel Security Research Center

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940

REPORT DOCUMENTATION PAGE	**Form Approved** **OMB No. 0704-0188**

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE *(DD-MM-YYYY)* 29-04-2005	2. REPORT TYPE Management	3. DATES COVERED *(From – To)* September 2003 to January 2004

4. TITLE AND SUBTITLE Security Background Investigations and Clearance Procedures of the Federal Government	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Eric L. Lang	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER MR 05-5
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite. 455-E Monterey, CA 93940-2497 Central Intelligence Agency DCI Special Security Center U.S.A.	10. SPONSORING/MONITOR'S ACRONYM(S) 11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified; Distribution Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Intelligence Authorization Act for Fiscal Year 2004 required the Director of Central Intelligence, the Secretary of Defense, the Attorney General, the Director of the Office of Personnel Management, and the heads of other appropriate federal departments and agencies (as determined by the President) to jointly submit a report to Congress that evaluates and makes recommendations regarding (1) the utility and effectiveness of personnel security background investigations and clearance procedures of the federal government, (2) the costs and benefits of conducting background investigations for Secret clearances with those of full-field investigations, and (3) the standards governing the denial and revocation of security clearances. At the request of senior staff at the Director of Central Intelligence Special Security Center and the Counterintelligence and Security office of the Under Secretary of Defense for Intelligence, PERSEREC reviewed relevant personnel security literature, such as executive orders, commission reports, Congressional testimony, and research and policy papers, to summarize information and make recommendations that address the Congressional report objectives stated above.

15. SUBJECT TERMS

Personnel Security, Security Clearance, Background Investigation, Clearance Procedures, Vetting

16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON James A. Riedel, Director
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED		166	19b. TELEPHONE NUMBER *(Include area code)* (831) 657-3000

Preface

Congressional Bill HR 2417 (Intelligence Authorization Act for Fiscal Year 2004, H.R. 2417, 108th Cong., 2003) required the Director of Central Intelligence (DCI), the Secretary of Defense, the Attorney General, the Director of the Office of Personnel Management, and the heads of other appropriate federal departments and agencies (as determined by the President) to jointly submit a report to Congress that evaluates (1) the utility and effectiveness of personnel security background investigations and clearance procedures of the federal government, (2) the costs and benefits of conducting background investigations for Secret clearances with those of full-field investigations, and (3) the standards governing the denial and revocation of security clearances. The Bill also required the joint report to include recommendations for improving federal personnel security programs.

The Defense Personnel Security Research Center (PERSEREC) was invited by senior staff at the Director of Central Intelligence Special Security Center (DCI/DSSC) and the Counterintelligence and Security office of the Under Secretary of Defense for Intelligence (USD(I)/CI&S) to evaluate and synthesize relevant research, reports and government documentation. In November 2003, PERSEREC sent the findings of this evaluation to DCI/DSSC and USD(I)/CI&S staff. The resultant report is an organized examination of specific aspects of U.S. federal personnel security programs including challenges in defining and gathering relevant effectiveness data. Pertinent program effectiveness evidence is summarized along with notes on key information that is not available. We believe that these examinations and discussions will help the DCI, Secretary of Defense and others evaluate clearance procedures of the federal government and address the requirements of Congressional Bill HR 2417.

James A. Riedel
Director

Executive Summary

Congressional Bill HR 2417 (Intelligence Authorization Act for Fiscal Year 2004, H.R. 2417, 108th Cong., 2003) requires the Director of Central Intelligence (DCI), the Secretary of Defense, the Attorney General, the Director of the Office of Personnel Management, and the heads of other appropriate federal departments and agencies (as determined by the President) to jointly submit a report to Congress that evaluates (1) the utility and effectiveness of personnel security background investigations and clearance procedures of the federal government, (2) the costs and benefits of conducting background investigations for Secret clearances with those of full-field investigations, and (3) the standards governing the denial and revocation of security clearances. The joint report also must include recommendations for improving federal personnel security programs.

At the request of senior staff at the Director of Central Intelligence Special Security Center (DCI/DSSC) and the Counterintelligence and Security office of the Under Secretary of Defense for Intelligence (USDI/CI&S), PERSEREC reviewed relevant personnel security literature, such as executive orders, commission reports, Congressional testimony, and research and policy papers, to summarize information that addresses the Congressional report objectives stated above.

Report Scope

Based on language in H.R. 2417, and discussions with DSSC and DoD staff, the report scope is limited to federal personnel security policies and procedures, including background investigations and adjudication, that serve the "clearance" process, i.e., for determining eligibility to access classified information. Special Access Programs (SAPs) and background investigations conducted for positions of trust are not addressed. Because the focus of the Congressional requirement appears to be on macro-level issues that relate to effectiveness across federal personnel security programs, the report does not focus on personnel security program details and operational differences among the many individual federal agencies. Finally, although security training and education are important aspects of personnel security programs, issues in this area are broad and complex, and are currently being addressed by a Joint Security Training Consortium (JSTC). JSTC programs are summarized in appendix A. In addition to addressing the specific requirements outlined in H.R. 2417, the current report attempts to respond to the spirit of the requirement, as reflected by the rationale provided by the Senate Committee on Intelligence (see Senate report 108-044), where the report requirement originated.

Report Organization

The report begins with an overview of the policies that define federal personnel security programs, with particular attention to the subset of policies that define program goals. This is followed by a discussion acknowledging that any evaluation of effectiveness requires a clear articulation of program objectives, utility, and performance criteria. This discussion provides the context and definitions for a report section that evaluates program effectiveness according to five program objectives and three performance criteria. The next three sections address the three specific Congressional report requirements: (1) the costs and benefits of a full-field versus a secret-level investigation, (2) the standards governing the denial and revocation of security clearances, and (3) opportunities for improving federal personnel security programs. Finally, five supporting appendices include: (A) a brief history of federal personnel security policies, programs, and reform efforts, (B) research and discussion regarding indirect benefits of personnel security programs, (C) a brief overview of public opinion and support for federal personnel security programs, (D) excerpts of summaries and recommendations from a recent (2000) evaluation of the DoD personnel security program, and (E) a description, current as of 2002, of personnel security programs at the Defense Security Service (DSS), Office of Personnel Management (OPM), Department of Energy (DoE), Central Intelligence Agency (CIA), and National Reconnaissance Organization (NRO).

Program Effectiveness

Evaluating the effectiveness and utility of federal personnel security programs first requires agreement on what constitutes the goal, program objectives, and program performance criteria. Although a common goal statement regarding the trustworthiness, loyalty and reliability of an acceptable cleared workforce can be culled from the principal executive orders that govern federal personnel security programs, there is no authoritative policy enunciating program objectives and performance criteria. Based on an interpretation of relevant policy documents and principles of program evaluation, we proposed the following five program objectives:

- Deny unacceptable applicants initial eligibility for access to classified information
- Deter cleared individuals from engaging in unacceptable behavior
- Detect, and appropriately follow-up on, evidence indicating that cleared individuals may have become unacceptable to hold a security clearance
- Assist cleared individuals who have, or appear to be developing, problems that could interfere with reliable job functioning
- Revoke the clearances of cleared individuals shown to be unacceptable,

and three program performance criteria:

- Timeliness (refers to operational deadlines for completing an objective)
- Efficiency (refers to resources expended to accomplish an objective)
- Fairness (refers to legal and appropriate treatment of program participants)

These program objectives and performance criteria were used to discuss and evaluate personnel security program effectiveness. The broader concept of utility was defined as an assessment of the total direct and indirect costs and benefits of a program, i.e., the total fiscal and subjective value of a program for which indirect, and even unintended, consequences are considered.

Security clearance procedures and the Adjudicative Guidelines have been developed through years of investigative and security-related experience concerning practical and logical risk factors for security. Research on many of the concerns represented in the Adjudicative Guidelines has shown a link between the concerns and security-relevant performance problems at work. It should be recognized that there are difficulties collecting useful objective data on characteristics such as loyalty, and there are problems of population unknowns, such as not knowing the total number of cleared individuals with espionage intent, which make it difficult to evaluate many aspects of personnel security effectiveness. With respect to utility, these issues create difficulties in directly associating objective national security benefits with personnel security program budgets.

One area in which these challenges do not pervade, i.e., where an objective measure of personnel security program effectiveness can be obtained, is in meeting program timeliness standards that entail stated deadlines. OPM states that "standard" priority investigations should be completed within 75 or 180 days, depending on the type of investigation. As of September 2004, approximately 28.3% (91,154/321,951) of OPM pending investigations were more than 180 days old. Among the overdue investigations, 40,081 (44%) were more than 360 days old. Timeliness problems have been persistent, e.g., as of May 2004, 29.6% (82,890/279,635) of pending investigations were more than 180 days old, including 50,517 (60.9% of the overdue cases) that were more than 360 days old.

For many of the remaining aspects of assessing personnel security programs, the following is clear: *improvements in effectiveness and utility* have been demonstrated and can be pursued further. Examples within each of the five program objectives include:

1. Deny unacceptable applicants initial eligibility for access to classified information. Federal personnel security programs are successfully pursuing changes that should improve program efficiency at the front end. Four noteworthy examples are: (1) a set of e-clearance initiatives, which enables federal workers and government contractors to file security clearance forms electronically, eliminates unnecessary and duplicative paperwork, reduces the burden on people coming into the federal government, allows agencies to access the results of background investigations or view employees clearance forms by searching in a single database, and cuts the time involved in processing clearances while preserving the integrity of investigations; (2) a fee-for-service initiative, which enables certain investigation requesters, such as the military, to be charged directly for each investigative service they request, (3) the Joint Personnel Security Adjudication System (JPAS), which represents the virtual consolidation of the DoD central adjudication facilities (CAFs). JPAS is expected to improve efficiency through the use of a centralized database with centralized computer processing and application programs for standardized personnel security procedures that relate to the entire clearance process; and (4) research on a promising new two-step investigative approach (known as phasing) may provide an option for substantially reducing initial clearance costs without significantly reducing investigative quality. Finally, research suggests that security-related employee screening methods yield additional utility by improving the suitability and productivity of the workforce, e.g., enlisted personnel who pass initial background investigations are less likely to be discharged from military service for reasons of unsuitability. Overall, improvements are likely to yield benefits throughout personnel security programs, reduce the current backlog of investigative cases, and help avoid future backlogs.

2. Deter cleared individuals from engaging in unacceptable behavior. Although there is a dearth of assessment studies regarding the deterrence effects of personnel security education programs or attestation requirements, research involving several thousand OPM periodic reinvestigation cases found that these reinvestigations appear to deter individuals from remaining in a cleared position for which they may not be suitable. Specifically, cleared persons with derogatory issues were more likely to resign prior to the adjudication of their periodic reinvestigation than were persons with very minor or no known issues.

3. Detect, and appropriately follow-up on, evidence indicating that cleared individuals may have become unacceptable to hold a security clearance. Research on military samples has shown that continuing evaluation efforts regarding the cleared workforce surfaces substantial amounts of security-relevant information and results in four to six times more clearance revocations and suspensions than does periodic reinvestigations. Given the extensive period of time between periodic reinvestigations (5-15 years), effective continuing evaluation efforts are critical for reducing the opportunity for cleared individuals to engage undetected in activities that could compromise national security. Work is currently under way to finalize and promulgate a Counterintelligence Reporting Essentials ("CORE") guide, which will improve coworker security reporting requirements by focusing on a smaller set of reportable behaviors related to counterintelligence activities of concern.

In the near future, continuing evaluation efficacy and timeliness in DoD is likely to get a boost from a system known as the Automated Continuing Evaluation System (ACES), a system for automated checks and scoring of key government and commercial databases to identify cleared personnel who may be engaging in acts of security concern in between regular personnel security investigations. Recent analyses of the utility and costs associated with implementing ACES in concert with a phased reinvestigation found that the combination is likely to yield more frequent in-depth detection and follow-up of security-related information at a lower annual cost.

4. Assist cleared individuals who have, or appear to be developing, problems that could interfere with reliable job functioning. Although studies have shown that a subset of employees with suitability problems eventually become security problems if not helped, research revealed complex reasons for many employees not feeling at ease with consulting government employee assistance programs (EAPs). Finding ways to improve EAP use would: (1) limit the potential security risk for persons with suitability problems, (2) significantly reduce suitability problems, and (3) increase the number of individuals who can be retained in their positions, saving organizations from the costs associated with lost personnel. Recommendations for improving this area are under review at DoD.

5. Revoke the clearances of cleared individuals shown to be unacceptable. Given the enormous damage that cleared individuals can cause to national security, it is critical to suspend or revoke clearances when necessary. The revocation rate across the federal community traditionally has been low and there have been no studies suggesting that it should be substantially different. The community has addressed changes in national threats and technology by refining adjudicative guidelines and procedures, and by supporting initiatives such as ACES, which improve revocation-related efficiency and timeliness.

The personnel security program has demonstrated its ability to adopt new ideas and technological advances that improve effectiveness. Future improvements can and should be pursued, e.g., through the appropriate use of technology and automation, by developing policies that provide government-wide standards as well as flexibility to meet agency-specific needs, and by implementing faster and more cost-effective investigation and clearance procedures that do not compromise security concerns.

Costs and Benefits of a Full-Field Versus a Secret-level Investigation

Numerous investigative sources, such as the subject interview, the personnel security questionnaire, reference interviews and records checks, are used in full-field background security investigations, each having its own degree of investigative value. Sources are used to uncover issue-relevant information[1] as well as information that mitigates the significance of derogatory information. Assessing the relative productivity of sources used in investigations is an empirical and justifiable method for evaluating the effectiveness of background security investigations. Each investigative source accounts for a percentage of the total cost of a full-field investigation as well as a percentage of the total amount of issue-relevant information yielded in the investigation.

Because research shows that the Subject Interview is a very productive investigative source by itself, we distinguish gains associated with the addition of the Subject Interview to the Secret-level investigation, from gains that could result from the inclusion of all remaining investigative sources. Analyses of cost and productivity data pertain to: (1) the initial Secret-level investigation (known as a NACLC[2]), (2) the initial full-field investigation for a Top Secret or Q clearance (known as the Single Scope Background Investigation or SSBI), (3) the periodic reinvestigation for a Secret-level clearance (NACLC-PR), and (4) the periodic reinvestigation for a Top Secret level clearance (Single Scope Background Investigation-Periodic Reinvestigation or SSBI-PR). Results indicate that the investigative sources required for the Secret-level clearance combined with the Subject Interview are most cost-effective for surfacing issue-relevant and mitigating information.

[1] "Issue-relevant Information" is information relevant to establishing that an issue is of potential current security concern. It is information that an adjudicator would want to review in making a clearance decision. The Adjudicative Guidelines provide a framework for distinguishing issue-relevant information.

[2] "NACLC" includes National and Local Agency Checks, Credit Reports checks, and completion of a Personnel Security Questionnaire (PSQ).

Extending the logic of the comparison required by H.R. 2417 results in the following question: What investigative approach maximizes the cost-effectiveness of investigative procedures, without decreasing the investigative power to uncover cases requiring an adverse adjudicative action ("actionable cases")? Research in this area with SSBI-PRs resulted in the development of a two-phase reinvestigative approach in which the least productive sources are used only where the most productive sources indicate that further investigation is warranted. Thus, the process of phasing results in a more cost-effective use of investigative resources, minimal loss of derogatory information, and no loss in the detection of actionable cases.

Standards Governing the Denial and Revocation of Security Clearances

Overall, the personnel security adjudication system is working effectively. It can be improved, and work on those improvements is under way. The basic principles underlying the Adjudicative Guidelines are sound, but some updating and clarification is needed to adapt to changing societal conditions. The proposed guideline changes are intended to clarify the adjudicative issues and their potentially disqualifying and mitigating conditions, alleviate ambiguities encountered when implementing the current guidelines, and incorporate new and emerging issues as well as new research findings on traditional issues. Principle recommendations include revising three of the 13 Adjudicative Guidelines—"Foreign Influence," "Security Violations," and "Emotional, Mental, and Personality Disorders"—and adding a 14th guideline on "Gambling Practices." For example, the Foreign Influence guideline should be updated to reflect our increasingly global economy and increasingly multi-ethnic society. The focus should be on conflicting foreign interests and divided loyalties as well as vulnerability to coercion and on foreign business and professional associates, friends and family members.

Adjudicative standards are also reflected in security clearance denial and revocation rates. For example, approximately 3.9% of all DoD adjudicative decisions were unfavorable in calendar year 2002, including an unspecified number of applicants who were eliminated by a prescreening process or by their own decision not to apply for fear of being turned down. However, because this rate results primarily from the strictness level of the guidelines, which can be made more or less strict by policy modifications, the rate alone is not readily interpretable in terms of effectiveness. Determining whether 3.9% represents an efficient and effective rate depends on whether the quality and number of individuals in the cleared workforce is adequate. That assessment has not been conducted for DoD or the federal government as a whole.

Opportunities for Improving Federal Personnel Security Programs

Eleven opportunities for improving federal personnel security programs are listed in three categories based on the extent of previous development underlying each opportunity: (1) Opportunities Based on Extensive Development, (2) Opportunities Based on Partial Development, and (3) Opportunities Based on Preliminary Development.

Opportunities Based on Extensive Development

1. Phased SSBI-PR. As an alternative to the traditional SSBI-PR (“full-field”) security background reinvestigation, the Phased SSBI-PR approach is likely to reduce by approximately 42% the investigative costs on approximately 70% of employees requiring an SSBI-PR—with a reliable expectation that no actionable cases would be missed. Because the Phased SSBI-PR and the traditional SSBI-PR entail the same expectation regarding actionable cases, agencies should be permitted—through revised personnel security policy—to use either approach to satisfy the periodic reinvestigation requirement for Top Secret, Sensitive Compartmented Information (SCI), and Q-level periodic reinvestigations.

2. Automated Continuing Evaluation System (ACES). ACES queries selected commercial and government databases to identify cleared personnel who appear to be engaging in acts of security concern between regular personnel security investigations. Research indicates that ACES not only enhances the timeliness and efficiency of detecting security-relevant information, it also helps identify serious cases that would have otherwise been missed. Implementation of ACES should continue within DoD along with consideration for possible adoption by personnel security programs in other departments of the Executive Branch.

3. Adjudicative Guidelines Revision. One of the best ways to improve the effectiveness of personnel security adjudication is to revise the Adjudicative Guidelines to better define listed security principles and concerns, so that they more directly address emerging areas related to security risk, such as foreign preference among cleared individuals. Such a revised set of Adjudicative Guidelines is under review by the Personnel Security Working Group (PSWG).

4. Automated Financial Disclosure Collection. Executive Order 12968, 50 USC 435 (Pub. Law 103-359), and Section 341 of the Intelligence Authorization Act for Fiscal Year 2004 mandate implementation of financial disclosure programs for people granted regular access to one or more of five categories of especially sensitive types of classified information identified by the order. The Records Access & Information Security (RA&IS) Policy Coordinating Committee of the National Security Council approved a standard set of data elements to be collected in all financial disclosure programs required under the order. A centralized automated data collection system similar to e-QIP should be developed by OPM for those agencies and departments that wish to use it. The software core of that program should be made available to other organizations that chose not to use that centralized collection system because of special security concerns applicable to their populations. This would eliminate the need for each agency to build and pay for its own system, as well as ensure greater interoperability and data standardization.

5. Access to National Driver Register Records. The National Driver Register (NDR) is a central repository of information on individuals whose privilege to drive has been suspended or canceled, or who have been convicted of one or more especially serious traffic-related offenses. All 50 States and the District of Columbia participate in the

NDR. Among the offenses most applicable to personnel security determinations are: (1) operating a motor vehicle while under the influence of alcohol or a controlled substance, (2) failing to stop and provide identification when involved in an accident resulting in death or personal injury, and (3) perjury or knowingly making a false affidavit or statement to officials about activities governed by a law or regulation on the operation of a motor vehicle. Legislation is needed before the Department of Transportation will allow federal agencies and departments to have routine access to this information for personnel security purposes.

Opportunities Based on Partial Development

6. Phased SSBI. Because (1) completed research has consistently indicated that a phased approach will substantially improve the timeliness and efficiency of SSBI-PRs, and (2) in-progress research suggests that similar benefits could be obtained by employing a phased approach to SSBIs (initial "full-field" security background investigations), DoD and other agencies should encourage continued research in this area and determine whether, when, and how to support a policy allowing a phased SSBI to fulfill the requirement for Top Secret, SCI, and "Q"-level background investigations.

7. Adjudication Decision Support. Research on phased reinvestigations, clean-case screening, and automated expert systems suggests that an Adjudication Decision Support (ADS) system could offer significant benefits for improving personnel security clearance processing. Using computer-readable records checks and data from a clearance applicant's personnel security questionnaire (e.g., the SF-86), adjudication decisions for some portion of cases could be made in a more objective fashion, be more consistent and fair, and could be accomplished in less time, thereby reducing personnel security program costs, enhancing productivity, and improving customer satisfaction. As the name suggests, the ADS system would be designed to support adjudicators, not replace them. Research suggests that it is feasible to develop an ADS by combining expert knowledge available in the CAFs with software algorithms that integrate and process this knowledge.

8. Investigative Desk Reference. Because there is no national standard for topics that should be covered or questions that should be asked in personnel security investigations (PSIs), there are substantial differences among federal agencies in the content of their background investigations. The Investigative Standards approved by the National Security Council apply only to what sources should be contacted during an investigation, not to what information should be obtained from those sources or how that information should be obtained. The Adjudicative Guidelines identify topics of security concern, but they are written with language designed to meet the needs of adjudicators, not as guidance for investigators. The need for common guidance for investigators has become more evident and more pressing in recent years due to the widespread privatization of personnel security investigations. Each of these service providers is already conducting investigations for other government agencies. A single source of investigative guidance for these and other contractors would increase efficiency, consistency, inter-agency reciprocity, and quality of investigations. An Investigative Desk Reference (IDR) would serve as a job aid and training aid by providing automated sets of investigative guidance and relevant background information. In form and function, it builds on the success of its adjudicative counterpart, the widely used Adjudicative Desk Reference (ADR). With Community input and support, it could become a program of best practices that represents a voluntary standard for how investigations should be conducted.

9. Model for Predicting Personnel Security Requirements. Because investigative and adjudicative efficiency is limited by an inability to accurately predict and program for military and industry PSI requirements—which constitute the majority of PSI requirements across the federal government, (1) the Army and Navy should be encouraged to complete their efforts to develop a PSI prediction model that is comparable to the Air Force's model, and (2) current efforts to develop a PSI prediction model for industry should continue.

Opportunities Based on Preliminary Development

10. Counterintelligence Indicators. Personnel security programs can improve their understanding of, and approaches to handling, counterintelligence concerns. Research evidence and risk management logic suggest that counterintelligence risks increase relative to the depth, breadth, and years of access the cleared personnel have had to classified and sensitive material. Two potential improvements in this area warrant further support: (1) widespread agency review of the CORE list currently under review by DoD's Counterintelligence Field Activity (CIFA) and Counterintelligence Directorate; and (2) enhancing automated counterintelligence monitoring and assessment systems to help identify and better track cases involving cleared personnel that reflect issues of concern, such as significant inconsistencies related to self-reported foreign travel, financial disclosure information, connections, associations, and contacts; sources of wealth; need to know; handling of classified information; or other work or after work activities.

11. Investigative Quality Assurance Program. Many of the discussions in this report imply a need to better define, measure, and assure investigative quality, which would contribute to improving the effectiveness of security background and clearance procedures, as well as PSI contract monitoring. An investigation quality assurance program should distinguish between the extent to which PSIs (1) comply with formal policy requirements and (2) meet adjudicator, i.e., "customer" needs. Recent research in this area supported by DoD and the intelligence community suggests that good personnel security investigations provide enough relevant information to allow clearance eligibility determinations to be made with confidence. Investigations should satisfy Executive Order 12968 requirements, resolve potentially disqualifying information, be organized and clear, and include all necessary documentation. In accordance with the Privacy Act of 1974, reported information should be complete, accurate, and relevant. Continued community support for efforts to improve investigative quality will result in increased effectiveness of federal personnel security programs.

Table of Contents

List of Figures

List of Tables

Introduction

Background

Congressional Bill HR 2417—*Intelligence Authorization Act for Fiscal Year 2004*—includes the following requirements:

> (a) REPORT REQUIRED—The Director of Central Intelligence (DCI), the Secretary of Defense, the Attorney General, the Director of the Office of Personnel Management (OPM), and the heads of other appropriate federal departments and agencies (as determined by the President) shall jointly submit to the appropriate committees of Congress[3] a report on the utility and effectiveness of the current security background investigations and security clearance procedures of the federal government in meeting the purposes of such investigations and procedures.
>
> (b) PARTICULAR REPORT MATTERS—The report shall address the following:
>
> > (1) A comparison of the costs and benefits of conducting background investigations for Secret clearance with the costs and benefits of conducting full-field background investigations.
> > (2) The standards governing the revocation of security clearances.
>
> (c) RECOMMENDATIONS—The report under subsection (a) shall include such recommendations for modifications or improvements of the current security background investigations or security clearance procedures of the federal government as are considered appropriate as a result of the preparation of the report under that subsection.

The Defense Personnel Security Research Center (PERSEREC) was asked by senior staff at the Director of Central Intelligence Special Security Center (DCI/DSSC) and the Counterintelligence and Security office of the Under Secretary of Defense for Intelligence (USDI/CI&S) to evaluate and synthesize relevant research, reports, and government documentation for consideration in the preparation of a joint report to Congress.

Approach and Report Organization

PERSEREC reviewed relevant personnel security literature, e.g., executive orders, commission reports, Congressional testimony, and research and policy papers, to identify documents and data that address the Congressional report objectives stated above. PERSEREC analyzed the most relevant management and research data to define and assess personnel security program effectiveness and utility. As required by H.R. 2417, we (1) compared the costs and benefits of conducting background investigations

[3] The report is required to be submitted to the Select Committee on Intelligence and the Committees on Armed Services and the Judiciary of the Senate; and the Permanent Select Committee on Intelligence and the Committees on Armed Services and the Judiciary of the House of Representatives.

for Secret clearances with the cost and benefits of conducting full-field investigations, and (2) evaluated the effectiveness of the adjudication guidelines governing denial and revocation of security clearances.

In addition to addressing the specific requirements outlined in H.R. 2417, the current report attempts to address the spirit of the requirement, as reflected by the rationale provided by the Senate Committee on Intelligence, where the report requirement originated[4]. The rationale appears in Senate report 108-044, *Authorizing Appropriations for Fiscal Year 2004 for Intelligence and Intelligence-Related Activities of The United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for other Purposes*, as follows:

> Most publicly known instances of foreign espionage in this country have been committed by persons who legitimately obtained sensitive security clearances before deciding to betray their country. The Committee is concerned that current security investigations, however, focus more upon screening individuals prior to giving them clearances than upon ascertaining their trustworthiness on an ongoing basis. With this in mind, the Committee has requested a report to assess the relative risks of pre-clearance and post-clearance compromise. This report should state whether current approaches address adequately the risk of cleared employees compromising classified information after their period of access to such information has already begun. The report should also make recommendations about how background investigations might in the future be better targeted to historically verifiable counterintelligence vulnerabilities (p. 30).

Senate Report 108-044 also includes a reference to the connection between security clearance procedures, sharing sensitive information, and risks posed by “cleared insiders”:

> Further, the Intelligence Community must recognize that information sharing cannot succeed without revised security policies and technologies. This Bill, therefore, requires several related reports, including reviews of security clearance procedures, the threats to networks posed by ‘cleared insiders,’ and the growing reliance of the United States on foreign hardware and software. Only with a broad approach, encompassing policy and technology and security and sharing, can we achieve the maximum advantages offered by modern information technologies and a highly trained and motivated workforce (pp. 26-27).

Consequently, the current report attempts to review research and frame opportunities for program improvement in light of the original concerns raised by the Senate Committee on Intelligence.

[4] See Senate Bill 1025.

Limits to the Study Scope

Based on language in H.R. 2417, and discussions with DSSC and Department of Defense (DoD) staff at an interim project briefing (Defense Personnel Security Research Center, 2003), the PERSEREC report limits the scope of the study to federal personnel security policies and procedures, including background investigations and adjudication, that serve the "clearance" process, i.e., for determining eligibility to access classified information. Consequently, Special Access Programs (SAPs) and background investigations conducted for positions of trust will not be addressed. Because the focus of the Congressional requirement appears to be on macro-level issues that relate to effectiveness across federal personnel security programs, the PERSEREC report will not focus on personnel security program details and operational differences among the many individual federal agencies. Finally, although security training and education are important aspects of personnel security programs, issues in this area are broad and complex, and are currently being addressed by a Joint Security Training Consortium (JSTC). Therefore, the PERSEREC report will summarize briefly the most relevant JSTC activities (see the "Professional Development of the Security Workforce" section of Appendix A).

Report Organization

The remaining sections of this report begin with an overview of the policies that define federal personnel security programs, with particular attention to the subset of policies that define program goals. This is followed by a discussion acknowledging that any evaluation of effectiveness requires a clear articulation of program objectives, utility, and performance criteria. This discussion provides the context and definitions for a report section that evaluates program effectiveness according to five program objectives and three performance criteria. The next three sections address the three specific Congressional report requirements: (1) the costs and benefits of a full-field versus a secret-level investigations, (2) the standards governing the denial and revocation of security clearances, and (3) opportunities for improving federal personnel security programs. Finally, five supporting appendices include: (A) a brief history of federal personnel security policies, programs, and reform efforts, (B) research and discussion regarding indirect benefits of personnel security programs, (C) a brief overview of public opinion and support for federal personnel security programs, (D) excerpts of summaries and recommendations from a recent (2000) evaluation of the DoD personnel security program, and (E) a description, current as of 2002, of personnel security programs at the Defense Security Service (DSS), Office of Personnel Management (OPM), Department of Energy (DoE), Central Intelligence Agency (CIA), and National Reconnaissance Organization (NRO).

Policies that Define Federal Personnel Security Programs

Overview of Relevant Policies

Efforts to ensure the trustworthiness and reliability of federal government employees date back to the Civil Service Act of 1883, which included a principle of "suitability" as a requirement for federal government employment. This principle was defined as "a requirement or requirements for government having reference to a person's character, reputation, trustworthiness, and fitness as related to the efficiency of the service."

Loyalty requirements became important during World Wars I and II. President Wilson issued an executive order in 1917 that required federal government employees to support government policy. Later that year, Congress passed the Espionage Act of 1917 to punish acts of espionage and interference with military operations. In 1939, Congress passed the Hatch Act to prohibit individuals who advocated the overthrow of the United States government from federal government employment. During World War II, several federal agencies created loyalty requirements. These efforts culminated in March 1947 with President Truman's Executive Order 9835, which required loyalty investigations of Executive Branch employees and denied employment to individuals where there was reasonable doubt about their loyalty.

During the Cold War, national security concerns became increasingly important due to fears that Soviet and international Communism would infiltrate government and industry, and threaten U.S. military and industrial strength. A primary concern was that spies would be recruited from those who were sympathetic to Soviet Union ideology or from those who could be blackmailed or influenced to divulge national security secrets. During the period, The Internal Security Act of 1950, or McCarran Act, was passed "to protect the United States from certain un-American and subversive activities." This act required the registration of Communist-related organizations and made it unlawful for individuals to conceal membership in the Communist party when seeking government employment or using a U.S. passport.

Below, we outline several policies (laws, executive orders, directives) that provide context through the establishment of national security organizations, or directly impact (e.g., by specifying individuals' rights) personnel security programs across the federal government. We follow this outline with a deeper exploration of the key policies that define the goals of current personnel security programs. For more context and details of the history of federal personnel security policies, programs, and reform efforts, see Appendix A of this report.

Executive Order 10450 (Security Requirements for Government Employment, 1953). Executive Order 10450 outlined the fundamental principles for the current personnel security program and is the seminal policy document for the federal personnel security program. This order required that all federal employees privileged to be employed in the departments and agencies of the government be "reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States … to insure that the employment and retention in employment of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security." It specified the general behaviors, activities, and associations for meeting this standard, and required individuals who enter or work in "sensitive" positions that involve federal government service to undergo a background investigation, the scope of which would be determined by the degree of adverse effect the position holder could have on the national security.

Other important executive orders, laws, regulations, directives, and authorities that impact the federal personnel security program include the following:

National Security Act of 1947 (50 U.S.C. 401). This act established the National Security Council and the Central Intelligence Agency.

The Atomic Energy Act (1954) (42 U.S.C. 2011 et seq.). This act created a restricted data classification system to protect restricted data and special nuclear materials related to atomic energy. This classification structure differs from than the structure used for national security clearances.

Public Law 86-36 (National Security Act of 1959). This act established the National Security Agency.

Executive Order 10865 (Safeguarding Classified Information Within Industry, 1960). This order established standards that govern access to classified information for industry employees.

Title 5, Code of Federal Regulations, Parts 731, 732, 736 (Suitability; National Security Positions; Personnel Investigations). These regulations outlined the requirements for making suitability and security determinations for competitive service positions within the federal government. Part 731 specified the criteria for making suitability determinations. Part 732 set forth procedures for determining national security positions within the federal government. Part 736 specified the requirements for personnel investigations conducted by the Office of Personnel Management (OPM).

Public Law 88-290 (Personnel Security in the National Security Agency, 1964). This law revised the Internal Security Act of 1950 to strengthen personnel security in the National Security Agency.

Freedom of Information Act of 1969 (5 U.S.C. 552, as amended). This act provided individuals the right to obtain access to their federal agency records, except to the extent that these records are protected from disclosure by various exemptions or law enforcement record exclusions.

Privacy Act of 1974 (5 U.S.C. 552a, as amended). This act provided individuals with protections against unwarranted invasions of their privacy stemming from federal government collection, maintenance, use, and disclosure of personal information about them. It also established requirements for collecting and retaining information on individuals.

DoD Directive 5200.2-R (1979; as amended 1987). This directive consolidated all Department of Defense (DoD) personnel security programs into one program and described the operational requirements for this personnel security program.

Executive Order 12333 (United States Intelligence Activities, 1981). This order set forth the goals, direction, duties, and responsibilities of various agencies and departments of the federal government with respect to the national intelligence effort. It also outlined general principles for the conduct of intelligence activities.

Executive Order 12356 (National Security Information, 1982). This order prescribed a uniform system for classifying, declassifying, and safeguarding national security information.

Director Central Intelligence Directives 1/14 (Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, 1986, as amended 1994) and 6/4 (Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information, 1998). These directives established adjudication standards for personnel with access to sensitive compartmented information (SCI).

National Security Directive 63 (Single Scope Background Investigations, 1991). This directive established common government-wide background investigative standards for access to Top Secret and SCI.

Executive Order 12829 (National Industrial Security Program, 1993). This order created a National Industrial Security Program (NISP) to safeguard federal classified information that is released to industry personnel. The order consolidated federal industrial security programs and regulations.

Executive Order 12958 (Classified National Security Information, 1995). This order prescribed a uniform system for classifying, declassifying, and safeguarding national security information.

Executive Order 12968 (Access to Classified Information, 1995). Along with Executive Order 10450, Executive Order 12968 is the most significant policy document for the federal personnel security program. The order established a uniform personnel security program for employees who are being considered for initial or continued access to classified information. The order also tasked the Security Policy Board to develop a common set of adjudicative guidelines for determining eligibility for access to classified information and uniform investigative standards for obtaining background information. These Adjudicative Guidelines and investigative standards were issued in a memo from

Samuel Berger, Assistant to the President for National Security Affairs, on March 24, 1997.

DoD 5220.22-M (National Industrial Security Program (NISP) Operating Manual (NISPOM) (1995). Issued pursuant to Executive Order 12829, this document is the operating manual for the National Industrial Security Program.

Fair Credit Reporting Act (15 U.S.C. 1681, as amended in 1996). This act provided protections to individuals regarding the information provided by consumer reporting agencies to employers.

Security Clearance Information Act (5 U.S.C. Section 9101) (1998). This act required criminal justice agencies to provide criminal history information for individuals who are being considered for access to classified information or assignment to sensitive national security duties to certain requesting agencies.

Goals of Federal Personnel Security Programs

Several of the policy documents above include statements of one or more goals of personnel security programs. A standard definition for "goal" is "the final purpose or aim" of an effort[5]. A goal statement is typically broad. We present below key policy statements that articulate such goals for federal personnel security programs. Following this section we argue that evaluating the effectiveness of a program requires the further specification of program objectives and performance criteria.

Executive Order 10450. Executive Order 10450 provides the foundation and legal basis for the current personnel security program. The order states:

> "WHEREAS the interests of the national security require that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States; and
>
> "WHEREAS the American tradition that all persons should receive fair, impartial, and equitable treatment at the hands of the Government requires that all persons seeking the privilege of employment or privileged to be employed in the departments and agencies of the government be adjudged by mutually consistent and no less than minimum standards and procedures among the departments and agencies governing the employment and retention in employment of persons in the federal service." [Introduction]
>
> "The head of each department and agency of the Government shall be responsible for establishing and maintaining within his department or agency an effective program to insure that the employment and retention in employment

[5] *Webster's Revised Unabridged Dictionary, © 1996, 1998 MICRA, Inc.*

> of any civilian officer or employee within the department or agency is clearly consistent with the interests of the national security." [Sec. 2]

Although not explicitly stated, the implicit goal of Executive Order 10450 was to prevent Communist agents from entering government service (Defense Personnel Security Research Center, 1998).

Executive Order 12968. Executive Order 12968 established a uniform personnel security program for federal government employees. The order states:

> "The national interest requires that certain information be maintained in confidence through a system of classification in order to protect our citizens, our democratic institutions, and our participation within the community of nations. The unauthorized disclosure of information classified in the national interest can cause irreparable damage to the national security and loss of human life.
>
> "Security policies designed to protect classified information must ensure consistent, cost effective, and efficient protection of our Nation's classified information, while providing fair and equitable treatment to those Americans upon whom we rely to guard our national security.
>
> "This order establishes a uniform federal personnel security program for employees who will be considered for initial or continued access to classified information." [Introduction]
>
> The "Access Eligibility Standards" section states:
> "eligibility for access to classified information shall be granted only to employees … whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. … Eligibility shall be granted only where facts and circumstances indicate access to classified information is clearly consistent with the national security interests of the United States" [Sec. 3.1(b)]
>
> In the section "Access Eligibility Policy and Procedure," the order states:
>
> "Determinations of eligibility for access to classified information … are separate from suitability determinations with respect to the hiring or retention of persons for employment by the government or any other personnel actions." [Sec. 2.1]

Director Central Intelligence Directive (DCID) 6/4. This directive discusses the general personnel security standards and procedures that govern eligibility for access to Sensitive Compartmented Information (SCI). The stated purpose of this directive is:

> “to enhance the security protection of SCI through the application of personnel security standards, procedures, and continuing security programs. [Sec. 2]

Later, in the section on personnel security standards, the directive specifies the criteria for approving individual’s access to SCI:

> “a. The individual … must be a US citizen.
>
> “b. The individual’s immediate family must also be US citizens.
>
> “c. Members of the individual’s immediate family and any other persons to whom he or she is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power or by persons who may be or have been engaged in criminal activity, nor advocated the use of force or violence to overthrow the Government of the United States or the alternation of the form of Government of the United States by unconstitutional means.
>
> d. The individual must be stable; trustworthy; reliable of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States.” [Sec. 5]

Director Central Intelligence Directive (DCID) 1/19. This directive also discusses security policy for SCI, as well as the concept of risk management:

> “In order to protect SCI, risk-based analysis should be employed when implementing protection measures. Risk management is essential to balance threat and vulnerability with appropriate security measures.” [Sec. 2.0]

Each federal government department and agency also has a separate personnel security (or security) directive, standard, and/or manual. From a personnel security perspective, the largest department is the Department of Defense.

Department of Defense Directive Number 5200.2 (1999). This directive describes the goal of the DoD personnel security program as follows:

> “The [goal] of the Personnel Security Program is that military, civilian, and contractor personnel assigned to and retained in sensitive positions, in which they could potentially damage national security, are and remain reliable and trustworthy, and there is no reasonable basis for doubting their allegiance to the United States.” [3.1]

This directive also states:

> “No person shall be appointed or retained as a civilian employee in a sensitive positive of the Department of Defense, … accepted for entrance into the Armed Forces of the United States, or assigned to duties that require a

> personnel security investigation … unless such appointment, acceptance or assignment is clearly consistent with the interests of national security." [3.2]
>
> "no person shall be deemed to be eligible for access to classified information unless such access is clearly consistent with the interests of national security." [3.3]
>
> "eligibility for access to classified information or assignment to sensitive duties shall be granted only to individuals who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information. [3.4]

Department of Defense Personnel Security Program Regulation DoD 5200.2-R (1987). The stated purpose of the DoD personnel security program regulation is:

> "to establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of civilian employees of the DoD, and granting members of the Armed Forces, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security." [Sec. 1-200]
>
> Later, this regulation describes the "clearance and sensitive position standard" as: "The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security." [Sec. 2-101]

Joint Security Commission. In a report to the Secretary of Defense and the Director of Central Intelligence, the Joint Security Commission (1994) described the goal of the personnel security program as follows:

> "So far as concerns the DoD and the Intelligence Community, the main purpose of personnel security programs is to protect the national security interests of the United States by insuring the reliability and trustworthiness of those to whom information vital to those interests is entrusted." [Chap. 4]

An Alternative Goal Statement. In a 1998 memorandum to the Deputy Director of Security (Defense Personnel Security Research Center, 1998), PERSEREC staff summarized their thoughts regarding the goal of a personnel security program. They suggested the following statement:

> “The objective of the personnel security system is to increase the probability that persons assigned to and retained in positions, in which they could potentially damage national security are and remain reliable, trustworthy, and loyal.”

They argued that this proposed goal statement has several advantages over the existing goal statement. First, this proposed statement emphasizes something positive to be achieved, rather than something negative to be avoided. Second, this statement avoids unattainable expectations (i.e., any damage to national security is considered a program failure). Third, this statement results in a more measurable standard. Finally, this statement encourages the utilization of other programs or procedures that support effective personnel security, such as employee assistance programs and security awareness. Overall, this goal statement provides a more realistic statement for the goals of the personnel security system, one consistent with today’s changing personnel security environment.

Summary of Goal Statements

The primary stated or implied goals of federal personnel security programs include: (1) ensuring that employees are reliable, trustworthy, loyal, and of good character, and (2) taking personnel actions (e.g., accepting and retaining employees) that are consistent with the interests of the national security. Other themes mentioned include: (3) the concept of fairness and equitable treatment, (4) ensuring that employees have good judgment, discretion, honesty, and allegiance to the United States, and (5) having a program that is efficient, effective, consistent, and based on risk management principles.

Considerations Regarding Objectives, Effectiveness, Utility, and Performance Criteria

Because goal statements typically are broad, they provide only limited guidance on how a program should be operationalized, measured, and evaluated, i.e., how program effectiveness should be assessed. Specific program *objectives* are needed to translate desired program goals into operational terms amenable to empirical evaluations of program performance, i.e., *effectiveness* (Rossi, Freeman & Wright, 1979). Well-written objectives suggest measures that can be used to evaluate program effectiveness. Below, we discuss considerations regarding the definition and measurement of effectiveness, objectives, utility, and performance criteria for federal personnel security programs. Based on these considerations we will outline, in a subsequent section of this report, five objectives and three performance criteria for federal personnel security programs.

Objectives and Effectiveness

The manner in which an objective is defined is important because it affects the measures chosen to evaluate that objective. Consider the following example (from Defense Personnel Security Research Center, 1998). If the program objective is to prevent unreliable, untrustworthy, or disloyal persons from gaining or retaining access to classified information, then a relevant measure of program effectiveness is the number of clearance denials and revocations. In contrast, if the objective is to prevent the compromise of classified information, then a relevant measure of program effectiveness is the number and magnitude of espionage cases. Although the General Accounting Office (GAO) (1999) has framed an objective of federal personnel security programs in terms of meeting the cleared manpower needs of government agencies and government contractors, such a statement begs the question of what are such "needs," i.e., exactly what quality of personnel is needed and, aside from simply counting the number of cleared position vacancies, how can we evaluate whether the need is adequately met? Thus, different objectives suggest different measures, which in turn can lead to different conclusions about the effectiveness of a personnel security program.

In the personnel security context, several issues must be considered in developing measures of objectives to assess program effectiveness. Unique challenges associated with including espionage-specific objectives are highlighted.

First, some program objectives are difficult to measure. Ideally, good measures should be relevant to an objective of interest and statistically reliable. For some objectives, it may be difficult to identify measures that meet these standards. For example, vetting and retaining cleared employees who are loyal to American interests is clearly relevant. However, loyalty is difficult to measure, and self-report and interview questions are weak data-gathering methods when applied to employees who pose the greatest risk—those who are motivated to hide their true feelings or disloyal intentions. Consequently, it is difficult to directly employ the concept of loyalty to measure program effectiveness (Palmer & Eisle, 2003).

Second, a lack of information about the expected rate of occurrence, i.e., a base rate problem, for some security-related outcomes makes it difficult to interpret program effectiveness results. For example, without a confident estimate of the total number of individuals who *attempt* espionage each year, it is difficult to interpret program effectiveness by the number of *identified* espionage cases. Consider the following: identifying 20% more spies among cleared personnel from one year to the next may or may not represent good personnel security program effectiveness. For this indicator, an interpretation of effectiveness will depend on whether the total number of espionage attempts, i.e., the base rate, was higher, lower, or the same as the previous year. The problem continues to be that we have no valid method to estimate the espionage base rate.

Third, in the case of espionage, the evaluation of effectiveness is made difficult by the very low rate of identified spies (a few cleared individuals each year, according to unclassified data), relative to the vast number of cleared employees (over two million) at work each year. Thus, identifying spies and reducing their activity are difficult objectives to use in measuring the effectiveness of personnel security programs because over 99.999% of cleared personnel are not distinguishable on a measure of espionage.

Fourth, the scientific literature offers no valid and reliable profile of psychological or behavioral characteristics—short of close contact with spies or a prior history of espionage—to predict espionage behavior. Where profiles have been suggested, as with the finding that individuals who spied against America were most likely to report being motivated by financial gain (Herbig and Wiskoff, 2002), such profiles are not useful in distinguishing individuals at high risk, from the much larger population of low-risk individuals with the same profiles, i.e., although spies are most likely to be motivated by financial gain, most individuals motivated by financial gain are not likely to be spies.

A fifth issue regarding program objectives and their link to effectiveness involves the range of outcomes to include in the assessment of program effectiveness. As previously discussed, security indicators, such as espionage, may be difficult to develop and may be associated with low rates of occurrence. In contrast, suitability indicators, such as drug use, tend to be more measurable and have higher rates of occurrence. However, the relevance of suitability to personnel security goals is less certain, making interpretations of suitability indicators less certain (than security indicators) as assessments of program effectiveness.

Utility

A concept directly related to effectiveness is utility. Whereas effectiveness refers to the accomplishment of program objectives, utility refers to the total value of an organizational program (Boudreau, 1991). Utility analyses are used to assess the total direct and indirect costs and benefits associated with an organizational program.

Utility analysis can serve at least three purposes. First, as mentioned, it can provide information about the value of a program or program procedure. Second, it can provide information about which program procedures to include, e.g., which background investigation sources to use. From a utility perspective, procedures that have additional (incremental) utility beyond the utility obtained using some core set of procedures should be retained, whereas those procedures with limited or negative incremental utility should be excluded. Third, utility analyses can provide information about which procedures to include when program resources are limited. A utility perspective would suggest that those procedures with the highest utility should be retained.

When applied to the personnel security context, there are at least two key issues that must be considered in any utility analysis. First, how should the outcome of the analyses be expressed? It is often difficult to monetize certain costs and benefits associated with the personnel security system (Joint Security Commission, 1994). In such situations, an alternative utility outcome that expresses the benefit in nonmonetary terms (e.g., amount of issue-information produced for a given expenditure of resources) may be more practical and appropriate.

A second issue in applying utility analysis involves the challenges of specifying and measuring the full range of the program or program procedure benefits. For example, the personnel security program has both direct benefits, e.g., reducing security-related concerns such as espionage and sabotage, as well as indirect benefits, e.g., reducing counterproductive behavior. Furthermore, some benefits may not be obvious, e.g., effective personnel security may improve morale (Appendix B includes a fuller discussion of research on indirect benefits of personnel security programs). In addition, some benefits are difficult to measure, e.g., what is the value of preventing espionage?

It should be noted that utility considerations are also consistent with the concept of risk management. Risk management is based on an understanding of the threat, and the capability to measure the cost and risk (Joint Security Commission, 1999). The personnel security system should utilize (cost effective) procedures for the highest threat areas and eliminate less productive procedures. Utility analyses can play a role in making these determinations.

A recent review did not locate any studies that assessed the full utility of the DoD personnel security program (Bosshardt, 2001). However, some indirect evidence was found for the utility of security-related hiring procedures and for the utility of security interventions that were designed to reduce counterproductive behavior. Relevant studies are briefly described in Appendix B.

A final important consideration in evaluating the utility of any program is to address the issue of who ultimately bears the program costs and benefits, i.e., utility for whom? In the case of a federal program, the American public is the primary consumer, benefactor, risk-assumer, and financier. Consequently, it is relevant to ask, to what extent does the American public support the objectives and procedures of federal personnel security programs? The best evidence on this question comes from national public opinion surveys and studies which, taken together, show consistent support, over time, for the requirement for strong security, the need to balance personal privacy against national security, and for the goals and procedures of federal personnel security programs. Relevant highlights from these studies appear in Appendix C.

Overall, a utility perspective forces one to consider the relative costs and benefits of program procedures or elements. Such knowledge, in turn, is invaluable when evaluating the usefulness of program procedures or when making decisions about procedures to include in the program.

Because it was beyond the scope of this report to gather complete financial and other cost data on all procedures of federal personnel security programs, we will evaluate program utility—in two later sections of this report—in terms of: (1) evidence on the degree to which federal personnel security programs effectively meet five primary program objectives, and (2) comparisons of the costs versus productive value of components of a full-field security background investigation. Beyond this, we refer readers to research and discussions of indirect benefits presented in Appendix B. As discussed in the following text, utility should be achieved and program effectiveness must be met, in accordance with acceptable program performance criteria.

Program Performance Criteria

Although programs typically strive to achieve specific objectives and maximize overall utility, the methods, policies, and resources employed to accomplish these aims must adhere to acceptable operational practices, i.e., program performance criteria. For example, it is not acceptable to meet a specified program objective through illegal operations. With respect to federal personnel security programs, performance criteria fall into three categories: timeliness, efficiency, and fairness.

Timeliness refers to the operational deadlines for completing a program objective. The appropriate measures of timeliness for any objective will depend upon the nature of that objective. For objectives involving background investigations and reinvestigations, timeliness criteria should reflect acceptable time limits for gathering and processing investigative information. For example, the recent draft of DoD Directive 5200.2-R, Personnel Security Program Regulation (2002, June), suggests that investigative and adjudicative actions for initial Secret-level investigations should be completed in 75 days, initial Top Secret investigations in 90 days, Top Secret periodic reinvestigations in 120 days, Secret periodic reinvestigations in 120 days, and Special Investigative Inquiries (SIIs) in 90 days. Timelines criteria for some types of objectives may be less exact or irrelevant, e.g., as with a program objective to deter individuals from wrongdoing.

Efficiency refers to the resources expended to accomplish a program objective. For example, for background investigations and reinvestigations, an efficiency measure would evaluate the extent to which personnel security investigations (PSIs) are completed at an acceptable cost.

Fairness refers to the appropriate treatment of program participants. This involves: communicating program requirements or responsibilities in a manner that does not violate policies regarding protected groups, conducting program procedures in a manner that does not infringe on the legal or Constitutional rights of individuals, and providing full and equal treatment for applicants and employees. Measures of these criteria might be reflected in the numbers of formal challenges to program procedures, and group utilization rates for program procedures.

Specifying and assessing these program performance criteria—timeliness, efficiency, fairness—is necessary to evaluate the effectiveness of program objectives.

Summary of Objectives, Effectiveness, Utility, and Performance Criteria Issues

This subsection indicated that program objectives translate the general goals of a personnel security program into more specific and operational statements regarding the desired accomplishments of the program. Such objectives—five are specified in a subsequent section of this report—are important because they impact the perception of the personnel security challenge, the procedures used to deal with the challenge, the measures used for evaluating program effectiveness, and the estimated utility of the program.

Utility was defined as the total direct and indirect costs and benefits associated with a program. Because the manner in which a program raises utility and achieves objectives is important, three performance criteria—timeliness, efficiency, fairness—were defined and proffered as essential in evaluating personnel security program effectiveness. Thus, federal personnel security programs can be assessed as effective to the extent that they meet stated program objectives within performance criteria.

As a final and necessary prelude to outlining specific program objectives and assessing effectiveness, we turn to a discussion of issues regarding the definitions and degrees of program emphasis on security and suitability factors.

Considerations Regarding Security and Suitability

The relationship between direct security issues and indirect suitability issues has important conceptual and practical implications for the personnel security program evaluation. Conceptually, these relationships should be aligned with the goal and objectives of a personnel security program. Practically, the degree of focus on suitability concerns impacts the resources that are expended for the personnel security program.

Definitions of Security and Suitability

The terms security and suitability are not defined in the several key personnel security policy documents, including the Executive Order 10450, Executive Order 12968, or the DoD personnel security program regulation (DoD Directive 5200.2-R, 1987). Below are some definitions of these terms.

Security. Webster's Third New International Dictionary (1986) definition of "security" includes the following:

> "4. something that secures: defense, protection, guard as a: measure taken (as by a military unit) to ensure against surprise attack b: measure taken (as by a national government or a governmental unit) to guard against espionage, observation, sabotage and surprise c: protection against economic vicissitudes d: penal custody"

The DoD Dictionary of Military Terms defines "security" as follows:

> "1. Measures taken by a military unit, activity, or installation to protect itself against all acts deigned to, or which may, impact its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hastily acts or influences. 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interest of national security."

The term “personnel security” is also relevant here. Surprisingly, the DoD Dictionary of Military Terms does not define this term. However, it defined a “personnel security investigation” as follows:

> “An inquiry into the activities of an individual, designed to develop pertinent information pertaining to trustworthiness and suitability for a position of trust as related to loyalty, character, emotional stability, and reliability.”

OPM security regulation [Title 5, Part 732] discusses security determinations for positions in the competitive service. Although this regulation does not define “personnel security,” it states that “national security positions” include:

> “(1) Those positions that involve activities of the Government that are concerned with the protection of the nation from foreign aggression or espionage, including development of defense plans or policies, intelligence or counterintelligence activities, and related activities concerned with the preservation of the military strength of the United States; and (2) positions that require regular use of, or access to, classified information.”

Although it does not formally define “personnel security,” Executive Order 10450 indicates that:

> “all persons privileged to be employed in the departments and agencies of the government, shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.”

Suitability. Webster’s Third New International Dictionary (1986) defines suitability as the “state of being suitable.” The term “suitable” is defined as:

> “1. Matching or correspondent (as in character, condition, or kind): like, similar 2a. adapted to a use or purpose: fit b. appropriate from the viewpoint of propriety, convenience, or fitness: proper, right c. having the necessary qualifications: meeting requirements: apt, qualified.”

The DoD Dictionary of Military Terms does not define “suitability.”

OPM suitability regulation [Title 5, Part 731] describes “suitability” as:

> “based on an individual’s character or conduct that may impact the efficiency of the service by jeopardizing an agency’s accomplishment of its duties or responsibilities, or by interfering with or preventing effective service in the position applied for or employed in, and determinations that there is a statutory or regulatory bar to employment.”

Other Distinctions Between Security and Suitability. An alternate method of distinguishing between security and suitability is to identify factors that are considered security- and suitability-related in key policy regulations and operational forms.

DoD personnel security regulation (DoD Directive 5200.2-R, 1987) lists 17 "criteria for application of security standards." The regulation indicates that criteria 1 to 6 are core security factors and criteria 7 to 17 are suitability factors. The core security factors refer to such actions as sabotage, espionage, treason, terrorism, anarchy, sedition, use of force or violence to overthrow the government, unauthorized disclosure of classified information, and serving the interests of another government in preference to the interests of the United States. The suitability factors refer to disregard of laws or regulations, criminal conduct, poor judgment, unreliability, vulnerability to coercion, financial difficulties, alcohol use, drug use, falsification, refusal to answer questions required by a Congressional committee, and sexual misconduct.

What are the main considerations for including indirect issues (suitability) in personnel security investigations and adjudications?

DoD policy documents (e.g., DoD Personnel Security Program Regulation 5200.2-R, Executive Order 10450) provide no explicit rationale for including indirect issues in the personnel security program, although several explanations, discussed below, have been offered for doing this.

Recent research (Herbig and Wiskoff, 2002) found that 17% of American spies were naturalized citizens (rather than native born Americans), which is approximately four times higher than the rate of naturalized citizens in the general population, and that a substantial proportion of American spies showed evidence of unsuitability related to areas of concern in the Adjudicative Guidelines, e.g., evidence of foreign attachments (44%), inordinate debt (39%), illegal drug use (27%), and immoderate alcohol use (27%). In addition, research from Project Slammer found that some suitability concerns were common among convicted spies (e.g., financial considerations, alcohol abuse, drug use), although other suitability factors were not common (e.g., mental/emotional disorders, criminal conduct) (Reilly & Joyal, 1993). These authors noted that while spies may exhibit both suitability and espionage behaviors, suitability behaviors may be the only behaviors that are observed. It should be noted that the sample in this study was small (n=24).

Reviews of empirical literature have also been offered for including suitability factors in the personnel security program. Heuer (1998) discussed the relevance of each suitability factor for security adjudications in a series of reports on specific suitability factors (e.g., financial irresponsibility, drug abuse, alcohol abuse, criminal behavior (Heuer, 1991a, 1991b, 1992, 1993, 1994).

Some researchers have suggested that suitability problems lead to maladaptive behaviors which, left unrecognized or uncorrected, eventually result in negative outcomes that have serious organizational consequences (Barge, Hough, Kemery, Dunnette, Kanfer, Kamp, & Cardozo, 1984; Shaw, Ruby, & Post, 1998). Barge et al. reviewed the academic literature on behavior reliability and presented a heuristic model of the behavior reliability process, whereas Shaw et al. presented a model to describe the vulnerabilities of Critical Information Technology Insiders. Both present conceptually similar models that describe how loyal employees become disloyal. In both models, employees with predisposing personality traits are likely to show maladaptive behavior when faced with stressful environmental conditions or significant life events. These conditions and events create physiological, psychological or behavioral stress, which leads the employee to use certain coping mechanisms. These coping mechanisms may be maladaptive behaviors, such as anger, depression, anxiety, or unsuitable job behaviors. While these initial maladaptive behaviors generally have few serious organizational consequences, left unrecognized or untreated, these behaviors may escalate into more damaging acts. If the organization fails to either recognize the problem or take proper action, the employee becomes more likely to eventually exhibit serious destructive acts, such as espionage, sabotage, fraud, or violence.

Bosshardt (2000), in interviews with security professionals, identified two additional reasons for including indirect factors in security determinations. First, even though some suitability factors in the Adjudicative Guidelines have only modest relationships with personnel security outcomes, these factors are likely related to other important organizational outcomes such as accidents, errors, damage to equipment, or unintentional compromise of sensitive/classified information. Even if such outcomes are not considered to be security outcomes, they improve organizational productivity and have utility from an organization's perspective.

Security professionals also noted that the inclusion of indirect factors in the personnel security program is important for ensuring program credibility. An example may clarify this point. A December 1999 *USA Today* article found that the Defense Office of Hearings and Appeals (DOHA) had granted clearances to military contractors with histories of substance abuse, financial problems, sexual misconduct and criminal behavior. As a result, four U.S. senators threatened to amend a Pentagon funding bill with legislation that would deny clearances to individuals who have been convicted of crimes punishable by prison terms of more than one year (Pound, 2000). Although subsequent research found that 86% of similar DOHA cases actually resulted in clearance denials (Crawford, Youpa, & Hagan, 2000), the example highlights how program credibility has practical implications for the personnel security program.

Some Implications of Including Suitability Factors

Finally, it should be noted that there are several practical implications associated with including suitability concerns within the personnel security program.

One implication is confused or unbalanced program priorities (Builder, Jackson, & Starr, 1988). These researchers suggested that those objectives that are most easily addressed (e.g., suitability concerns) would be given greater emphasis than objectives that are less easily addressed (e.g., security concerns).

A second consequence is the enormous amount of resources that are expended to gather suitability information. The current investigative and adjudicative processes focus largely on suitability concerns. As noted earlier, the DoD personnel security regulation 5200.2-R, includes more suitability factors (11) to be considered than security factors (6). In addition, these suitability factors tend to have higher base rates than the security factors, which results in proportionally more resources being devoted to suitability factors.

A third consequence of incorporating suitability within the personnel security framework involves the difficulty of integrating suitability screening within a larger system that includes screening for: (a) general federal government employment, (b) access to sensitive (but unclassified) information, and (c) access to classified information. All three screening programs currently evaluate suitability factors. However, these multiple suitability screenings result in duplicative steps, employee processing delays and confusion on the part of applicants and organization officials (Commission on Protecting and Reducing Government Secrecy, 1997). (This commission is often referred to as the Moynihan Commission after its chair, Senator Daniel Patrick Moynihan.)

Summary of Security and Suitability Issues

Overall, the distinctions between security and suitability are somewhat blurred. Suitability refers to an individual’s fitness or appropriateness for employment and whether an individual can reasonably be expected to promote the efficiency of the federal government. Security is a broader term that not only includes an individual’s suitability, but his/her trustworthiness, reliability, and loyalty, and considers whether an individual’s employment or retention can be expected to be consistent with the nation’s security interests. Additionally, there are undoubtedly other indirect factors that are rarely discussed explicitly in security regulations but, as with certain suitability issues, can impact security risk. For instance, incompetent work performance that creates security risk could also be considered a legitimate concern of personnel security programs in that classified systems and documents can be inadvertently compromised by incompetent cleared personnel.

The distinctions between security, suitability, and competency imply the need to develop a personnel security risk management model. Such a model would help personnel security programs address direct security-related issues and, for indirect issues such as suitability or competency issues, only those attributes of cleared individuals that can be reliably associated with an eventual risk to sensitive information, systems, and infrastructure. For assessing program effectiveness and allocating resources appropriately, it will be important to clearly define the extent to which personnel security programs focus on security, suitability, and other issues.

Evaluating Effectiveness Through Key Objectives and Performance Criteria

As previously discussed, evaluating program effectiveness requires: (1) translating broad program goals into more specific operational objectives, and (2) establishing program performance criteria. The focus of each program objective and performance criterion will drive what kind of evidence is gathered and how results are framed in terms of program effectiveness and utility.

No authoritative personnel security policy statement or report has yet articulated a comprehensive set of program objectives and performance criteria for federal personnel security programs. However, the various goal statements discussed earlier, along with the recommendation by Congress (e.g., Senate Report 108-044) and others (e.g., DoD Insider Threat Integrated Process Team, 2000) that personnel security should focus on mitigating insider threat, rather than simply protecting classified documents, suggests five objectives for federal personnel security programs. The set of five objectives along with three performance criteria—timeliness, efficiency, and fairness—will constitute the framework for evaluating the effectiveness and utility of federal personnel security programs.

Objective 1: Deny unacceptable applicants initial eligibility for access to classified information (i.e., a security "clearance")

Objective 2: Deter cleared individuals from engaging in unacceptable behavior

Objective 3: Detect, and appropriately follow-up on, evidence indicating that cleared individuals may have become unacceptable to hold a security clearance

Objective 4: Assist cleared individuals who have, or appear to be developing, problems that could interfere with reliable job functioning

Objective 5: Revoke the clearances of cleared individuals shown to be unacceptable

An "unacceptable" individual is defined as one who is not likely to be reliable, trustworthy, and loyal to the U.S.—which speaks to the overriding goal of personnel security programs—as determined through an application of the Adjudicative Guidelines by an authorized government representative. As suggested earlier, there are severe difficulties related to collecting extensive and valid empirical data on individuals' trustworthiness, loyalty, and reliability, as well as objective predictive links between these factors and national security outcomes, such as espionage. Consequently, security clearance procedures and the Adjudicative Guidelines have been developed through years of investigative and security-related experience concerning practical and logical risk factors for security (e.g., persons who commit crimes and then try to hide their involvement are likely to be unacceptable in a cleared position). Research on many of the concerns represented in the Adjudicative Guidelines has shown a link between the concerns and security-relevant performance problems at work (e.g., Personnel Security Managers' Research Program, 2003a, 2003b, 2003c, 2003d).

We introduce this section with a summary of background factors regarding the changing national security environment that: (1) support using this framework of objectives, and (2) has led to a number of personnel security program evaluation and reform efforts. Following the background discussion, each of the five program objectives, along with relevant performance criteria, will be discussed in term of what evidence exists, or is needed, to evaluate the effectiveness and utility of federal personnel security programs. Because the performance criterion, "fairness," involves a discussion that cuts across many of the objectives, this criterion is discussed after the presentations on the five objectives, and is followed by an overall section summary. Finally, to address the requirements of H.R. 2417 and the scope limitations for the current report, the discussion below: (1) takes a macro-level perspective and does not focus on personnel security program details and operational differences among the many individual federal agencies (a descriptive overview of personnel security program operational differences among DoD, OPM, DoE, NRO, and CIA, as of 2002, appears in Appendix E), and (2) acknowledges the importance of security training and education, but recognizes that these areas are not primary program objectives and are currently being addressed by a Joint Security Training Consortium (see Appendix A, section on "Professional Development of the Security Workforce").

Background

Today's personnel security programs must adapt to several important changes in the national security environment (Bosshardt, 2000; Heuer, 1999; Defense Personnel Security Research Center, 1998; Kramer, Heuer & Crawford, in review). These include: (a) the growth in automated information systems, (b) changes in foreign threats toward economic espionage, (c) changes in American business practices as corporations become increasingly global entities, (d) changes in DoD acquisition practices as military technology is increasingly developed in the private sector for commercial uses and adapted to military needs, (e) increases in the vulnerability of individuals to financial pressures, (f) changes in the diversity and attitudes of the American workforce, and (g) increases in the use of contractors to provide personnel security investigation services. Overall, these trends imply that insider threats will increase, personnel in sensitive positions will be able to do more damage to national security, information technology system misuse will become more critical, financial considerations and foreign associations will become more important, and pressures to monitor and improve personnel programs will increase. All this must be considered in the context of a federal population consisting of millions of cleared individuals. Although the exact number of cleared individuals is classified, in DoD alone (excluding cleared contractors), 2002 counts show a total of about 1.9 million cleared individuals, including 243,316 SCI; 136,244 Top Secret; 1,442, 398 Secret; and 35,347 Confidential (J.R. Goral, personal communication, October 21, 2003).

Personnel security programs must also adapt to several system constraints. These include legal considerations, public attitudes (see appendix C), and operational pressures (Bosshardt, 2000). For example, various legal considerations (e.g., Privacy Act, Fair Credit Reporting Act, Freedom of Information Act) that were not in existence when Executive Order 10450 was created offer greater protections to individuals and make it more difficult to gather security-related information. Changing public attitudes toward security impact the passage of security-relevant legislation and regulations, the willingness of potential applicants to apply for access to classified information, and the attitudes and conduct of security professionals and employees in cleared positions (Smith, 1996). Operational pressures, e.g., due to business processes that primarily reward PSI completion speed, can result in overlooked derogatory conduct of applicants and cleared employees.

In addition, differences in agency-specific missions and security threats have sometimes been used to argue that certain agencies, such as intelligence organizations, require a stricter approach to vetting and adjudication than do other agencies. Although it is difficult to find reliable data collections on which to justify such assertions, it is not unreasonable for agencies to want personnel security policies and procedures that are flexible enough to address their specific concerns. The need to balance agency-specific needs against federal-wide consistency has been a source of occasional tension.

Finally, today's personnel security program must operate within a broader organizational context that includes other programs and procedures that impact the reliability, trustworthiness, and loyalty of cleared persons (Bosshardt, 2000; Defense Personnel Security Research Center, 1998). These include military enlistment policy, prescreening, hiring practices, security awareness and education, employee assistance programs, physical security programs, information security programs, and counterintelligence. While the distinction between some of these procedures and procedures with personnel security programs is sometimes blurred, the impact of these other procedures on the effectiveness of personnel security programs is almost certainly significant (Defense Personnel Security Research Center, 1998).

As a result of these findings, trends, and constraints—as well as operational problems, such those associated with the initial implementation of the DSS Case Control Management System and a backlog of over 500,000 PSIs—many have called for evaluations and reforms in personnel security programs (e.g., Anderson, 1996; Builder, Jackson, & Starr, 1988; CODA (1999); DoD Office of the Inspector General, (1997, 1998, 2000a, 2000b, 2000c), General Accounting Office (1995, 1999, 2000); Department of Defense Security Review Commission, 1985; Joint Security Commission, 1994, 1999; Commission on Protecting and Reducing Government Secrecy, 1997; Personnel Security Investigations Process Review Team, 2000b; see also Appendix A). The most recent of these efforts—by the Personnel Security Investigations Process Review Team[6] (PSI-PRT, 2000b)—included: (1) a review, synthesis, and update of previously published reform recommendations, (2) a list of 29 "observations," i.e., descriptions of program needs, issues, and problems, and (3) a set of program recommendations.

[6] The PSI-PRT (2000b) evaluation focused primarily on the largest federal personnel security program (DoD). However, because the DoD program also served many of the PSI needs of the White House, several intelligence agencies, and their central adjudication facilities (e.g., WHS, NSA, and DIA), several of the PSI-PRT findings and recommendations apply to the intelligence community and non-DoD organizations as well.

Because the PSI-PRT (2000b) effort was the most recent and thorough personnel security program evaluation, we include in Appendix D a list of its summaries of prior evaluation recommendations and its own forward-looking recommendations. However, we do not orient the following current evaluation of program effectiveness around results of the PSI-PRT (2000b) report because: (1) the PSI-PRT report did not frame evaluations around clear definitions of personnel security program effectiveness, objectives, and performance criteria, which makes it difficult to interpret program significance of some report findings, (2) many of the report recommendations address acute, DoD-centric, or fine-grained operational problems, e.g., a recommendation to "develop procedures for returning incomplete (PSI) request packages," and (3) more than half of the recommendations have been overcome by recent events, such as the dismantling of the Security Policy Board and the impending transition of most DoD PSI responsibilities from DSS to OPM. Instead, in keeping with the Congressional requirement in H.R. 2417, we attempt in the following presentation to primarily address current federal-level program objectives and effectiveness.

Objective 1. Deny Unacceptable Applicants Initial Eligibility for Access to Classified Information (i.e., a Security "Clearance")

One way to determine whether personnel security programs are effective in denying unacceptable applicants an initial clearance is to examine clearance denial rates. With respect to DoD, which accounts for the largest number of federal clearances, approximately 3.9% of all adjudicative decisions were unfavorable in calendar year 2002, including an unspecified number of individuals who did not complete the initial clearance process due to "loss of jurisdiction," a prescreening process, or by their own decision not to apply for fear of being turned down. The Department of Energy has reported comparable percentages for its Personnel Security Assurance Program (Department of Energy, Office of Security, 2003).

As described in the report section below on "Standards Governing the Denial and Revocation of Security Clearances," the 3.9 percentage rate represents a level of screening that can be raised or lowered by tightening or loosening adjudicative standards. Should the standards be tightened or loosened? Have personnel security programs given clearances to too many individuals who should not be trusted with sensitive duties? To determine whether this or any clearance denial rate represents an acceptable level of program effectiveness depends on two assessments: (1) whether the actual trustworthiness, reliability, and loyalty of individuals in the cleared workforce is acceptable, and (2) whether the number of individuals in the cleared workforce is adequate for the government's needs.

With respect to #1, the assessment of the actual trustworthiness, reliability, and loyalty of individuals in the cleared workforce has not been conducted for the entire federal government or separately for DoD. For reasons, primarily measurement challenges, described earlier in this report, it would be very difficult to conduct such an assessment. In lieu of a reliable assessment of the cleared workforce quality, this aspect of effectiveness is reduced to a question of whether personnel security program managers and policy makers are comfortable with the assumption that the standards and application of the Adjudicative Guidelines are having the desired effect.

With respect to #2, evidence suggests that vacancies in cleared positions have existed (primarily in DoD) not because of a lack of qualified applicants, nor because the adjudicative standards have been too strict, but because in recent years DSS had accumulated a backlog of PSI cases that were experiencing unacceptably long processing delays (e.g., OASD, C3I, 2001; GAO, 1999; GAO, 2004). This constituted evidence of a program effectiveness problem. Although the responsibility for the majority of DoD PSI requirements (as of Oct 1, 2003) was transferred to OPM, PSI timeliness problems persist (described below).

The intelligence community has often used the polygraph as an additional screening tool for initial clearances. Despite a clear determination by the National Academy of Sciences that the accuracy of polygraph testing is "insufficient to justify reliance on its use in employee security screening" (National Research Council, 2003), the Department of Defense may enable greater polygraph use. Language in the 2004 Defense Authorization Act would: (1) “remove existing limits on the number of polygraph examinations that the Department of Defense may administer" and (2) eliminate the annual reporting requirement on the DoD polygraph program, substituting the public report with a requirement of the Secretary of Defense “to make information on polygraph testing "available to the congressional defense committees." To the extent that a tool’s efficacy is linked to its accuracy, the NAS conclusions suggest that a replacement for the polygraph is necessary.

Timeliness

Although DoD’s DSS had been criticized for unacceptably long PSI processing times, the recent transfer of the majority of DoD PSI work to OPM suggests that we examine OPM’s published PSI timeliness standards for an initial Secret-level background security investigation (NACLC), a Top Secret or “Q” level investigation (known as a Single Scope Background Investigation or “SSBI”), and the periodic reinvestigations (PR) for both. The following are examples of OPM’s “standard” PSI processing times[7].

- NACLC: 75 days
- SSBI: 75 days
- NACLC-PR: 75 days
- SSBI-PR: 180 days

Because these standards are currently under negotiation with DoD and are comparable to timeliness standards listed in the recently updated draft of DoD’s personnel security program policies (DoD Directive 5200.2-R, Personnel Security Program Regulation, draft, June, 2002), we can assume that they represent acceptable federal benchmarks for processing Secret and Top Secret-level investigations.

[7] OPM also offers “accelerated” and “priority” (i.e., faster) PSI processing services for higher reimbursement rates.

As of September 10, 2004, approximately 28.3% (91,154/321,951) of OPM pending investigations were more than 180 days old (Defense Security Service, 2004). Among the overdue investigations, 40,081 (44%) were more than 360 days old. Timeliness problems have been persistent, e.g., as of May 28, 2004, 29.6% (82,890/279,635) of pending investigations were more than 180 days old, including 50,517 (60.9% of the overdue cases) that were more than 360 days old.

Efficiency

The efficiency regarding objective 1 can be addressed through three considerations, some of which have implications beyond objective 1:

1. Is the cost of initial clearance vetting worth the benefit to national security? Because the nation must ensure security, policymakers address this issue primarily by looking for ways to improve personnel security program efficiency, e.g., by reducing program costs without incurring significant additional risk to security. Such improvements are further addressed below in items 2 and 3.

2. Among current PSI providers, are there systems or operations related to initial clearances that could be improved, resulting in substantially lower costs without incurring unacceptable risk? The answer is yes. It is likely that many, if not all, federal personnel security programs pursue changes that improve program efficiency, e.g., through greater automation. Although it is beyond the scope of this report to detail the variety of such improvements, estimate aggregate costs, or assess the overall benefits among personnel security programs, three examples of noteworthy improvements (a-c) are presented followed by an example of a current efficiency problem.

> (a) **Joint Personnel Security Adjudication System (JPAS).** JPAS represents the virtual consolidation of the DoD CAFs. When fully implemented, JPAS is expected to improve efficiency through the use of a centralized database with centralized computer processing and application programs for standardized personnel security processes that relate to adjudication, such as: (1) automating both core and CAF-unique functionality, (2) providing "real-time" information regarding clearance, access and investigative status to security personnel and authorized organizations, e.g., DSS, Defense Manpower Data Center, Defense Civilian Personnel Management System, OPM, and Air Force Personnel Center, and (3) providing comprehensive and up-to-date reporting capabilities across adjudicative activities.
>
> (b) **E-Clearance**. As of 2003, federal workers and government contractors can file security clearance forms electronically. The electronic filing system, developed by OPM as part of a three-step e-clearance project, allows employees to fill out their SF-86 and SF-86C forms on a password-protected Web site. The SF-86C reduces the amount of paperwork from 13 pages to two which workers must complete to renew security clearances. Employees and contractors can save their work

as they fill out the form, enabling them to complete it over an extended period of time if desired. The e-clearance initiative will eliminate unnecessary and duplicative paperwork, reduce the burden on people coming into the federal government, cut time involved in processing clearances, while preserving the integrity of investigations. A second component of e-clearance technology allowing agencies to create digital images of investigative files has also been deployed. This new system will save time and space, allowing OPM to process an annual average of roughly 2 million new background investigations more efficiently. OPM has also made progress on the Clearance Verification System, the third major component of e-clearance, which will allow agencies to access the results of background investigations or view employees clearance forms by searching in a single database. Until recently, most civilian agencies tracked employees clearance histories in separate databases. OPM has transferred more than 90% of background check and clearance files to the new database. OPM has not been able to provide estimates of how much the e-clearance project will cost, but has said the initiative will save taxpayers millions of dollars over the next 10 years, because the streamlined security clearance system will process forms in one tenth the time of the prior process (Gruber, 2003).

(c) **Fee for Service**. Instead of allowing PSI requesters, such as military services, to submit as many PSI requests as they choose (against an aggregate annual budget that may or may not prove to be adequate), a fee-for-service arrangement involves charging PSI requesters directly for the services they request. OPM found that a similar arrangement resulted in substantially improved efficiency (Joint Security Commission, 1994).

An example of an efficiency weakness concerns DoD's limited ability to accurately predict military and industry PSI requirements, which constitute the majority of personnel security requirements across the federal government. With the exception of a newly developed Air Force prediction model, no reliable method is currently in place to predict DoD personnel security requirements[8]. Without this ability, it is difficult for DoD to budget accurately for investigative and adjudicative work, or forecast the effects of policy changes on the personnel security program.

3. Could initial clearance costs be lowered by identifying investigative elements that can be eliminated without significantly reducing PSI quality? Because the answer appears to be yes with respect to an approach known as a phased reinvestigation (Kramer et al, 2001), this bodes well for a similar approach to initial investigations (Kramer & Richmond, in press). This topic relates directly to a question posed in H.R.

[8] The Office of the Deputy Undersecretary of Defense for Intelligence (Counterintelligence and Security) has encouraged each of the military services to develop a personnel security prediction model. The Air Force has made exceptional progress in this area. Predicting industry requirements is more difficult (e.g., because of the probabilistic nature of securing government contracts and the lack of a centralized industry coordinating body) and will require a substantially different model than any used for a military service. PERSEREC is currently working with staff at the DSS Central Requirements Office to explore possibilities for improved prediction of industry personnel security requirements.

2417 and is addressed in the following report section on “Costs and Benefits of a Full-Field Versus a Secret-level Investigation.”

Utility Considerations

A growing body of research suggests that security-related employee screening methods improve the suitability and productivity of the workforce. For example, research has shown that enlisted personnel who pass initial background investigations are less likely to be discharged from military service for reasons of unsuitability (Crawford & Wiskoff, 1988; Flyer, 1986). Research in the field of personnel psychology has shown that security-related screening procedures predict various counterproductive behaviors/outcomes (Ones, Viswesvaran, & Schmidt, 1993), such as turnover (Hunter & Hunter, 1984, Schmitt, Gooding, Noe, and Kirsch, 1984), absenteeism (Helm and Associates, 1985; Hough, 1986), theft (e.g., Longmore-Etheridge, 1999; Ones et al., 1993), and substance abuse (Barge & Hough, 1983). In addition, a recent study indicated that security prescreening could improve the cost-effectiveness of vetting applicants for positions within the intelligence community (Hein, 2002). Finally, one can logically assume that the appearance of rigorous programs for initial access determinations will, to some degree, dissuade unacceptable applicants and would-be spies from applying for a security clearance, although research has not determined the degree to which federal personnel security programs benefit from this effect.

Objective 2. Deter Individuals from Engaging in Unacceptable Behavior

Once individuals have eligibility to access classified information, a challenge for personnel security programs is to increase the likelihood that these persons remain reliable, trustworthy, and loyal. This can be achieved in a number of ways, such as detecting security-relevant problems (Objective 3), intervening to help correct emergent security-relevant problems (Objective 4), and, in the most serious cases, revoking the clearances of unacceptable individuals (Objective 5). In addition, an effective personnel security program should try to deter or curtail the development of security-related problems.

In practice, personnel security programs try to deter unacceptable behavior through security education programs (e.g., DoD requires cleared personnel to have an annual security refresher briefing that highlights security responsibilities and the potential negative consequences for violations) and continuing evaluation programs (e.g., periodic reinvestigations, ongoing coworker reporting requirements and, in some facilities, random drug testing). In addition, as of 1999 DoD required all cleared personnel—for Top Secret (TS), Sensitive Compartmented Information (SCI), and Special Access Programs (SAPs)—to make a witnessed verbal attestation (after access is initially granted or at the first periodic reinvestigation of already cleared personnel) of their commitment to protect national security information and to adhere to the provisions stated on Standard Form 312 “Classified Information Nondisclosure” and or the SCI/SAP Indoctrination Form (DoD, OASD, 1999).

There is limited empirical evidence on the extent to which personnel security programs deter individuals in cleared positions from exhibiting unacceptable behavior. Recent research from a study involving several thousand OPM periodic reinvestigation cases found that periodic reinvestigations may deter individuals from remaining in a cleared position for which they may not be suitable (Timm, 2001). Specifically, this study found that cleared persons with derogatory issues were more likely to resign prior to the adjudication of their periodic reinvestigation than were persons with very minor or no known issues. Furthermore, the more serious the derogatory issues were, the more likely the individual was to withdraw. No studies could be located that linked education programs directly with positive deterrence effects. No studies could be located that linked the DoD attestation requirement with positive deterrence effects, or whether the requirement was being consistently observed.

Efficiency and Timeliness

Although deterrence effects have the potential to be cost effective in that they limit both the number and severity of security- and suitability-related problems, no data could be found that compared estimated resource use against deterrence outcomes. Timeliness standards do not apply to this objective.

Objective 3. Detect, and Appropriately Follow-Up On, Evidence Indicating That Cleared Individuals May Have Become Unacceptable to Hold a Security Clearance

Executive Orders 10450 and 12968 indicate that personnel security programs should ensure that the retention in employment of cleared personnel is clearly consistent with the interests of national security. Stated differently, personnel security programs should provide continuing evaluation of cleared individuals.

Several factors highlight the importance of procedures that monitor the reliability, trustworthiness, and loyalty of cleared individuals. First, as insiders, many cleared personnel have the capacity to cause significant damage to national security. Second, initial screening will always be imperfect since it relies on past behavior that may have occurred years ago to predict future security-related behavior, and makes predictions about situations (protecting classified or sensitive information) that an applicant has not experienced (Perry, Bennett, & Wood, 1979). Third, individuals who are reliable, trustworthy, and loyal at the time of hire may undergo behavioral changes in response to personal or environment situations. Fourth, some research findings suggest that persons with suitability problems may eventually become security problems if not helped (Barge et al., 1984; Shaw, Ruby, & Post, 1998; Wood and Fischer, 2002). Finally, effective continuing evaluation is likely to reduce unsuitable job behavior, which has potentially significant benefits for an organization (Heuer, 1998).

In addition, research on convicted spies suggests that relatively few espionage offenders entered government service with the intent of committing espionage (Herbig and Wiskoff, 2002; Reilly & Joyal, 1993). Such research indicates that many of these espionage offenders may have been acceptable applicants at the time of their initial background investigation, but later turned to espionage as a result of personal and environmental circumstances. Consequently, many have called for greater emphasis on what happens to cleared employees after they have been assigned to a sensitive position—versus what happens before they are accepted into such positions—(e.g., Commission on Protecting and Reducing Government Secrecy, 1997; Defense Personnel Security Research Center, 1998; Personnel Security Investigations Process Review Team, 2000b).

Overall, these considerations suggest that effective personnel security programs must have: (1) effective programs for detecting individuals who are unacceptable for cleared positions and (2) policies and procedures that enable necessary follow-up action in such situations.

With respect to effectiveness, research has shown that continuing evaluation surfaces substantial amounts of derogatory information (Bosshardt, DuBois, & Crawford, 1991) and results in four to six times more clearance revocations and suspensions than does periodic reinvestigations in military samples (Bosshardt, DuBois, Crawford, & McGuire, 1991). Given the extensive period of time between periodic reinvestigations (5-15 years[9]), effective continuing evaluation efforts are critical for reducing the opportunity for cleared individuals to engage undetected in activities that could compromise national security.

Coworker reporting is another opportunity for detection of security-related problems. Although there is a requirement for cleared coworkers to report derogatory security-relevant knowledge that they become newly aware of regarding another cleared individual (Department of Defense Personnel Security Program Regulation DoD 5200.2-R, 1987), there is evidence that many individuals find the requirement ill-defined, e.g., the requirement included items that did not appear to relate directly to security risks, and so individuals often choose not to report (Wood & Marshall-Mies, 2003). Work is currently under way to improve the reporting requirement by focusing attention on a smaller set of reportable items—Counterintelligence Reporting Essentials (CORE)—consisting primarily of clear behavioral examples of counterintelligence related activities of concern (Wood, Crawford & Lang, in review).

In the near future, continuing evaluation efficacy in DoD is likely to get a boost from a system that is currently being developed known as the Automated Continuing Evaluation System (ACES). ACES will provide a system for automated checks and scoring of key government and commercial databases—e.g., personnel security questionnaire records, national credit vendor databases, FBI criminal history files, U.S. Customs databases on foreign travel, federal court records, and others—in order to identify cleared personnel who may be engaging in acts of security concern in between regular personnel security investigations. When fully implemented, ACES should greatly enhance access to and assessment of security relevant information sources on cleared personnel for use by JPAS and other authorized agencies (Chandler, Timm, Massey, & Zimmerman, 2001).

[9] A periodic reinvestigation is required every 5 years for a Top Secret clearance, 10 years for a Secret clearance, or 15 years for a Confidential clearance.

ACES is currently being beta-tested on DoD personnel cleared at the Top Secret and SCI levels.

Efficiency and Timeliness

Recent analyses by PERSEREC (Crawford & Timm, 2002) estimated the utility and costs associated with implementing ACES in concert with a two-phase reinvestigation (in place of the standard 5-year SSBI-PR). The following report section on "Costs and Benefits of a Full-Field Versus a Secret-level Investigation" contains a discussion of a phased investigative approach. That study and more recent analyses at PERSEREC found that the added costs of running and following up on annual ACES checks—which are expected to surface information that would instigate investigations on approximately 5% of individuals cleared at the Top Secret and SCI levels—would be more than offset by the reduced costs associated with a phased periodic reinvestigation. Thus, the net result of implementing both programs is likely to be more frequent in-depth detection and follow-up of security-related information and at a lower annual cost.

Objective 4. Assist Cleared Individuals Who Have, or Appear to be Developing, Problems That Could Interfere With Reliable Job Functioning

Personnel security programs regularly evaluate millions[10] of cleared individuals in the workplace, the majority of whom have no intention of committing a security offense but may—over a period of time or in changing contexts—develop temporary personal problems, such as serious financial difficulties or increasing alcohol use, that could result in their becoming a security risk. An objective of personnel security programs should be to identify people who need assistance in taking care of personal problems. Counseling or other treatment at employee assistance programs (EAPs) should be provided while the problem is new, rather than waiting until it is full-blown and the person may become desperate or present a security risk.

Thus, government has attempted to move away from the earlier strict law-enforcement model of personnel security where no defects were tolerated. That was a system that removed problem people simply by separating them from federal employment. The 1986 Executive Order 12564, Drug-free Federal Workplace, was issued in an effort to eliminate the use of illegal drugs by all federal civilian employees. The order required that the government "…show the way towards achieving drug-free workplaces through a program designed to offer drug users a helping hand…" Later, in the 1995 Executive Order 12968, Access to Classified Information, emphasis was placed on retaining personnel while they dealt with their problems through counseling, medical treatment, or life-skills development in EAPs. The aim has been to get individuals back as soon as possible to performing the function for which they had been employed and trained.

[10] Although the total number of cleared individuals across the federal government is classified, DoD alone accounted for nearly two million clearance holders in 2002, not including cleared contractors.

Executive orders may offer “a helping hand,” but a tension exists between the orders and agency level of security policy. Security pulls one way (it wants clean employees), whereas EAP policies pull the other (they want cleared employees to get help). Government cleared workers are often reluctant to avail themselves of EAP services for fear that confidentiality, a supposed feature of EAP programs, might be breached. As a result, security personnel might discover that they had attended an EAP and were, therefore, a possible security risk. A PERSEREC study (Wood & Fischer, 2002) interviewed 146 individuals mostly in DoD, including adjudicators, policymakers, DoD EAP personnel at headquarters, and individuals at 10 military installations, such as security and EAP personnel, contractors, and chaplains. Focus groups revealed complex reasons for employees not feeling at ease with consulting government-mandated EAPs. Often, they would go “off the base” to confer with private psychiatrists and other counselors.

Other research has shown that a subset of employees with suitability problems eventually become security problems if not helped (Barge et al., 1984; Shaw, Ruby, & Post, 1998). Research on convicted spies suggests that inadequate employee assistance programs (EAPs) were a factor in some espionage cases (Reilly & Joyal, 1993). This research indicated that espionage was a means to solve personal problems for some spies and that inadequate EAPs were a factor in their failure to seek assistance at an early stage.

Programs that encourage the utilization of effective assistance to individuals with problems should yield several benefits. Such programs should: (1) limit the potential security risk for persons with suitability problems, (2) significantly reduce suitability problems, and (3) increase the number of individuals who can be retained in their positions, saving an organization from the difficulties and expense that are associated with lost personnel. The problem appears to be, in DoD at least, getting people to use these services. No research has reliably estimated the number of cleared individuals with early-stage or serious personal problems who choose not to request EAP services.

Efficiency and Timeliness

Executive Order 12968 mandated that EAP information be included in security education programs for the cleared workforce. Every department or agency in the federal government is required to offer EAP services to its employees. We are not aware of specific government requirements to follow up referrals in a timely manner, but EAP staff who operate within the principles of social work and clinical practice would be expected to do so.

The Army announced in May 2003 a sweeping overhaul of its program to help soldiers returning from combat duty to readjust to civilian life (Schmitt, 2003). These changes came about partly in response to five killings in 2002 involving Amy couples at Fort Bragg, NC. Recommendations in the Wood and Fischer (2002) report are currently under DoD review for potential implementation.

Utility Considerations

Several studies have documented the high costs of various employee suitability problems (Heuer, 1991a, 1991b, 1992, 1993, 1994, 1998). Other research has documented the potential benefits of programs that assist individuals with suitability problems (Barnes et al., 1988; Cascio, 2000), although none of the studies located dealt with cleared populations. Respondents in the Wood and Fischer study of 2002 indicated that, for the most part, it is far more cost-efficient to put employees with curable problems into EAPs than to fire them and begin training new personnel.

Objective 5. Revoke the Clearances of Cleared Individuals Shown to be Unacceptable

Despite the efforts of personnel security programs to promote early detection and amelioration of problems that could compromise an employee's trustworthiness, loyalty, or reliability, some proportion of cleared employees have historically been assessed as unacceptable for continued access to classified information. For example, about 3.9% of all DoD adjudicative decisions were unfavorable in calendar year 2002. This percentage include revocations, denials, and an unspecified number of applicants who were eliminated by a pre-screening process or by their own decision not to apply for fear of being turned down. Failures of early detection may result from: (1) a long time lag between the occurrence of a security-related incident and a personnel security investigation, (2) reticent coworker reporting due to concerns for the coworker (e.g., loss of clearance or job), concerns for themselves (e.g., confidentiality, legal, social ostracism), concerns about the quality of available assistance, or because they never detected the security-issue conduct, (3) under use of EAPs because cleared individuals with problems fear the loss of their clearance, loss of their position, loss of their privacy, or lack confidence in the quality of the assistance that would be provided, and (4) the fact that some who do seek help for problems may not be treatable from a security perspective due to the severity of their problem(s).

Given the enormous damage that cleared individuals can cause to national security, it is critical to suspend or revoke clearances when necessary. The costs of espionage are in the billions of dollars. This suggests that, left unchecked, the consequences of adverse security behavior are enormous and that timely, fair, and reliable procedures must be in place to remove those who have committed severe security breaches or are likely to do so.

How do we know if personnel security programs are effective in meeting this objective? As discussed under Objective 1, the revocation rate indicates little about effectiveness because the rate reflects the contrived strictness level of the Adjudicative Guidelines. A second problem is the unknown number of unacceptable clearance holders that successfully avoid detection. In recent Congressional testimony (United States Senate, 2003), the Deputy Secretary of Energy referred to such misses as "false negatives" in the detection process.

> What we must keep in mind is that every "clearance" procedure has the problem of "false negatives." It is just as dangerous to simply assume that a successfully completed background check means that we "know" the person is loyal to the United States. All that we "know" is that we have not found any evidence of disloyalty. The same should hold for thinking about what it means to "pass" a polygraph exam. We actually don't "know" that the person is not being deceptive. We simply have not found anything indicating that he or she is. The real life public policy challenge is that we have to make a judgment about how far we go, how many resources we expend, in the search for perfection when it comes to counterintelligence. Quite obviously, considering the many tens of thousands of Americans who have access to information or programs the protection of which is absolutely critical, we are forced to make a probabilistic judgment on how far is enough. The right way to think about this is "defense in depth." One tool alone will not suffice.

Efficiency

Ultimately, because we do not know the absolute number of unacceptable clearance holders who should be detected and revoked, efficiency and effectiveness must be viewed in relative terms. Thus, personnel security programs must strive to: (1) increase the speed and detection power of investigative tools and continuing evaluation, (2) improve the fairness of investigative, adjudicative, and due-process procedures (details on this topic appear below under “Fairness”), while (3) capitalizing on opportunities to reduce costs, e.g., through efficient application of automation. As discussed above, the ACES program shows promise as cost-effective, automated, screening and detection tool.

Timeliness

With respect to revocation, timeliness has two components. The first timeliness issue concerns the amount of time that can elapse once sufficient derogatory information has surfaced on a cleared individual to warrant a “Letter of Intent” (LOI). An LOI is a formal notice to the individual regarding the reasons for a pending negative adjudicative action. A recent study of clearance revocation cases in DoD (Fischer and Morgan, 2002) indicates that the average time elapsed from a serious event or initial report of security concern to the issuance of an LOI to revoke a clearance is 7 months for enlisted military personnel and civilian employees, 9 months for officers, and 2 months for contractor employees (during a 3-month period in 2002, slightly more than 1,000 LOIs were awaiting a response or pending final adjudicative action). According to DoD policy (5200.2-R, 1987), access to classified information should be suspended upon receipt of the LOI. However, because it is not always clear from adjudicative records or the DCII whether (or how soon), after an initial report of serious security concern, access is suspended, there is an unevaluated degree of security risk associated with the period of continued access allowed to such individuals.

Second, timeliness is relative in the sense that shorter (rather than longer) intervals of time for derogatory information to remain undetected is better. The cost-effectiveness of ACES checks should afford personnel security programs the benefit of performing powerful records checks annually or as often as deemed necessary.

Fairness

Fairness as a criterion by which to evaluate the effectiveness and utility of the five objectives of federal personnel security programs means evaluating whether procedures and policies are impartial, just and honest, unprejudiced, and carried out according to the rules as they exist (Webster's New World Dictionary, 509). Considerations about the fairness of procedures for vetting to determine initial access eligibility, deterrence of unsuitable behaviors by persons with access, continuing evaluation of eligibility, assistance to cleared persons with personal problems, and the denial or revocation of eligibility cluster around two legal and Constitutional issues: the right to due process and the right to privacy.

The Right to Due Process

Denials and Revocations. The right to "due process of law" is an ancient tenet of English common law. The phrase comes from the *Magna Carta* signed by the British King John in 1225 that was written into the United States Constitution in numerous places. It assumes that the interests of the government and those of the citizens might well conflict, and because the government is the more powerful, citizens need the protection of agreed-upon legal procedures. There are two types of due process, and both are relevant to eligibility determinations. *Procedural* due process protects the rights of individuals when they have been accused of wrongdoing, whether in criminal or administrative proceedings. The fourth, fifth, sixth, and eighth amendments to the Constitution outline specific procedural due process protections that include the right to trial by jury, the right to refuse to incriminate oneself, and in general a guarantee that "No person shall be…deprived of life, liberty, or property without due process of law" (Moore, Plesser, and Jaksetic, 1988). *Substantive* due process protects individuals, even if they have been accorded proper procedures, from being judged by capricious, arbitrary, or discriminatory standards. These rights are described in the first, fifth, and fourteenth amendments.

Personnel security programs for government employees began in 1953 with Executive Order 10450, and it only took a few years for a legal challenge claiming denial of due process rights to make its way to the Supreme Court. The Court decided the case of *Greene v. McElroy* in 1959, and their decision became one of the legal foundations for the administration of eligibility determinations. The decision in favor of Mr. Greene, the employee of a defense contractor, found that administrative procedures such as clearance denials must include the opportunity for the accused to review the evidence against him or her and to confront the witnesses. Spurred by this decision, in 1960 President Eisenhower issued Executive Order 10865 to put this into effect. DoD Directive 5220.6 implemented the procedures in the executive order to define the due process rights of defense contractors, and the DoD procedures were widely adopted by at least 20 other federal agencies. These two executive orders, 10450 and . 10865, set out two different sets of procedural rights of due process, one for government employees and the other for defense contractors. Contractors were assured a full, trial-like hearing when faced with the denial or revocation of a security clearance; government employees were not. Several decades of court rulings, procedural reforms, and legal studies eventually produced a narrowing of these differences in Executive Order 12968 in August 1995, but it did not eliminate the differences (Cohen, 2000).

A second important Supreme Court case dating from 1988 set parameters for the procedural due process rights of government employees. This decision came in the case of *Department of the Navy v. Egan*. The Court established that "no one has a right to a security clearance" and that the granting of a clearance is an act of discretion by the government that must decide what is in the interest of national security (Cohen 2000). Thus, the Court found that persons who hold security clearances do not have an inherent right to them and so have neither liberty nor property rights in the clearance; the Executive Branch has the discretionary right to grant or not grant access to classified information; an adverse decision should not be considered a judgment on the individual's background; and the Merit Systems Protection Board (the appeals body for civilian employees) does not have the expertise to hear appeals on security clearance decisions.

Due process rights for government employees facing a denial or revocation of a security clearance were implemented in DoD Regulation 5200.2-R in 1979, and revised in 1987. Minimum due process rights were defined by the *Egan* case as a detailed statement of reasons for an unfavorable action such a denial or revocation, the chance to reply in writing to the authority that issued the statement of reasons, a written response from the authority giving the final decision to revoke or deny and reasons for the action, and the right to appeal in writing to a higher authority within the DoD component (Cohen, 2000). Unlike defense contractors, military or civilian employees had "no right to a personal appearance, no right to see or challenge the evidence on which the decision was based, no right to know or cross-examine the accuser, and no right to present testimony, either personally or by witnesses, to counter the accusations or to support a continuation of a clearance (Cohen, 2000)." Since the Court found that a security clearance was not an enforceable right, it did not address the issue of due process since no such rights were due. Since *Egan*, a considerable body of case law had built up defining the legal aspects of loss of classified access (Gray, 2001).

A PERSEREC study on due process in 1993 surveyed the discrepancies between appeals procedures available to military, civilian, and contractor employees in DoD and recommended the creation of Personnel Security Appeals Boards (PSABs) in each DoD component (Riedel & Crawford, 1993). These boards were in fact created, along with several other improvements to due process, in Executive Order 12968, Access to Classified Information, in 1995. This executive order and its implementing directives are the basic statement of uniform investigative standards and adjudicative guidelines across the Executive Branch for all manner of employees. It outlines specific procedures for the review of unfavorable access determinations, adding to the minimum due process steps the right of an appellant to request all relevant documents, the right to be informed of their right to obtain counsel at their own expense, the right to be informed of their right to obtain and review their investigative file (within the limits of national security), the right to appear in person before an impartial adjudicative authority or before the appeals board itself. This personal appearance, however, is not the same as a trial-like hearing, since it lacks the right to hear or to cross-examine the government witnesses or to present witnesses oneself, or to know the identity of accusers. Other provisions such as record-keeping requirements are similarly narrowed (Cohen, 2000).

An official from the Office of the Secretary of Defense (OSD) explained in 1997 that the decision to craft a less-than-complete due process procedure for government employees was based on "time and cost (Lardner, 1997). The Joint Security Commission study (1994) had recommended against extending contractor appeal procedures to the government employees, fearing an avalanche of hearings would descend based on undisputed facts. The compromise sought to make the due process rights available to government employees better without "bogging down the system (Joint Security Commission, 1994)." Others, including the American Bar Association, advocated for full hearing rights given the importance of eligibility determinations to an individual's livelihood—losing a clearance often means losing a job (Aftergood, 1995).

Thus, the due process rights of government employees faced with unfavorable access determinations at present remain less than for employees of defense contractors, and this could be argued to be unfair.[11] There are somewhat different procedures for military employees and civilian employees, and higher levels of appeal involve DOHA which provides administrative judges to preside over hearings, sit for personal appearances, and make written decisions (Department of Defense, Defense Legal Service Agency, 2002). Those persons needing access to SCI are governed by a different authority, the DCI and the directives that are issued by the DCI. Different and less compete appeals procedures, compared to those found in Executive Order 12968, are outlined for persons with SCI access in Annex D of the basic directive, DCID 6/4, dating from 1998 (Cohen, 2000).

Vetting. The major study published by the Commission on Protecting and Reducing Government Secrecy (1997) recommended five guiding principles for an updated personnel security system that would build on the accomplishments in Executive Order 12968 a few years earlier. Three of the five guiding principles related to fairness: (1) openness and clarity of standards and the provision of clear information to all on the vetting process, (2) non-discrimination principles that would preclude "arbitrary and capricious standards," and (3) assurances of due process to include written statements and an appeal to a higher authority not involved in the original decision (Department of Defense Inspector General, 1997). The Commission suggested that sustained work was needed to achieve common standards and procedures across the government that would minimize distinctions and maximize fairness.

[11] Although this report does not focus on Special Access Programs (SAPs), it is interesting to note that persons working in SAPs currently have no due process rights. This is based on an interpretation of the 1959 case *Greene V. McElroy,* which held that the President would have the authority, in effect, to deprive a person of his or her employment if it were done explicitly. The resulting policies in Executive Order 10865 and DoD Directive 5220.6 explicitly excluded contractor employees working in SAPs from due process rights. Executive Order 12968 in 1995 extended this exclusion from appeals of SAP access decisions to all government employees.

In 1995, Executive Order 12968 included an explicit statement forbidding discrimination in eligibility determinations based on race, sex, color, religion, national origin, disability, or sexual orientation in granting access to classified information. While there have been numerous studies on aspects of implementation of the executive order, such as the application of uniform investigative standards and Adjudicative Guidelines, there have been few studies on the degree of discrimination on these various grounds that could be practiced in vetting, continuous evaluation, or denial or revocation of access.

The Right to Privacy

Deterrence and Continuous Evaluation. A second fairness-related issue in how we would evaluate the five objectives of personnel security programs concerns the right to privacy. Personnel security programs operated for roughly 25 years without many explicit privacy policies until, in 1974, Congress began to pass laws defining and protecting a person's right to privacy as it relates to personal information. While there are no blanket prohibitions on the federal government's access to public information, such as mortgage and real property records, personal information has increasingly come under protection in the last several decades as the Constitutional right to privacy has been expanded by the Supreme Court and federal and state law. Both the government's efforts to deter unacceptable behavior and its continuous evaluation for on-going or renewed security clearances require the collection and use of personal information about an individual with access eligibility. Therefore, both these objectives potentially come into conflict with the evolving right to privacy. Because the legal right to privacy in various contexts is now expressed in many different laws, to deny a person his or her privacy rights may be considered unfair.

The basic federal legislation in this area, the Privacy Act of 1974 (5 U.S.C 552a), is meant to protect individuals from unwarranted invasions of their privacy from the federal government collecting, maintaining, using, and disclosing to others personal information about them. Related important laws include the Freedom of Information Act (5 U.S.C. 552, amended in 1974) that grants persons the right, enforceable in court, to obtain access to federal agency records that are not otherwise exempted from disclosure. The Fair Credit Reporting Act (15 U.S.C. 1681, amended in 1996) protects individuals' rights in information provided to employers by consumer reporting agencies (Bosshardt, 2000). Other sectors of information that each have its own law protecting the privacy of personal information include education, banking, cable, video, motor vehicle, health, children, and financial (Stevens, 2003). There is no one overarching statute that defines or protects privacy *per se*.

Vetting for initial eligibility access to classified information obviously requires the collection and use of personal information about the applicant in the background investigation, but an applicant voluntarily agrees to waive claims to privacy when he or she fills out and signs the Questionnaire for National Security Positions, the SF-86. Upon being granted access to classified information, an individual assumes responsibility for self-reporting to a security officer specified information about his or her travel, finances, health, associates, and other security-relevant issues and behaviors. Large areas of privacy are voluntarily waived by the person who seeks and assumes eligibility access.

The evolving ability to use information technology to do data-mining does raise questions about its impact on the remaining privacy of cleared personnel. The fourth amendment to the Constitution, in which unreasonable searches and seizures are forbidden, as are "general warrants" that target unnamed groups rather than specific persons, is the main Constitutional foundation for privacy laws. When computer systems in this era of automated databases can search multiple databases and collect information on a person from many disparate sources, construct profiles, search for defined qualities, or track the habits and activities of individuals, where do these abilities cross the definition of unreasonable searches (Clark, 2003)? The issue of monitoring of private life by government is controversial, and it has become more so after the terrorist attacks of September 11, 2001, and legislation passed in response to it such as the USA Patriot Act of 2001. Policies supporting increased monitoring and data-mining of information have expanded more rapidly than studies can be conducted to document the results of such activities.

Assistance to Cleared Personnel with Problems. One response to a person who has a security clearance and a personal problem is to refer him or her to an EAP provided by the agency. As described under Objective 4, PERSEREC has studied the nature of such programs and their availability across the various agencies in DoD (Wood and Fischer, 2002). The provisions for privacy and confidentiality for the person who seeks help with a personal problem vary among programs. The basic contradiction for persons with access eligibility that underlies many of the EAPs, however, is that, in the name of protecting national security, security officials insist on access from the EAP to information about personal problems that could be security-relevant, while counselors in the EAP insist that confidentiality is essential to allow people to actually come forward and confide their problems. Focus group research results suggest that, too often, employees sense that information shared with the EAP gets back to the security office and other authorities. This could threaten a job, which undermines an employee's decision to use an EAP. Research results further suggest a sincere recognition by security personnel that helping a cleared person with a problem before it escalates is the cost-effective and humane choice. Yet until the contradiction in how EAPs are used is resolved, this help may be illusory. Relying on EAPs that cannot provide help would seem to be an issue of fairness in the personnel security system.

Summary of Effectiveness Evaluations

Evaluating the effectiveness and utility of federal personnel security programs first requires agreement on what constitutes the goal, program objectives, and program performance criteria. Although a common goal statement regarding the trustworthiness, loyalty and reliability of an acceptable cleared workforce can be culled from the principal Executive Orders that govern federal personnel security programs, there is no authoritative policy enunciating program objectives and performance criteria. Based on an interpretation of relevant policy documents and principles of program evaluation, we proposed the following five program objectives:

- Deny unacceptable applicants initial eligibility for access to classified information
- Deter cleared individuals from engaging in unacceptable behavior
- Detect, and appropriately follow-up on, evidence indicating that cleared individuals may have become unacceptable to hold a security clearance
- Assist cleared individuals who have, or appear to be developing, problems that could interfere with reliable job functioning
- Revoke the clearances of cleared individuals shown to be unacceptable,

and <u>three program performance criteria:</u>

- Timeliness
- Efficiency
- Fairness

These program objectives and performance criteria were used to discuss and evaluate personnel security program effectiveness. The broader concept of utility was defined as an assessment of the total direct and indirect costs and benefits of a program, i.e., the total fiscal and subjective value of a program for which indirect, and even unintended, consequences are considered.

As described earlier, security clearance procedures have been developed and improved through many years of investigative and security-related experience—taking into account practical and logical risk factors for security, as well as relevant social science research results. Measurement and data collection challenges (e.g., difficulties collecting useful objective data on loyalty), as well as the problem of population unknowns (e.g., not knowing the total number of cleared individuals with espionage intent), make it difficult, if not impossible, to evaluate many aspects of personnel security effectiveness in terms of absolutes. With respect to utility, these issues create difficulties in calculating certain kinds of utility outcomes, such as a national security benefit-per-dollar ratio.

One area in which these challenges do not pervade, i.e., where an objective measure of personnel security program effectiveness can be obtained, is in meeting program timeliness standards that entail stated deadlines. OPM states that "standard" priority investigations should be completed within 75 or 180 days, depending on the type of investigation. As of September 2004, approximately 28.3% (91,154/321,951) of OPM pending investigations were more than 180 days old. Among the overdue investigations, 40,081 (44%) were more than 360 days old. Timeliness problems have been persistent, e.g., as of May, 2004, 29.6% (82,890/279,635) of pending investigations were more than 180 days old, including 50,517 (60.9% of the overdue cases) that were more than 360 days old.

For the remaining aspects of assessing personnel security programs we can assert the following: *Improvements in effectiveness and utility* have been demonstrated and can be pursued further. With respect to the five program objectives, an example of an improvement in effectiveness is assisting more cleared individuals who need help (Objective 4), even without knowing the total number who might need help. With respect to program performance criteria, personnel security programs are positioned to show improvements in efficiency (e.g., e-clearance), timeliness (e.g., ACES), and fairness (e.g., improved due process procedures).

Consequently, it is clear that improvements to personnel security effectiveness can and should be pursued, e.g., through the appropriate use of technology and automation, by developing policies that provide government-wide standards as well as flexibility to meet agency-specific needs, and by implementing faster and more cost-effective investigation and clearance procedures that do not compromise security concerns. This last example is the focus of the following report section on the costs and benefits of different investigative approaches.

Costs and Benefits of a Full-Field Versus a Secret-level Investigation

As previously stated, a utility perspective requires one to consider the costs and benefits of personnel security program procedures such as background investigations undertaken to determine eligibility for access to classified information.[12] Numerous sources such as the subject interview, the personnel security questionnaire, reference interviews and records checks are used in investigations, each having its own degree of investigative value. Sources are used to uncover issue-relevant information[13] as well as information that mitigates the significance of derogatory information. Because there are no reliable datasets available that directly link national security outcomes to personnel security program procedures or policies, assessing the relative productivity of sources used in investigations is an empirical and justifiable method for evaluating the effectiveness of background security investigations.

Each investigative source accounts for a percentage of the total cost of an investigation as well as a percentage of the total amount of issue-relevant information yielded in the investigation. In our analyses we present cost and productivity data pertaining to: (a) the initial Secret-level investigation (known as a NACLC), (2) the initial "full-field investigation" for a Top Secret or "Q" clearance (known as the Single Scope Background Investigation or SSBI), (3) the periodic reinvestigation for a Secret-level clearance (NACLC-PR), and (4) the periodic reinvestigation for a Top Secret level clearance (Single Scope Background Investigation-Periodic Reinvestigation or SSBI-PR). SSBI-PRs are supposed to be conducted 5 years after a Subject's initial investigation closes. NACLC-PRs should be conducted 10 years after an initial Secret level clearance.

It is essential to discuss initial background investigations separately from periodic reinvestigations because Subjects undergoing these two types of investigations differ in some important ways. For initial investigations the Subject typically has had no access to

[12] For the remainder of this discussion, the colloquial term "clearance" may be used in place of the formal phrase "eligibility for access classified information."

[13] "Issue-relevant Information" is information relevant to establishing that an issue is of potential current security concern. It is information that an adjudicator would want to review in making a clearance decision. The Adjudicative Guidelines provide a framework for distinguishing issue-relevant information.

classified information and therefore may pose less of a security threat than the Subject undergoing a reinvestigation who typically has had several or many years of eligibility for access to classified information. In addition, initial investigations and reinvestigations entail different cost structures.

The degree of utility of an investigative source is based on the amount of issue-relevant information yielded by the source. For the discussion and tables that follow, it is important to understand how source productivity was measured. Rather than representing the yield of each individual source in a case, source-yield was conceptualized at the case-level. A source is said to yield an item of information if one or more elements of the source yielded issue-relevant information in the case. For example, Local Agency Checks (LACs) in a case either yielded an item of issue-relevant information or yielded no issue-relevant information – each local agency record check was not considered separately.[14]

To understand which SSBI sources add much or little incremental productive value beyond those used in a NACLC, it is useful to compare the proportion of cost contributed by these sources with the proportion of issue-relevant information they yield. This comparison is one of the requirements (b)(1) of Congressional Bill HR 2417. The NACLC includes the following sources:

- Personnel Security Questionnaire (PSQ)
- National and Local Agency Checks
- Credit Reports checks.

The SSBI includes the NACLC investigative sources as well as the following sources:

- Subject Interview
- Ex-Spouse Interview (if applicable)
- Employment Interviews (coworkers and supervisor)
- Listed Reference Interviews (those who the Subject listed on the PSQ)
- Developed Reference Interviews (developed during the course of the investigation)
- Other records checks (medical, military, education).

Table 1 shows the cost differences that exist between the NACLC and the SSBI for both initial and periodic reinvestigations.[15] In the following tables OPM cost data are used because OPM currently conducts the majority of PSIs for the federal government, including DoD[16].

[14] For more information concerning this conceptualization of source productivity, see *SSBI-PR Source Yield: An Examination of Sources Contacted During the SSBI-PR* (Kramer, Crawford, Heuer & Hagen, 2001).

[15] OPM also provides "accelerated" and "priority" PSI processing for higher rates. Some federal agencies have negotiated slightly different PSI rates with OPM.

[16] Because OPM cost proportions for the Subject Interview were not available, cost proportions for the Subject Interview that appear in Tables 2-4 are based on DSS cost estimates.

Table 1
Cost Standards

Type of Investigation	Level of Access	OPM Costs
NACLC	Secret	$168
SSBI	Top Secret	$2,830
NACLC-PR	Secret	$148
SSBI-PR	Top Secret	$1,840

OPM charges $168 for each NACLC and $2,830 for an initial SSBI. There is a similar cost differential between the periodic reinvestigation for Secret-level and the Top Secret level investigations – $148 and $1,840, respectively.

Cost-Benefit – DOD SSBIs

In evaluating the incremental utility of sources used in SSBIs (and SSBI-PRs) but not currently used in NACLC investigations (and NACLC-PRs), we distinguish gains associated with the inclusion of the Subject Interview in the NACLC from gains that could result from the inclusion of all remaining investigative sources. Because research shows that the Subject Interview is a very productive investigative source (Kramer & Richmond, in press; Carney, 1996; Kramer et al., 2001), we present the incremental value of the Subject Interview separately. Using source productivity data from earlier research in which 1,124 SSBIs were reviewed and coded by experts, and cost data obtained primarily from OPM, Table 2 shows the costs and benefits (portion of issue-relevant information yielded) for sources that currently comprise the NACLC, the Subject Interview, and all other sources used in the SSBI.

As shown in Table 2:

- Fifty-one percent of issue-relevant information yielded in the average Single Scope Background Investigation is yielded by the PSQ, NAC, LAC, and credit report. In other words, approximately half of the issue-relevant information is surfaced through NACLC sources at approximately 6% of the total SSBI cost.
- The Subject Interview alone accounts for 20% of issue-relevant information yielded in the average SSBI and constitutes approximately 17% of the total SSBI cost.
- Sources used in the NACLC and the Subject Interview, when combined, account for approximately 71% of issue-relevant information and constitute approximately 23% of the total cost of the SSBI.
- The remaining 28% of issue-relevant information is obtained through all other sources that comprise the SSBI. These sources account for approximately 77% of the cost of the SSBI.

Table 2
Cost-Benefit Analysis of Issue-relevant Information
DOD SSBIs[a]
(N=1,124 SSBIs)

Source Categories	Cost: Portion of Total Cost of SSBI	Benefit: Portion of Issue-Relevant Information Yielded
PSQ, NAC, LAC & Credit Report	6%	51% (828 items)
Subject Interview	17%	20% (327 items)
All Other Sources (including NAC-Spouse)	77%	28% (459 items)
Total	100%	100% 1,614 items

[a]Percentages may not total 100% due to rounding

Cost-Benefit – DOD, OPM, CIA, and NRO SSBI-PRs

Whereas for initial background investigations, productivity data exist for DoD only, for PRs, productivity data exist for DoD, OPM, CIA, and NRO (Kramer et al., 2001). Although available cost data apply to DoD and OPM only, there is no evidence to suggest that cost proportions would be greatly different for CIA and NRO.

Table 3 illustrates differences in productivity of sources used in DoD, OPM, CIA, and NRO SSBI-PRs. Subject interviews constitute a substantial greater proportion of the total cost of the periodic reinvestigation than the SSBI – 30% versus 17%. Overall, results obtained from our analysis of cost and productivity data for SSBI-PRs shows a similar utility pattern to results regarding initial investigations:

- Twenty-six to 52% of issue-relevant information is surfaced through sources used in the NACLC-PR at approximately 8% of the total SSBI-PR cost.
- The Subject Interview alone accounts for 24% to 43% of issue-relevant information at approximately 30% of the total SSBI-PR cost.
- Sources used in the NACLC-PR and the Subject Interview, when combined, account for 64% to 77% of issue-relevant information for approximately 38% of the total cost of an SSBI-PR.

Table 3
Cost-Benefit Analysis of Issue-relevant Information
DOD, OPM, CIA and NRO SSBI-PRs[a]

Source Categories	Cost: Portion of Total Cost of SSBI	Benefit: Portion of Issue-Relevant Information Yielded			
		DoD (N=1,611 SSBI-PRS)	OPM (N=1,332 SSBI-PRs)	CIA (N=855 SSBI-PRs)	NRO (N=923 SSBI-PRs
PSQ, NAC, LAC & Credit Report	8%	49% (407 items)	52% (507 items)	26% (131 items)	34% (181 items)
Subject Interview	30%	28% (238 items)	24% (235 items)	38% (188 items)	43% (224 items)
All Other Sources (including NAC-Spouse)	62%	23% (193 items)	24% (236 items)	36% (178 items)	23% (120 items)
Total	100%	100% 838 items	100% 978 items	100% 497 items	100% (525 items)

[a]Percentages may not total 100% due to rounding

- The remaining 23%-36% of issue-relevant information is obtained through all other sources that comprise the SSBI-PR and accounts for approximately 62% of the cost of the SSBI-PR.

Mitigating Information in Periodic Reinvestigations

The Adjudicative Guidelines also specify types of mitigating information that should be considered in evaluating investigative results. Research data pertaining to source productivity in terms of yielding mitigating information is available for SSBI-PRs, but not for initial investigations. Table 4 illustrates how the respective investigative source categories perform in providing information that mitigates the significance of issue-relevant information obtained in SSBI-PRs across four agencies.

Data presented in Table 4 reveal a similar pattern of relatively high utility for sources used in the NACLC-PR, substantial utility for the Subject interview, and relatively low utility for the remaining investigative sources in terms of yielding mitigating information:

Table 4
Cost-Benefit Analysis of Mitigating Information
DoD, OPM, CIA, and NRO SSBI-PRs [a]

Source Categories	Cost: Portion of Total Cost of the SSBI-PR	Benefit: Portion of Mitigating Information Yielded			
		DoD (N=1,611 SSBI-PRs)	OPM (N=1,332 SSBI-PRs)	CIA (N=855 SSBI-PRs)	NRO (N=923 SSBI-PRs)
PSQ, NAC, LAC & Credit Report	8%	32% (255 items)	57% (831 items)	25% (99 items)	35% (199 items)
Subject Interview	30%	48% (384 items)	29% (418 items)	48% (189 items)	49% (279 items)
All Other Sources (including NAC-Spouse)	62%	19% (153 items)	15% (215 items)	27% (109 items)	16% (91 items)
Total	100%	100% (792 items)	100% (1,464 items)	100% (397 items)	100% (569 items)

[a] Percentages may not total 100% due to rounding.

- Twenty-five to 57% of mitigating information is surfaced through sources used in the NACLC-PR at approximately 8% of the total SSBI-PR cost.
- The Subject Interview alone accounts for 29% to 49% of mitigating information at approximately 30% of the total SSBI-PR cost.
- Sources used in the NACLC-PR and the Subject Interview together account for 73% to 86% of mitigating information and approximately 38% of the total cost of an SSBI-PR.
- The remaining 23% to 36% of mitigating information is obtained through all other sources that comprise the SSBI-PR, and accounts for approximately 62% of the cost of the SSBI-PR.

Productivity of Sources Summary

Overall, results displayed in Tables 2, 3, and 4 indicate that the investigative sources that have the greatest utility in terms of cost-effectiveness for surfacing issue-relevant and mitigating information are the Subject Interview and sources currently required for the Secret-level clearance.

While these cost-benefit analyses show the amount of information yielded in the NACLC and the SSBI, it bears mentioning that PERSEREC has undertaken analyses for the specific purpose of identifying investigative procedures that can be used to maximize the utility of sources in SSBI-PRs. Similar to the focus implied by the H.R. 2417 report requirement (2)(B), PERSEREC's goal was to identify an investigative approach that would increase the cost-effectiveness of investigative procedures, without decreasing the investigative power to uncover cases requiring an adverse adjudicative action ("actionable cases"). PERSEREC's research in this area resulted in the development of a two-phase reinvestigative approach in which the least productive sources are used only in SSBI-PRs where the most productive sources indicate (through the development of issue-relevant information) that further expansion of the investigation is warranted.

Maximizing Utility through a Phased Reinvestigation Approach

To briefly summarize, research on the phased reinvestigation (Heuer et al, 2001; Heuer, et al., 2003; Kramer et al., in review) entailed developing and testing various SSBI-PR models. In the two-phase SSBI-PR model that emerged as most effective, sources were divided into two categories: Phase 1 sources (to be used in all SSBI-PRs) and Phase 2 sources (used only if Phase 1 sources surface issue-relevant information). If in Phase 1 no issue-relevant information is developed, the case is adjudicated without additional investigation. If issue-relevant information surfaces during Phase 1, the case receives further investigation, i.e., Phase 2 sources are added (equivalent to conducting a full SSBI-PR). Phase 1 sources include all sources used in the SSBI-PR aside from listed and developed references, neighborhood interviews, and neighborhood records (Phase 2 sources).

In the phasing studies, Phase 1 sources did not yield issue-relevant information in approximately 70% of SSBI-PRs, and thus Phase 2 sources were not used in these periodic reinvestigations. Findings of this initial research, as well as follow-up studies conducted with SSBIs (Kramer et al., in press), show that phasing misses very little issue information and that all actionable cases are identified as warranting a full investigation. Phase 2 sources account for approximately 42% of the total cost of an SSBI-PR, and approximately 47% of an SSBI[17].

Figure 1 provides a conceptual illustration of the phased reinvestigation approach.

Conclusion

Results presented here indicate that the investigative sources required for the Secret-level clearance, combined with the Subject Interview, are most cost-effective for surfacing issue-relevant and mitigating information. Related research was presented regarding the merits of the two-phased reinvestigation in which the least productive sources are not used in all SSBI-PRs. Results of phasing research show that phasing results in a more cost-effective use of investigative resources, minimal loss of derogatory information, and no loss in the detection of actionable cases.

[17] Based on cost data from Mitchell (1999).

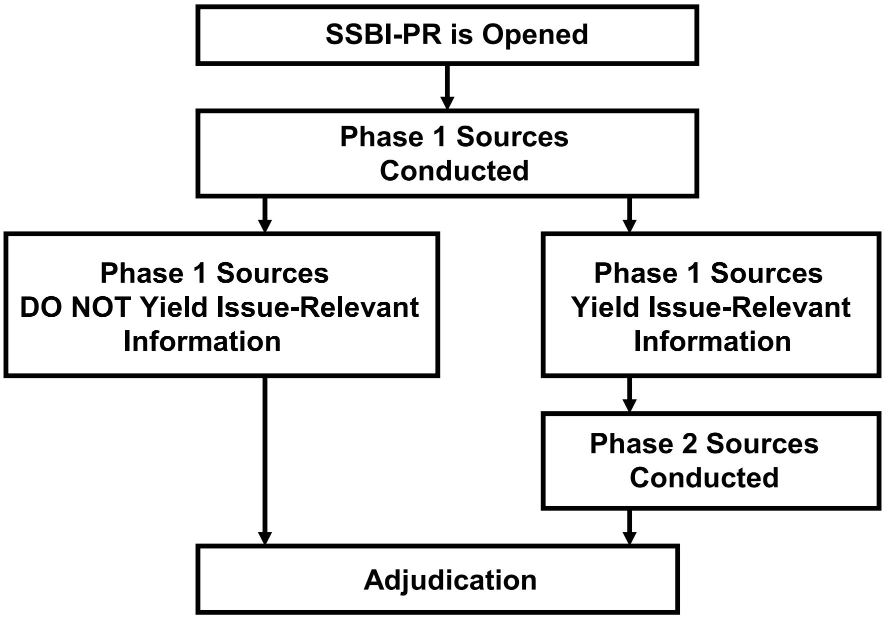
SSBI-PR is Opened
Phase 1 Sources Conducted
Phase 1 Sources DO NOT Yield Issue-Relevant Information
Phase 1 Sources Yield Issue-Relevant Information
Phase 2 Sources Conducted
Adjudication

Figure 1 Steps in Conducting a Phased Reinvestigation.

Standards Governing the Denial and Revocation of Security Clearances[18]

Executive Order 12968, Access to Classified Information, dated August 1995, sets the eligibility standard for access to classified information. It states: "Eligibility for access to classified information shall be granted only to employees who are United States citizens for whom an appropriate investigation has been completed and whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."

This eligibility standard is met through the application of Adjudicative Guidelines for Determining Eligibility for Access to Classified Information, approved by President Clinton in March 1997. These guidelines were officially implemented in the security community in 1998 and marked the beginning of a common standard within the U.S.

[18] This section addresses report requirements (b)(2) of Congressional Bill HR 2417.

government as a whole for the adjudication of security clearances. Previously, each agency had its own standards.

Presidential approval of the current Adjudicative Guidelines was transmitted in a letter from the Assistant to the President for National Security Affairs (NSC). This letter required that a report of the effectiveness and efficiency of the new guidelines, with recommendations for any adjustments that may be needed, be transmitted to the President within one year after implementation.

In response to the NSC requirement, Director of Security, Assistant Secretary of Defense for Command, Control, Communication, and Intelligence (ASD, C3I), directed PERSEREC to conduct a study of the efficiency and effectiveness of the revised guidelines as implemented in the Department of Defense (DoD). The findings of that study (Carney & Marshall-Mies, 2000) are discussed below.

Adjudicative Guidelines

The Adjudicative Guidelines approved in 1997 define 13 areas of an individual's background that may be of security concern. The guideline for each area states the reason the area is of concern to national security and provides potentially disqualifying and mitigating factors. The 13 areas are as follows:

- Allegiance to the United States
- Foreign Influence
- Foreign Preference
- Sexual Behavior
- Personal Conduct
- Financial Considerations
- Alcohol Consumption
- Drug Involvement
- Emotional, Mental, and Personality Disorders
- Criminal Conduct
- Security Violations
- Outside Activities
- Misuse of Information Technology Systems

Conduct in each of these areas is to be evaluated using what is called the whole-person concept, which includes consideration of the following factors:

- The nature, extent, and seriousness of the conduct.
- The circumstances surrounding the conduct to include knowledgeable participation.
- The frequency and recency of the conduct.
- The individual's age and maturity at the time of the conduct.
- The voluntariness of the conduct.

- The presence of absence of rehabilitation and pertinent behavioral changes.
- The motivation for the conduct.
- The potential for pressure, coercion, exploitation, or duress.
- The likelihood of continuation or recurrence.

The Adjudicative Guidelines are designed to help agencies meet their personnel security program goal—assuring a more reliable, trustworthy, and loyal workforce—by screening out individuals with detectable criminal tendencies, drug abuse, alcohol problems, serious financial or mental health problems, and individuals who are vulnerable to foreign influence or may have conflicting loyalties. They might be thought of as criteria for providing due diligence in protecting national security by screening out individuals whose known past or current behavior indicates a significant risk of unreliability, untrustworthiness, or disloyalty.

Assessment of Effectiveness and Efficiency of the Adjudicative Guidelines

The PERSEREC study described above assessed the effectiveness and efficiency of the Adjudicative Guidelines. As discussed earlier, effectiveness refers to the achievement of program objectives, such as "denying unacceptable applicants initial eligibility for access to classified information," and "revoking the clearances of cleared individuals shown to be unacceptable," according to accepted program performance criteria, such as efficiency. The PERSEREC study used three procedures: (1) a survey was administered to all DoD personnel responsible for determining eligibility for access to classified information; (2) a workshop was designed to provide a quantitative measure of how consistently the guidelines are applied to difficult cases by senior DoD adjudicators; and (3) focus group interviews were conducted with Personnel Security Appeals Board members and administrative judges.

The study found that the new Adjudicative Guidelines had been successfully implemented in DoD. On the measures of efficiency, the guidelines were rated as "clear" and "easy" to apply, i.e., implying that resources were not typically wasted on unnecessarily difficult applications of the guidelines. On the measures of effectiveness, operationalized in terms of their coverage of security concerns, the guidelines as a whole were rated "adequate," but there were significant differences among guideline areas. Those ranked highest in terms of their adequacy (effectiveness) were: Financial Considerations, Criminal Conduct, Alcohol Consumption, and Drug Involvement. Those rated lowest were: Foreign Preference, Emotional/Mental and Personality Disorders, Outside Activities, and Misuse of Information Technology Systems.

To measure consistency of adjudications, 15 senior adjudicators independently adjudicated 13 cases, one for each guideline. Very difficult cases were selected in order to *maximize* the chances of inconsistent decisions. Overall, there was 81% agreement among the senior adjudicators on recommended eligibility determinations. For nine of the 13 cases, there had already been an official decision, and for these cases there was 62% agreement between the senior adjudicators and the official decision. These findings suggest there may be a high level of consistency among senior adjudicators when applying the guidelines to identical cases; however, outcomes may differ when the circumstances of a case do not exactly fit the guideline.

General Versus Specific Standards

During the course of development and approval of the 1997 Adjudicative Guidelines, there was considerable debate regarding how general or specific the guidelines should be. It was decided that they should be rather general. As a result, the guidelines list behaviors that "may be" disqualifying or mitigating, but provide few specific thresholds for how recent, frequent, or serious the behavior must be before it is actually disqualifying. This gives adjudicators the flexibility to take fully into account the multitude of factors involved in making a whole-person judgment about a person's reliability, trustworthiness, and loyalty. The downside of this approach is that it does open the possibility for different adjudicators to arrive at different determinations after applying the same guidelines to a given set of investigative findings.

The alternative is to set specific thresholds for when alcohol abuse, past drug use, financial problems, etc., reach a level that warrants denial or revocation. The current guidelines contain terms such as "significant," "serious," "not recent," and "not frequent." Some adjudicators would prefer that these terms be defined in terms of months, years, or number of incidents so that decisions would be less dependent upon the judgment of individual adjudicators. Although this would facilitate consistency of adjudicative decisions, there is no empirical justification for many specific thresholds. For example, although a 2002 national survey found that 29.8% of college-age Americans[19] used marijuana at least once within the past year, there are no consistent research results indicating that experimental use of marijuana in college predicts post-college drug use for individuals who enter the workforce in positions that require abstinence from drug use. In this example, implementing a strict one-year threshold would "cost" the nation in terms of reducing the proportion of individuals who can obtain or retain a security clearance, without any evidence of a comparable benefit to national security.

An advantage of the general guidelines is that the same guidelines can be used to screen both applicants for an initial clearance and existing employees. In the area of drug use, for example, existing employees have accepted an explicit obligation to remain drug-free. That goes with the job, and any deviation from this obligation is grounds for revocation. A very different standard is applied to an applicant recently graduated from high school or college where experimental use of marijuana was rather common. The alcohol guideline is also flexible enough that different standards can be applied to initial applicants and to continuing evaluation of already cleared personnel. An initial applicant with a serious alcohol problem will normally be denied a clearance. A cleared employee who develops an alcohol problem after a period of satisfactory performance will usually be sent for counseling or treatment, with revocation a last resort if counseling and treatment fail.

[19] The study statistic comes from an annual survey by the Department of Health and Human Services and refers to all civilian, non-institutionalized Americans age 18 to 25.

While it is desirable and even necessary that adjudicative standards be flexible, the absence of specific thresholds in key areas of concern does make it more difficult to achieve consistent adjudicative decisions, which was a principal rationale for developing the current, common set of adjudicative guidelines for all agencies. Common standards are a prerequisite for consistent adjudicative decisions but do not, themselves, assure that outcome. Additional research and applications regarding quality assurance is needed to develop common practices for the implementation of these standards.

Consistency is a particular concern of DoD in that responsibility for adjudication is assigned to eight separate DoD organizations. The DoD Inspector General in 1998 recommended a peer review program to ensure that DoD adjudication facilities consistently meet performance standards (Department of Defense Inspector General, 1998). The GAO in 2001 recommended standardization of procedures for documenting the rationale for adjudicative decisions, common adjudicator training requirements and increased training opportunities, greater use of the explanatory guidance in the Adjudicative Desk Reference (ADR)[20] and implementation of a joint quality assurance program (General Accounting Office, 2001).

Several programs are underway or in process to facilitate and promote consistency of adjudicative decisions. A DoD proposal to update and clarify the Adjudicative Guidelines has been submitted for review and coordination by the overall security community, as discussed below. The changes should facilitate application of the guidelines. When new guidelines are approved, DoD will update the ADR. The ADR has extensive background information on each of the 13 areas of adjudicative concern. It was developed as an operational aid to help adjudicators implement the 1997 Adjudicative Guidelines and has been used as a common basis for adjudicator training across many federal personnel security programs.

PERSEREC has an active research program to develop quality review procedures for DoD adjudications. The first step is to develop consistent procedures for how DoD adjudicative facilities enter their rationale for adjudicative decisions in DoD's new JPAS. The second step will be a quality review program involving review of randomly selected cases to evaluate adjudicative decisions and the rationale for those decisions.

Proposed Changes to the Adjudicative Guidelines

The previously noted PERSEREC study assessing the effectiveness and efficiency of the Adjudicative Guidelines provided feedback on each guideline, including terms that need clarification and recommendations for improving the statement of concern, disqualifying conditions, and mitigating conditions. As a result, the Deputy Director for Personnel Security, OASD(C3I), tasked PERSEREC to draft and coordinate within DoD proposed changes to the Adjudicative Guidelines. The DoD proposal, *Proposed Update and Clarification of the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information and/or Assignment to Sensitive Positions* was submitted to the

[20] The ADR is described on the DSS website at http://www.dss.mil/nf/adr/index.htm (where it is also available for download).

Personnel Security Working Group of the Policy Coordinating Committee for Records Access and Information Security Policy (Heuer, Youpa, & Carney, 2003), which is reviewing it for applicability across the federal community.

DoD believes the basic principles that underlie the current Adjudicative Guidelines are still sound, but some conditions have changed and federal personnel security programs have had almost 6 years to observe the strengths and weaknesses of the particular wording in the guidelines. The proposed guideline changes are intended to clarify the adjudicative issues and their potentially disqualifying and mitigating conditions, alleviate ambiguities encountered when implementing the current guidelines, and incorporate new and emerging issues as well as new research findings on traditional issues. Principle recommendations include the following:

- The Foreign Influence guideline should be updated to reflect our increasingly global economy and increasingly multiethnic society. The focus should be on conflicting foreign interests and divided loyalties as well as on vulnerability to coercion and on foreign business and professional associates and friends as well as on family members.

- A Gambling Practices guideline is proposed to focus attention on problems associated with compulsive gambling, which has been described as the fastest-growing and most under-diagnosed addiction in America.

- The Security Violations guideline is proposed to be revised and renamed Mishandling Protected Information. The goal is twofold: (1) to focus more attention on serious security and counterintelligence concerns as compared with accidental administrative violations, and (2) to make it clear that past mishandling of sensitive but unclassified information is also a security concern.

- The Emotional, Mental, and Personality Disorders guideline is proposed to be renamed Psychological Conditions. The term “disorder” sets an unnecessarily high standard for action under this guideline. The proposed guideline enables adverse action to be taken either on the basis of a diagnosed disorder or on the basis of unusual or undesirable behavior that clearly raises questions about an individual’s reliability, trustworthiness, judgment, or emotional stability.

Frequency and Causes of Denials and Revocations

In calendar year 2002, DoD made 564,554 access eligibility decisions for military personnel, civilian employees of the department, and individuals in the private sector who are employed on DoD contracts. Clearances were denied or revoked in about 0.7% of these cases. This included 1,887 denials and 1,579 revocations for collateral clearances (Top Secret, Secret, and Confidential) and 329 denials and 210 revocations for SCI access. However, denials and revocations tell only part of the story. There were an additional 18,163 unfavorable adjudicative decisions in which denial or revocation was not formally completed due to what is called "loss of jurisdiction."[21] These were cases in which applicants withdrew their employment applications or existing employees resigned or retired while a denial or revocation was pending. They withdrew or departed rather than face the prospect of a negative clearance decision (J. R. Goral, e-mail communication, October 21, 2003).

In calendar year 2002, therefore, there were a total of 22,169 decisions (about 3.9%) that effectively denied or revoked clearances. This compares with 17,833 such decisions (about 4.5%) in 1998 (Carney and Marshall-Mies, 2000), over 20,000 (4.1%) in 1995 (Defense Personnel Security Research Center, 1995), and almost 17,000 (2.8%) in 1993 (Defense Personnel Security Research Center, 1993). The Department of Energy has reported slightly higher but comparable percentages for its Personnel Security Assurance Program (Department of Energy, Office of Security, 2003).

Denial or revocation of a DoD clearance is subject to an appeal process that differs for government personnel and employees of private companies working on classified DoD programs. During the period 1996-1999, the Personnel Security Appeals Boards handled about 290 cases per year of appeals by DoD applicants or employees. Of these, the appeals board upheld the denial or revocation in about 75% of the cases. During this same period, administrative judges heard about 295 appeals per year by employees of DoD contractors, upholding the denial or revocation in about 70% of these cases (Carney & Marshall-Mies, 2000).

DoD adjudicative facilities revoked 2,033 clearances during fiscal year 1998. PERSEREC studied these revocations to determine the reasons for the revocations and the sources of information that triggered the start of the revocation process. This study did not examine the much larger number of cases of individuals who resigned or retired after learning that their clearances might be revoked. In these 2,033 cases, the actual revocation of clearance can usually be traced back to a precipitating event such as an arrest, complaint, or a personnel security investigation. The personnel security investigation in this context includes both PRs and initial SSBI investigations to upgrade an existing Secret or Confidential clearance to Top Secret or SCI (Fischer & Morgan, 2002).

The most common precipitating event varied by employment category. For military personnel and DoD civilians, the most common precipitating events were prosecution or police reports of criminal conduct, positive tests for drug use, and a personnel security investigation (PR or SSBI). For contractors, the most common precipitating events were a Special Investigative Inquiry undertaken to resolve adverse information reported between investigations, a personnel security investigation (PR or SSBI), and a National Agency Check (not conducted as part of any other investigation).

[21] Owing to how data are coded in the Defense Clearance Investigations Index (DCII), it is not possible to say how many of these "loss of jurisdiction" cases are denials versus revocations. This is because many of the revocations result from initial SSBI investigations on individuals who already have a Secret clearance. In other words, the same investigation may lead to denial of the request for Top Secret clearance and revocation of the existing Secret clearance.

A personnel security investigation (PR or SSBI[22]) was the precipitating event leading to the revocation of clearance for 18% of enlisted military personnel who had their clearance revoked. For the remaining 82%, the revocation was precipitated by information from another source such as a drug test. For other groups, a personnel security investigation was the precipitating event leading to the revocation for 23% of the military officers, 31% of DoD civilians, and 28% of DoD contractors. The lower percentages for enlisted military personnel may be explained by the fact that their behavior is more readily observable in a close community of peers and is routinely subject to more intensive personal monitoring and command supervision. Therefore, problems are more likely to be identified, and action taken earlier, in a military than in a civilian environment.

Types of issue information that most often triggered revocation were drug use, financial issues, and criminal conduct. For military personnel and contractors, drug use was number one. For DoD civilians, financial issues were by far the most frequent trigger for revocation. A Statement of Reasons (SOR) is a part of each formal clearance revocation. Most SORs cited three or more reasons. Judging from the SORs, the most common cause for revocation was personal conduct. However, the Personal Conduct adjudicative guideline covers falsification of information or failure to cooperate during the investigation as well as generally unreliable behavior. In many cases, the personal conduct at issue was the withholding or falsification of information relating to the other primary issues—drugs, crime, and finances.

Foreign Influence and Foreign Preference issues were among the least frequently cited reasons for revocation—two each as compared with 444 citations for criminal conduct and 273 cases with financial issues. Since Foreign Influence and Foreign Preference issues are among the most important issues and are relatively common, these numbers raise questions about the ability of the investigation to obtain information to justify revocation under these guidelines.

Considerations Regarding an Appropriate Denial and Revocation Rate

As discussed in the early sections of this report, personnel security program goals are typically broad statements that do not easily lend themselves to empirical assessment. Although we then discuss the effectiveness of federal personnel security programs in terms of five empirically-oriented objectives, these objectives have never been formally codified in federal or agency-specific policy. This lack of codified empirically-oriented objectives has led some individuals to assume erroneously that program effectiveness can be judged by a readily available empirical outcome—the number of clearance denials and revocations. For example, a 1988 House of Representatives staff report wrote as follows:

> “Continued emphasis on pre-employment background investigations appears misplaced, since it is extremely rare that clearances are denied on the basis of these investigations …. low [adjudicative] standards explain why 99 percent of applicants are granted initial or continued access….Given the low turndown rates

[22] An SSBI was typically performed in response to a request to upgrade an individual’s clearance.

> experienced in the Department of Defense, it is questionable whether the resources and time invested in doing background investigations on all personnel requiring clearances is warranted…. Given these rejection rates, the continued viability and cost effectiveness of the DoD's security background investigation process is seriously in question" (House of Representatives, 1988).

It is not uncommon for critics of the clearance system to refer to a rejection rate of "only" one percent. This is technically accurate but highly misleading, because formal denial or revocation is only the last step in a multistep screening system. The heavy-duty screening is done by applicants themselves deciding not to apply because of the security clearance requirement and by "prescreening" during the application process to eliminate those who are unlikely to qualify for a clearance. As described above, 4% to 5% are then adjudicated unfavorably, but most of those withdraw their applications, resign or retire to avoid having a clearance denial on their record. That leaves about one percent, give or take a few tenths of a percent, whose clearances are formally denied or revoked. The effectiveness of the earlier steps in this screening process depends upon the existence and perceived credibility of the investigation and adjudication.

The rejection rate is influenced by many factors besides the adjudicative standards and how effectively they are implemented. It may be influenced by changes in the applicant pool, changes in prescreening procedures, and changes in the ability of the clearance investigation to identify adverse information. The effectiveness of applicant screening can influence the frequency of subsequent revocations. Revocations could be further reduced by more effective programs to ensure that employees who develop problems receive counseling or treatment before their problems become so bad that revocation results.

It would be easy to increase the number of denials and revocations if so desired, but this would mean a disproportionate increase in the number of "false positives"—individuals who, if their clearances had not been denied or revoked, would have developed into good employees.

Civil rights and simple fairness issues come into play when revoking clearances of existing personnel. In many organizations, revocation of clearance equals termination of employment as there are no suitable positions that do not require a security clearance. Under those circumstances, when an individual has multiple years of experience in an organization, a record of satisfactory performance, and perhaps a family to support, revocation of clearance and termination of employment cannot be done lightly. It requires clear evidence of unacceptable behavior that probably cannot be mitigated by counseling or treatment.

Conclusions

The personnel security adjudications system is working effectively. It can be improved, and work on those improvements is under way. The basic principles underlying the Adjudicative Guidelines are sound, but some updating and clarification is needed and that is already in process.

About 3.9% of all DoD adjudicative decisions were unfavorable in calendar year 2002, including an unspecified number of applicants who were eliminated by a prescreening process or by their own decision not to apply for fear of being turned down. To determine whether 3.9% represents an efficient and effective rate depends on whether the quality and number of individuals in the cleared workforce is adequate. That assessment has not been addressed.

There is inherent tension between the need for general guidelines and the need for consistent adjudicative determinations across agencies and within each agency. Managing that tension requires ongoing monitoring and management oversight to assure an appropriate level of consistency. That effort is now under way.

Opportunities for Improving Federal Personnel Security Programs

Eleven opportunities for improving federal personnel security programs are listed in three categories based on the extent of previous development underlying each opportunity. The first category, Opportunities Based on Extensive Development, represents considerations that have a substantial foundation of research and testing. The second category, Opportunities Based on Partial Development, represents considerations for transferring a well-developed idea in one area into a different area of application. The third category, Opportunities Based on Preliminary Development, represents considerations that are currently being researched and, because they address a critical issue, warrant further exploration.

These eleven opportunities do not constitute an exhaustive list. Each opportunity represents potential for substantially improving the effectiveness of federal personnel security programs by addressing important program needs discussed previously in this report, such as: (1) increasing relative program effectiveness by improving one or more areas of program performance (timeliness, efficiency, fairness), and (2) improving practical definitions and standards for clearance procedures and outcomes. Several opportunities also reflect the rationale—regarding counterintelligence concerns and interest in cost-effective approaches to conducting full-field security background investigations—provided by the Senate Committee on Intelligence (Senate Report 108-044, 2003), where the HR 2417 report requirement on personnel security program effectiveness originated.

Opportunities Based on Extensive Development

Phased SSBI-PR

As an alternative to the traditional SSBI-PR ("full-field") security background reinvestigation, the Phased SSBI-PR approach, outlined in an earlier report section on *Costs and Benefits of a Full-Field Versus a Secret-level Investigation*, is likely to reduce by approximately 42% the investigative costs on approximately 70% of employees requiring an SSBI-PR—with a reliable expectation that no actionable cases would be missed. Because the Phased SSBI-PR and the traditional SSBI-PR entail the same expectation regarding actionable cases, agencies should be permitted—through revised personnel security policy—to use either approach to satisfy the PR for Top Secret, SCI, and "Q"-level PRs.

Automated Continuing Evaluation System (ACES)

ACES queries selected commercial and government databases to identify cleared personnel who appear to be engaging in acts of security concern between regular personnel security investigations. Research indicates that ACES not only enhances the timeliness and efficiency of detecting security-relevant information, it also helps identify serious cases that would have otherwise been missed. Implementation of ACES should continue within DoD along with consideration for possible adoption by personnel security programs in other departments of the Executive Branch.

Adjudicative Guidelines Revision

One of the best ways to improve the effectiveness of personnel security adjudication is to revise the Adjudicative Guidelines to better define listed guidelines and concerns, so that they more directly address emerging areas related to security risk, such as foreign preference among cleared individuals. Such a revised set of adjudicative guidelines is under review by the Personnel Security Working Group (PSWG). This group should complete its review in a timely manner so that an action plan for this area can be developed.

Automated Financial Disclosure Collection

Executive Order 12968, 50 USC 435 (Pub. Law 103-359), and Section 341 of the Intelligence Authorization Act for Fiscal Year 2004 mandate implementation of financial disclosure programs for people granted regular access to one or more of five categories of especially sensitive types of classified information identified by the executive order. The Records Access & Information Security (RA&IS) Policy Coordinating Committee of the National Security Council approved a standard set of data elements to be collected in all financial disclosure programs required under the executive order. A centralized automated data collection system similar to e-QIP should be developed by OPM for those agencies and departments that wish to use it. The software core of that program should be made available to other organizations that chose not to use that centralized collection system because of special security concerns applicable to their population. This would eliminate the need for each agency to build and pay for its own system, as well as assure greater interoperability and data standardization.

Access to National Driver Register Records

The National Driver Register (NDR) is a central repository of information on individuals whose privilege to drive has been suspended or canceled, or who have been convicted of one or more especially serious traffic-related offenses. All 50 states and the District of Columbia participate in the NDR. Among the offenses most applicable to personnel security determinations are: (1) operating a motor vehicle while under the influence of alcohol or a controlled substance, (2) failing to stop and provide identification when involved in an accident resulting in death or personal injury, and (3) perjury or knowingly making a false affidavit or statement to officials about activities governed by a law or regulation on the operation of a motor vehicle. Legislation is needed before the Department of Transportation will allow federal agencies and departments to have routine access to this information for personnel security purposes.

Opportunities Based on Partial Development

Phased SSBI

Because: (1) completed research has consistently indicated that a phased approach will substantially improve the timeliness and efficiency of SSBI-PRs, and (2) in-progress research suggests that similar benefits could be obtained by employing a phased approach to SSBIs (initial "full-field" security background investigations), DoD and other agencies should encourage continued research in this area and determine whether, when, and how to support a policy allowing a phased SSBI to fulfill the requirement for Top Secret, SCI, and "Q"-level background investigations, especially in those cases where the applicant previously held a security clearance.

Adjudication Decision Support (ADS)

Research on phased investigations, clean-case screening, and automated expert systems suggests that an Adjudication Decision Support (ADS) system could offer significant benefits for improving personnel security clearance processing. Using computer-readable records checks and data from a clearance applicant's personnel security questionnaire (e.g., the SF-86), adjudication decisions for some portion of cases deemed to be "clean" could be made in a more objective fashion, be more consistent and fair, and could be accomplished in less time, thereby reducing personnel security program costs, enhancing productivity, and improving customer satisfaction. As the name suggests, the ADS system would be designed to support adjudicators, not replace them. A PERSEREC-sponsored report (Sands, 2001) suggests that it is feasible to develop an ADS by combining expert knowledge available in the CAFs with software algorithms that integrate and process this knowledge.

Investigative Desk Reference (IDR)[23]

Because there is no national standard for topics that should be covered or questions that should be asked in PSIs, there are substantial differences between federal

[23] Text describing the IDR was adapted from a briefing document (August 18, 2003) prepared by J. Richards Heuer.

agencies in the content of their background investigations[24]. The Investigative Standards approved by the National Security Council apply only to what sources should be contacted during an investigation, not to what information should be obtained from those sources or how that information should be obtained. The Adjudicative Guidelines identify topics of security concern, but they are written with language designed to meet the needs of adjudicators, not as guidance for investigators. The need for common guidance for investigators has become more evident and more pressing in recent years due to the widespread privatization of personnel security investigations. Each of these service providers is already conducting investigations for other government agencies. A single source of investigative guidance for these and other contractors would increase efficiency, consistency, inter-agency reciprocity, and quality of investigations.

An Investigative Desk Reference would serve as a job and training aid by providing automated sets of investigative guidance and relevant background information. In form and function, it builds on the success of its adjudicative counterpart, the widely used Adjudicative Desk Reference (ADR). With input and support from the federal personnel security community, it could become a program of "best practices" that represents a voluntary standard for how investigations should be conducted.

Model for Predicting Personnel Security Requirements

Because investigative and adjudicative efficiency is limited by an inability to accurately predict and program for military and industry PSI requirements—which constitute the majority of PSI requirements across the federal government—(1) the Army and Navy should be encouraged to complete their efforts to develop a PSI prediction model that is comparable to the Air Force's, and (2) current efforts to develop a PSI prediction model for industry should continue.

Opportunities Based on Preliminary Development

Counterintelligence Indicators

Personnel security programs can improve their understanding of, and approaches to handling, counterintelligence concerns. Research evidence and risk management logic suggest that counterintelligence risks increase relative to the depth, breadth, and years of access-cleared personnel have had to classified and sensitive material. Two potential improvements in this area warrant further support:

> (1) Widespread agency review of the *Counterintelligence Reporting Essentials* (CORE) list currently under review by DoD's Counterintelligence Field Activity (CIFA) and Counterintelligence Directorate. CORE was developed to improve the security reporting requirement by focusing attention on a smaller set of reportable items consisting primarily of clear behavioral examples of counterintelligence related activities of concern.

[24] Although this is also due in part to different agencies having different needs, there appears to be substantial opportunity for—and potential benefits from—improving standardization.

(2) Enhancing automated counterintelligence monitoring and assessment systems to help identify and better track cases involving cleared personnel that reflect issues of concern, such as significant inconsistencies related to self-reported foreign travel, financial disclosure information, connections, associations, and contacts; sources of wealth; need to know; handling of classified information; or other work or after work activities.

Investigative Quality Assurance Program[25]

Many of the discussions in this report imply a need to better define, measure, and assure investigative quality, which would contribute to improving the effectiveness of security background and clearance procedures, as well as PSI contract monitoring. An investigation quality assurance program should distinguish between the extent to which PSIs (1) comply with formal policy requirements and (2) meet adjudicator, i.e., "customer" needs. Recent research in this area supported by DoD and the intelligence community suggests that good personnel security investigations provide enough relevant information to allow clearance eligibility determinations to be made with confidence. Investigations should satisfy Executive Order 12968 requirements, resolve potentially disqualifying information, be organized and clear, and include all necessary documentation. In accordance with the Privacy Act of 1974, reported information should be complete, accurate, and relevant. Continued community support for efforts to improve investigative quality will result in increased effectiveness of federal personnel security programs.

[25] Text describing the investigative quality area was adapted from a draft document (August 17, 2003) prepared by Daniel Youpa and Ralph Carney at PERSEREC.

References

Aftergood, S. (March 1995). *Secrecy and Government Bullet, 45*. Retrieved September 3, 2003, from http://www.fas.org/spg/bulletin/sec45.html

American Enterprise Institute. (2003). *America after 9/11: Public opinion on the war on terrorism, the war with Iraq, and America's place in the world.* Washington, DC: Author.

Anderson, M. (1996). Personnel security: Now more important than ever. In Sarbin, T.R. (Ed.), *Vision 2021: Security issues in the next quarter century*. Monterey, CA: Defense Personnel Security Research Center.

Barge, B.N., & Hough, L.M. (1983). *Biographical data.* Unnumbered research report. Minneapolis, MN: Personnel Decisions Research Institute.

Barge, B.N., Hough, L.M., Kemery, E., Dunnette, M.D., Kanfer, R., Kamp, J., & Cardozo, M. (1984). *Behavioral reliability: A review of academic literature and organizational programs* (DNA-TR-85-21). Washington, DC: Defense Nuclear Agency.

Barke, C.R., Gerstein, L., & Johnson, S. (1987). *Dimensions of employee integrity: Factor analytic validation of a pre-employment screening measure*. Paper presented at the Annual Meeting of the American Psychological Association, New York, NY.

Barnes, V., Flemming, I., Grant, T., Hauth, J., Hendrickson, J., Kono, B., Moore, C., Olson, J., Saari, L., Toquam, J., Wieringa, D., Yost, P., Hendrickson, P., Moon, D., & Scott, W. (1988). *Fitness for duty in the nuclear power industry: A review of technical issues* NUREG/CR-5227, PNL-6652, BHARC-7000/88018. Seattle, WA: Battelle Human Affairs Research Centers.

Bosshardt, M.J. (2000). *Issues in developing a new conceptual framework for the DoD personnel security program* (Tech. Rep. 361). Minneapolis, MN: Personnel Decisions Research Institutes.

Bosshardt, M.J. (2001). *Does the DoD personnel security program have economic benefits for participating companies? A review and conceptual analysis.* Minneapolis, MN: Personnel Decisions Research Institutes.

Bosshardt, M.J., DuBois, D.A., & Crawford, K.S. (1991). *Continuing assessment of cleared personnel in the military services: Report 1--A conceptual analysis and literature review* (Tech. Rep. 91-001). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M.J., DuBois, D.A., Crawford, K.S., & McGuire, D. (1991). *Continuing assessment of cleared personnel in the military services: Report 2—Methodology,* *analysis, and results* (Tech. Rep. 91-002). Monterey, CA: Defense Personnel Security Research and Education Center.

Bosshardt, M.J., & Lang, E.L. (2002*). Improving the SSBI subject and employment interview processes: A review of research and practice* (Rep. No. 418). Minneapolis, MN: Personnel Decisions Research Institutes.

Boudreau, J.W. (1991). Utility analysis for decisions in human resources management. In Dunnette, M.D., & Hough, L.M. (Eds.) *Handbook of industrial and organizational psychology*. Palo Alto, CA: Consulting Psychologists Press.

Buck, K.R., & Reed, F.M. (2003). *Reliability of centralized criminal record repository checks in lieu of local criminal justice agency checks in four states: California, Florida, Pennsylvania, and Indiana* (Tech. Rep. 03-1). Monterey, CA: Defense Personnel Security Research Center.

Builder, C.H., Jackson, V.G., & Starr, R. (1988). *To repair or rebuild? Analyzing personnel security research agendas* (R-3652-USDP). Santa Monica, CA: RAND.

Carney, R.M. (1996). *SSBI source yield: An examination of sources contacted during the SSBI* (Tech. Rep. 96-001). Monterey, CA: Defense Personnel Security Research Center.

Carney, R.M., & Marshall-Mies, J.C. (2000). *Adjudicative guidelines and investigative standards in the Department of Defense* (Tech. Rep. 00-2). Monterey, CA: Defense Personnel Security Research Center.

Cascio, W.F. (2000). *Costing human resources: The financial impact of behavior in organizations.* Cincinnati, OH: South-Western College Publishing.

Chandler, C.J., Timm, H.W., Massey, K.R., & Zimmerman, R.A. (2001). *Defense Personnel Security Research Center database matching pilot study.* Monterey, CA: Defense Personnel Security Research Center.

Clark, D. (2003, March 25). Data mining sparks debate among lawmakers, administration. *Government Executive Magazine*.

CODA (Community Operational Definition of the Agile Intelligence Enterprise). (1999). *Improving personnel security: A report to the community management staff.* Washington, DC: Author.

Cohen, S.L. (2000). *Security clearances and the protection of national security information law and procedures* (Tech. Rep. 00-4). Monterey, CA: Defense Personnel Security Research Center.

Commission on Protecting and Reducing Government Secrecy. (1997). *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy* (Senate Rep. 105-2). Washington, DC: Author.

Crawford, K.S., & Wiskoff, M.F. (1988). *Screening enlisted accessions for sensitive military jobs* (Tech. Rep. 89-001). Monterey, CA: Defense Personnel Security Research and Education Center.

Crawford, K.S., & Timm, H.W. (2002). *Resource impact of implementing phased SSBI-PRs and the Automated Continuing Evaluation System (ACES)*. Monterey, CA: Defense Personnel Security Research Center.

Crawford, K.S., Riedel, J.A., & Carney, R.M. (1991). *Consolidation of personnel security adjudication in DoD.* Monterey, CA: Defense Personnel Security Center.

Crawford, K.S., Youpa, D.G., & Hagan, S.M. (2000). *An analysis of clearance review decisions by the Defense Office of Hearings and Appeals* (Tech. Rep. 00-1). Monterey, CA: Defense Personnel Security Research Center.

D'Addario, F. (1993, February). Security turns a profit at Hardee's. *Security Management, 3*(2), 30-33.

Defense Personnel Security Research Center (PERSEREC). (1993). *Department of Defense report on personnel security: Fiscal year 1993.* Monterey, CA: Author.

Defense Personnel Security Research Center (PERSEREC). (1995). *Department of Defense report on personnel security: Fiscal year 1995.* Unpublished draft.

Defense Personnel Security Research Center (PERSEREC). (1998, June 10). Objectives of the personnel security system. Memorandum to Bill Leonard, Deputy Director of Security, OASD(C3I).

Defense Personnel Security Research Center (PERSEREC). (2003, October 31). *Interim briefing on the effectiveness of federal personnel security programs: Preparation of a report to DSSC.* Briefing to DSSC and DoD staff.

Defense Security Service. (2004, September 21). *OPM age of pending investigations (FY03/FY04).* Weekly briefing on operations statistics.

Department of Defense, Defense Legal Service Agency (DLSA). (2002). Fiscal year (FY) 2003 budget estimates. Retrieved November 13, 2003, from http://www.Bfd.whs.mil/program/2004-5BES/om/disa/p_FY2004BESOP-5.doc

Department of Defense Industrial Security Review Committee. (1984). *Analysis of the effectiveness of the Department of Defense industrial security program and* *recommendations for program improvement.* Report to the Deputy Under Secretary of Defense for Policy. Washington, DC: Author.

Department of Defense Insider Threat Integrated Process Team. (2000). *DoD insider mitigation: Final report of the Insider Threat Integrated Process Team.* Washington, DC: Author.

Department of Defense Inspector General. (1997). *Personnel security in the Department of Defense* (Rep. No. 97-196). Washington, DC: Author.

Department of Defense Inspector General. (1998). *Audit report: Department of Defense adjudication program* (Rep. No. 98-124). Washington, DC: Author.

Department of Defense Inspector General. (2000a). *Security clearance investigative priorities* (Rep. No. D-2000-111). Washington, DC: Author.

Department of Defense Inspector General. (2000b). *Tracking security clearance requests* (Rep. No. D-2000-134). Washington, DC: Author.

Department of Defense Inspector General. (2000c). *Resources of DoD adjudication facilities* (Draft Rep. No. 9AD-0046.01). Washington, DC: Author.

Department of Defense Inspector General. (2001). *DoD adjudication of contractor security clearances by the Defense Security Service.* Washington, DC: Author.

Department of Defense Security Review Commission. (1985). *Keeping the nation's secrets: A report to the Secretary of Defense by the Commission to Review DoD Security Policy and Practices*. Washington, DC: Author.

Department of Defense, Under Secretary of Defense (Comptroller). (2000, June). Memorandum, *Personnel clearance backlog and security initiatives.*

Department of Defense, Office of the Assistant Secretary of Defense (1999, February). *Verbal attestation upon the granting of security access*. Memorandum.

Department of Energy, Office of Security. (2003). *Personnel security assurance program: Profile from 1992 through 2002* (Rep. No. ORISE 03-0953). Washington, DC: Author.

Dictionary of Military and Associated Terms. Retrieved November 3, 2003, from http://www.dtic.mil/doctrine/jel/doddict

DoD Directive 5200.2-R., Personnel Security Program Regulation (January 1, 1987, revised February 23, 1996).

DoD Directive 5200.2-R, Personnel Security Program Regulation (draft, June, 2002).

DoD Industrial Security Review Committee (1984, December 10). Analysis of the effectiveness of the Department of Defense industrial security program and recommendations for program improvement (“Harper” report), p. 24. Report to the Deputy Under Secretary of Defense for Policy. Washington, DC: Author. (FOUO).

Executive Order 10450, Security Requirements for Government Employment, April 29, 1953.

Executive Order 12968, Access to Classified Information, August 2, 1995.

Fischer, L.F., & Morgan, R.W. (2002). *Sources of information and issues leading to clearance revocations* (Tech. Rep. 02-1). Monterey, CA: Defense Personnel Security Research Center.

Flyer, E. (1986). *Personnel security research: Prescreening and background investigations* (Rep. No. 86-01). Alexandria, VA: HumRRO International.

General Accounting Office. (1995). *Background investigations: Impediments to consolidating investigations and adjudicative functions* (GAO/NSIAD-95-101). Washington, DC: U.S. Government Printing Office.

General Accounting Office. (1999). *DoD personnel: Inadequate personnel security investigations pose national security risks* (GAO/NSIAD-00-12). Washington, DC: U.S. Government Printing Office.

General Accounting Office. (2000). *More actions needed to address backlog of security clearance reinvestigations* (GAO/NSIAD-00-215). Washington, DC: U.S. Government Printing Office.

General Accounting Office. (2000). *Weaknesses in security investigation program are being addressed.* Testimony by Carol C. Schuster (GAO/T-NSIAD-00-65). Washington, DC: U.S. Governing Printing Office.

General Accounting Office. (2001). *DoD personnel: More consistency needed in determining eligibility for Top Secret security clearances* (GAO 01-465). Washington, DC: U.S. Governing Printing Office.

General Accounting Office. (2004). *DoD personnel clearances: Additional steps can be taken to reduce backlogs and delays in determining security clearance eligibility for industry personnel* (GAO 04-632). Washington, DC: U.S. Governing Printing Office.

Gray, J. (October 29, 2001). Loss of security clearances*.* *Bulletin.* U.S. Army Medical Command, Civilian Personnel Division.

Gruber, A. (2003, July 11). OPM completes system for filing security clearance forms online. Retrieved November 12, 2003, from http://www.govexec.com/dailyfed/0703/071103a1.htm

Harowitz, S.L., & Hargreaves, G. (1997). Security's positive return. *Security Management, 41*(10), 28-34.

Hein, A.F. (2002). *A prescreening model for the intelligence community.* Washington, DC: The Personnel Security Managers' Research Program, January 2002.

Helm & Associates. (1985). *Validation of the RELY: An inventory designed to measure job applicants' attitudes toward good work ethic, absenteeism, and punctuality* (Tech. Rep. 1409). Dallas, TX: Author.

Herbig, K.L., & Wiskoff, M.F. (2002). *Espionage against the United States by American citizens 1947-2001* (Tech. Rep. 02-5). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1991a). *Alcohol use and abuse* (Tech. Rep. 91-010). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1991b). *Financial irresponsibility: Background information for security personnel* (Tech. Rep. 91-011). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1992). *Compulsive gambling: Background information for security personnel* (Tech. Rep. 92-006). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1993). *Crime and security risk: Background information for security personnel* (Tech. Rep. 93-005). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1994). *Drug use and abuse: Background information for security personnel* (Tech. Rep. 94-003). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1998). *Adjudicator's desktop reference guide*. Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J. (1999). *The changing environment for the national industrial security program.* Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J., Crawford, K.S., Kramer, L.A., & Hagan, R.R. (2001). *A new approach to the SSBI-PR: Assessment of a phased reinvestigation* (Tech. Rep. 01-6) (FOUO). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J., Crawford, K.S., Kirkpatrick, S.N., & Kramer, L.A. (2003). *Final report on DSS test of phased reinvestigation* (Tech. Rep. 02-2). Monterey, CA: Defense Personnel Security Research Center.

Heuer, R.J., Youpa, D.G., & Carney, R.M. (2003). *Proposed update and clarification of the adjudicative guidelines for determining eligibility for access to classified information and/or assignment to sensitive positions* (Working Paper 03-1). Monterey, CA: Defense Personnel Security Research Center.

Hough, L.M. (1986). *Utility of temperament, biodata, and interest assessment for predicting job performance: A review and integration of the literature* (Tech. Rep. 145). Minneapolis, MN: Personnel Decisions Research Institutes.

House of Representatives. (1988). *U.S. counterintelligence and security concerns: A status report – Personnel and information security.* Report by the Subcommittee on Oversight and Evaluation of the Permanent Select Committee on Intelligence. Washington, DC: U.S. Government Printing Office.

Hunter, J.E., & Hunter, R.F. (1984). Validity and utility of alternative predictors of job performance. *Psychological Bulletin, 96*(1), 72-98.

Insurance Information Institute (2000, July). Retrieved November 12, 2003, from http://www.iii.org/media/issues/workerscomp.html

Intelligence Authorization Act for Fiscal Year 2004, H.R. 2417, 108th Cong. (2003).

Joint Security Commission. (1994). *Redefining security: A report to the Secretary of Defense and the Director of Central Intelligence.* Washington, DC: Author.

Joint Security Commission. (1999). *Report by the Joint Security Commission II.* Washington, DC: Author.

Jones, J.W., & Wuebker, L.J. (1988). Accident prevention through personnel selection. *Journal of Business and Psychology, 34*, 187-198.

Jones, J. W., Slora, K.B., & Boye, M.W. (1990). Theft reduction through personnel selection: A control group design in the supermarket industry. *Journal of Business and Psychology, 5*(2), 275-278.

Kapner, S. (1996). Background checks eyed as workplace safety measure. *Nation's Restaurant News, 30*(21), 3.

Kramer, L.A., Crawford, K.S., Heuer, R.J., & Hagen, R.R. (2001). *SSBI-PR source yield: An examination of sources contacted during the SSBI-PR* (Tech. Rep. 01-5). Monterey, CA: Defense Personnel Security Research Center.

Kramer, L.A., Heuer, R.J., & Crawford, K.S. (in review). *Technological, social, and economic trends that are increasing U.S. vulnerability to insider espionage.* Monterey, CA: Defense Personnel Security Research Center.

Kramer, L.A., & Richmond, D.A. (in press). *A new approach to the SSBI: Assessment of a phased single-scope background investigation* Monterey, CA: Defense Personnel Security Research Center.

Lang, E.L., & Herbig, K.L. (2002). *Model for a future defense personnel security system* (Tech. Rep. 03-2). Monterey, CA: Defense Personnel Security Research Center.

Lardner, R. (1997, February 1). Access denied. *Government Executive Magazine.*

Lee, R., & Booth, J.M. (1974). A utility analysis of a weighted application blank designed to predict turnover for clerical employees. *Journal of Applied Psychology, 59*, 516-518.

Lins, S., & Erickson, R.J. (1998). Stores learn to inconvenience robbers. *Security Management, 42*(11), 49-53.

Longmore-Etheridge, A. (1999). Stop insiders from eating profits. *Security Management, 43*(11), 61-63.

McDaniel, M.A. (1989). Biographical constructs for predicting employee suitability. *Journal of Applied Psychology, 74*, 964-970.

Mitchell, D. (1999). *Proposal for a new focus in personnel security investigation*. Arlington, VA: Defense Security Service.

Moore, J.N., Plesser, R.L., & Jaksetic E. (1988). *Due process in matters of clearance denial and revocation: A review of the case law*. Monterey, CA: Defense Personnel Security Research Center.

National Counterintelligence Policy Board. (1998). *Foreign intelligence threat awareness programs: A review* (Tech. Rep. 98-001). Monterey, CA: Defense Personnel Security Research Center.

National Research Council. (2003). *The polygraph and lie detection.* Washington, DC: Board on Behavioral, Cognitive, and Sensory Sciences and Education (BCSSE), Committee on National Statistics (CNSTAT).

Office of the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) (OASD[C3I]. (2001). *Mission degradation! Personnel security investigations: A readiness issue.* Washington, DC: Author.

Office of Personnel Management Investigations Service. (1999). *Personnel investigations processing system*. Washington, DC: Author.

Ones, D.S., Viswesvaan, C., & Schmidt, F. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology, 78*(4), 697-703.

Palmer, A.B., & Eisle, G.R. (2003). *A theoretical foundation for security risk assessments*. Center for Human Reliability Studies, Oak Ridge Institute for Science and Education, Oak Ridge, TN, Document No. ORISE 03-0577, June 2003.

Perry, R.W., Bennett, C.A., & Wood, M.T. (1979). *The role of security clearances and personnel reliability programs in protecting against insider threats* (B-HARC-411-018). Seattle, WA: Battelle Human Affairs Research Centers.

Personnel Security Investigations Process Review Team. (2000a, October). *An assessment of DoD's plan to eliminate the periodic reinvestigation (PR) backlog: Report to the Deputy Secretary of Defense*. Washington, DC: Author.

Personnel Security Investigations Process Review Team (PRT). (2000b, October). *An assessment of the Department of Defense personnel security program*. Washington, DC: Author.

Personnel Security Investigations Process Review Team (PRT). (2002, May). *Draft report to C3I to determine the optimal mix of personnel security investigations between DSS, OPM, and contractors*. Washington, DC: Author.

Personnel Security Managers' Research Program. (2003a). *Literature review and discussion of adjudicative guideline H: Drug involvement* (Rep. No. ORISE 02-1542). Oak Ridge, TN: Center for Human Reliability Studies, Oak Ridge Institute for Science and Education.

Personnel Security Managers' Research Program. (2003b). *Literature review and discussion of adjudicative guideline G: AlcohoilcConsumption* (Rep. No. ORISE 02-1543). Oak Ridge, TN: Center for Human Reliability Studies, Oak Ridge Institute for Science and Education.

Personnel Security Managers' Research Program. (2003c). *Literature review and discussion of adjudicative guideline D: Sexual behavior* (Rep. No. ORISE 02-1544). Oak Ridge, TN: Center for Human Reliability Studies, Oak Ridge Institute for Science and Education.

Personnel Security Managers' Research Program. (2003d). *Literature review and discussion of adjudicative guideline I: Emotional, mental, and personality disorders* (Rep. No. ORISE 02-1541). Oak Ridge, TN: Center for Human Reliability Studies, Oak Ridge Institute for Science and Education.

Personnel Security Overarching Integrated Process Team (OIPT). (2000, February 28). *Improving the PSI process. Briefing to the Deputy Secretary of Defense.*

Pound, E.T. (2000, June 8). Senators want tougher security clearances. *USA Today*.

Reilly, W., & Joyal, P. (1993). *Project SLAMMER: A critical look at the Director of Central Intelligence Directive No. 1/14 criteria.* Washington, DC: Director of Central Intelligence.

Riedel, J.A., & Crawford, K.S. (1993). *Due process for adverse personnel security determinations in the Department of Defense* (Tech. Rep. 93-006). Monterey, CA: Defense Personnel Security Research Center.

Rossi, P.H., Freeman, H.E., & Wright, S.R. (1979). *Evaluation: A systematic approach*. Beverly Hills, CA: Sage Publications.

Sands, W.A. (2001). *Development of a personnel security clearance adjudication decision support system for the Department of Defense.* San Diego, CA: Chesapeake Research Applications.

Schmitt, E. (2003, May 15). New Army rules on ways to cope with civilian life. *The New York Times*.

Schmidt, F.L., & Hoffman, B. (1973). Empirical comparison of three methods of assessing utility of a selection device. *Journal of Industrial and Organizational Psychology, 11*, 13-22.

Schmidt, F.L. & Hunter, J.E. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin, 124*(2), *262-274*.

Schmidt, F.L., Mack, M.J., & Hunter, J.E. (1984). Selection utility in the occupation of U.S. park ranger for three modes of test use. *Journal of Applied Psychology, 69*(3), 490-497.

Schmitt, N., Gooding, R.Z., Noe, R.A., & Kirsch, M. (1984). Meta-analysis of validity studies published between 1964 and 1982 and the investigation of study characteristics. *Personnel Psychology, 37*, 407-422

Senate Report 108-044 (2003). *Authorizing Appropriations for Fiscal Year 2004 for Intelligence and Intelligence-Related Activities of the United States Government, the Community Management Account, and the Central Intelligence Agency Retirement and Disability System, and for Other Purposes.*

Shahandeh, B. (1985). Drugs and alcohol abuse in the workplace: Consequences and countermeasures. *International Labour Review*, *124*(2), 207-223.

Shaw, E.D., Ruby, K.G., & Post, J.M. (1998). *Insider threats to critical information systems*. Bethesda, MD: Political Psychology Associates.

Smith, T.W. (1996). *Public attitudes towards security and counter-espionage matters in 1994 and 1996.* Chicago, IL: National Opinion Research Center.

Stevens, G.M. (2003). *Privacy: Total information awareness programs and related information access, collection, and protection laws*. Washington, DC: Library of Congress, Congressional Research Service.

Timm, H.W. (2001). *Estimated impact of the proposed automated continuing evaluation system (ACES) on personnel security effectiveness: A preliminary feasibility assessment* (Tech. Rep. 01-3). Monterey, CA: Defense Personnel Security Research Center.

Tippit, J.D., Rizzoli, R.A., Denk, R.P., & Fischer, L.F. (2001). *Defining the DSS training mission* (Mgt. Rep. 01-5). Monterey, CA: Defense Personnel Security Research Center.

TRW, Inc. (1999). *Evaluation of DSS CCMS: Final report.* Fairfax, VA: Author.

TRW, Inc. (2000). *In-progress review of DSS CCMS remediation activities, one year later: Final report*. Fairfax, VA: Author.

United States Senate. (2003). *Energy Department Polygraph Program*. Hearing before the Senate Energy and Natural Resources, 116th Congress (testimony by Kyle E. McSlarrow). Retrieved October 15, 2003, from http://www.nexis.com/research/snews/emailAlert?_pnewsAlert=0x000b4d7b-0x0002cc88%2f0x000b4d7b%2f20030905%2f08%3a18%3a29

U.S. Merit Systems Protection Board. (1993). *Whistleblowing in the federal government: An update.* Washington, DC: Author.

Webster's Third New International Dictionary of the English Language Unabridged (1986). Springfield, MA: Merriam-Webster, Inc.

Winans, B., & Cairns, G. (1996). Background checking: Reducing workers' compensation claims. *Risk Management, 43*, 31-32.

Wood, S. (2001). *Public opinion of selected national security issues: 1994-2000* (Mgt Rep. 01-4). Monterey, CA: Defense Personnel Security Research Center.

Wood, S., & Fischer, L.F. (2002). *Cleared DoD employees at risk – Report 2: A study of barriers to seeking help* (Tech Rep. 01-4). Monterey, CA: Defense Personnel Security Research Center.

Wood, S., & Marshall-Mies, J.C. (2003). *Improving supervisor and coworker reporting of information of security concern* (Tech. Rep. 02-3). Monterey, CA: Defense Personnel Security Research Center.

Wood, S., Crawford, K.S., & Lang, E.L. (in review). *Reporting of counterintelligence and security indicators by supervisors and coworkers.* Monterey, CA: Defense Personnel Security Research Center.

Appendix A

History of Federal Personnel Security Policies, Programs, and Reforms

History of Federal Personnel Security Policies, Programs, and Reforms[26]

Personnel security programs across the federal government focus on two primary elements. Historically, the largest element concerns the determination of eligibility or continuing eligibility for employment or access. The second element addresses education and training of the employee. The personnel security program did not deal with security training until the early 1950s and then only for specific types of sensitive duties or access. It was not until 1957 that employee training became a general concern. The following history highlights developments regarding these two elements.

Determination of Eligibility

The history of the nation's personnel security program began in the 19th century with an act of Congress, specifically the Civil Service or Pemberton Act of 1883. Section 5.2(a) of the act authorized the investigation of the qualifications and suitability of candidates for positions in the civil service. The next impetus for change came in the 20th century. The assassination of President McKinley in 1901, the growing Anarchist movement, and World War I represented significant threats to national security. These events provided motivation to Congress and the President to develop policies to identify and control individuals who could present a threat to national security.

In 1917, President Woodrow Wilson signed a confidential executive order that enabled the head of "a department or independent office" to remove any employee for "conduct, sympathies, or utterances, or because of other reasons growing out of the war."

In 1919, the Communist Party was formed in the United States. The party represented, for the first time, a radical group in America that owed its allegiance to a foreign government. In 1938, Congressman Dies chaired the Special Committee on Un-American Activities. His committee, which investigated alleged radical organizations, created much distrust by its errors, sensationalizing, and misstatements. One of the results of this committee, however, was greater public and Congressional awareness that federal employees with access to, or control of, sensitive information could be disloyal.

In 1939, the Hatch Act was modified to include Section 9-A. This section prohibited federal employees from being members of organizations that advocate the overthrow of the U.S. government. It is this modification that provided the authority for the next generation of personnel security investigations. In 1940, Public Law 713 was enacted allowing the War Department to dismiss anyone for "conduct inimical to the public interest in the defense program of the United States." Congress ensured this bill had due process provisions added to it before passage.

In June 1940, the Civil Service Commission issued Circular 222, which defined Section 9-A of the Hatch Act as the Communist Party, the German Bund or any other

[26] This Appendix draws on previous material prepared by Kathy Herbig (Northrop Grumman Mission Systems) and Richard Rizzoli (The Tippit Group). Much of the material was current as of October 2002 and some updated material has been added.

Communist, Nazi, or Fascist organization, and directed agency heads to remove employees suspected of such membership. The Civil Service Commission, after issuing this circular, began investigating and adjudicating allegations of violations of Section 9-A for employment applicants. The burden of investigating existing employees fell to the Justice Department, which, due to the war effort, was unable to carry out its mission. It became so ineffective that a presidential order directed the Justice Department to investigate incumbent federal employees only at the specific request of a department or agency, even though an allegation may have been made against the employee.

In 1940, Public Law 713 was enacted, which allowed the War Department to dismiss anyone for "conduct inimical to the public interest in the defense program of the United States." Due process provisions were added to the bill. Public Law 808 removed protections of civil service employees and allowed summary dismissal of employees in the War Department, Navy Department, or Coast Guard. This statute remained until 1950.

In 1942, the Attorney General set up the Interdepartmental Committee to assist agencies in this process. Since the authority for the committee was the Hatch Act, this limited the activities of the committee to allegations involving subversive organizations, and they could not address individual ideologies, basic loyalty, or other issues. The major accomplishment of this committee was the education of federal agencies on handling investigative reports, the idea of a preliminary investigation, and the dissemination of intelligence concerning organizations considered subversive. By the Justice Department's own conclusion, the result of the Interdepartmental Committee was that the "futility and harmful character of a broad personal inquiry have been too amply demonstrated" and that membership in a Communist organization did not necessarily indicate disloyalty.

In 1943, the President issued Executive Order 9300, Establishing the President's Interdepartmental Committee to Consider Cases of Subversive Activity on the Part of Federal Employees. This committee was the responsibility of the Justice Department. It was tasked to consider the problem of subversive activity in all of its forms. The committee decided that the term "subversive activity" must be clearly defined. It concluded that the only legal definition was that of the Hatch Act. The Dies committee, still in existence in 1943, broadened the definition of subversive activities to include "technocracy" and "nudism."

In February 1945, copies of over 1,000 classified documents, some Top Secret, were found in the office of the magazine *Amerasia*. This incident fueled concerns about internal threats, kept the loyalty issue alive, and helped plant the seed of trustworthiness issues. In January 1945, the Civil Service Committee of the House of Representatives was ordered to make a study of loyalty among federal employees. Its conclusion was that more research was needed, and it recommended that a committee be formed to develop a unified program to address loyalty in the federal service. In 1946, the McCarran Amendment gave the Secretary of State the right to summarily dismiss employees believed to be subversive.

On November 25, 1946, the President issued Executive Order 9806, Establishing the President's Temporary Commission on Employee Loyalty. This addressed the questions of existing standards, adjudications, and procedures for holding hearings. One of the commission's conclusions was that, due to the limitations of Executive Order 9300, individuals who commit subversive acts for purposes of personal gain could not be addressed. It concluded that existing security standards were inadequate. It recommended the screening of all applicants and, where derogatory information was found, a full-field investigation. In the case of individuals assigned to a sensitive position, a full-field investigation should be conducted whether derogatory information is present or not. The investigation of employees should be the responsibility of each agency. For continuity of interagency policies, however, it recommended an advisory agency be created.

On March 21, 1947, the President signed Executive Order 9835, Prescribing Procedures for the Administration of an Employee Loyalty Program in the Executive Branch of the Government. This order was the first to establish a comprehensive personnel security program. It not only included personnel screening, but also addressed employee suitability. It established the requirement for uniform polices for the protection of sensitive documents applicable to all agencies and departments. Nowhere, however, was the idea of a recurring investigation mentioned. Investigations were thought of only in response to a new employee, an allegation, or some other suspicion.

A letter published in *The New York Times* on April 13, 1947, authored by a team of Harvard law professors, summed up the order's shortcomings as disregarding centuries of experience in developing proper standards for reaching just decisions. Concern was expressed that the Attorney General's list (created by the order) violated the Constitution by listing political organizations. The program officially began on October 1, 1947.

On January 23, 1951, the President created the Commission on Internal Security and Individual Rights in order to "consider afresh in all its present-day ramifications the recurrent question of how a free people protect their society from subversive attack without at the same time destroying their liberties." Almost immediately, the National Security Resources Board superseded it, addressing the same issues. This board made a broad review of existing security programs and recommended that the three personnel programs (loyalty, suitability, and security) be merged into one and that all three aspects of the individual be considered concurrently. This marked a distinct change in philosophy for the personnel security program and paved the way for the present system.

Executive Order 10450, Security Requirements for Government Employment, was created in response to increasing security concerns. Although amended, it has changed little since April 24, 1953, when it was issued. It states that ". . . all persons privileged to be employed in the departments and agencies of the Government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States . …" These words form the standard for employment in the federal government. The order (as amended) requires agency heads to classify positions for sensitivity in relation to national security. An investigation appropriate to the sensitivity level is required on each person employed by the government to determine that his/her employment is clearly consistent with the interests of national security.

Starting with this order, the issue of suitability, sensitive positions, and access to classified national security information began to move apart as separate orders continued to define the differences. Today, we still have three separate programs. In 1960, the concern for fairness and a lack of authority in the present industrial clearance system with industry personnel resulted in Executive Order 10865, Safeguarding Classified Information Within Industry (as amended).

National Security Directive 63 established in 1991 single-scope background investigative standards for access to Top Secret/National Security Information and Sensitive Compartmented Information. In 1995, Executive Order 12968, Access to Classified Information, modified the requirements for access to classified information, thereby increasing individual reporting requirements. In 2000, the National Defense Authorization Act for Fiscal Year 2001 added a requirement that officers and employees of DoD, active duty members of the armed forces, and employees of DoD contractors cannot be granted a security clearance if they have been convicted in any U.S. court of any crime and sentenced to a term exceeding one year.

There are other major areas where authority for a more narrowly defined application of a personnel security program has been granted. Some of these areas have significant implications for government agencies:

In 1954, the Atomic Energy Act, now codified in Title 50 U.S.C., authorized the investigation and adjudication of individuals having access to nuclear technology. This authority is vested with the Department of Energy (DOE), which prescribes regulations in this area.

The 1947 National Security Act, codified in Title 50 U.S.C., created a Director of Central Intelligence (DCI) and gave some authority to the Director to prescribe rules for access. On December 4, 1981, Executive Order 12333, United States Intelligence Activities, authorized the DCI to promulgate rules to control access to intelligence information. This system created the now familiar system of DCI Directives (DCIDs). These DCIDs address personnel security requirements as well as security training requirements.

In 1987, the Computer Security Act was passed (codified in Title 15 & 40 U.S.C.). Advances in information technology, and the resultant risks, required that access to government computer systems be controlled. The Office of Management and Budget (OMB) (charged under the Act) issued Circular A-130, which authorized the "screening" of individuals commensurate with the "risk and magnitude of harm" they could cause to the system.

Education and Training

A study on security training mandates (Tippit, Rizzoli, Denk, & Fischer, 2001) summarizes the area of education and training regulations:

> The source of national policy for security training requirements comes from public laws, Executive Orders, National Security Directives, and other executive promulgations (SPB NSC, NSTISSC, etc.). Agencies may be directed by such laws or promulgations to develop implementing policies that are applicable to all agencies. In some cases, the law or order may create a department with the specific purpose to develop implementing regulation. Implementing regulations promulgated by agencies and departments may direct training even though the original authority did not specifically require it. In addition, some requirements are addressed only to government employees and some only to contractor personnel.

Executive orders for the protection of classified national security information have been issued since November 5, 1953, with Executive Order 10501, Safeguarding Official Information. These orders have always required security training. The most recent, Executive Order 12958 of April 12, 1995, Classified National Security Information, still contains a training mandate.

Executive orders and public laws require federal employees to be trained to be competent in their assigned responsibilities. Since 1958, the Government Employees Training Act (GETA), codified under Title 5 U.S.C., has been the primary source of government training policy. It required each agency to develop a training program in accordance with its needs. This statute provided the authority for an agency to perform training of its employees. In 1967, Executive Order 11348, Providing for the Further Training of Government Employees, directed OPM to coordinate interagency training programs and assist agencies in the implementation of training programs.

Background on DoD Implementation of Personnel Security Requirements

A brief introduction to the organization of personnel security requirements within DoD will assist in understanding this area.

There are multiple statutory authorities within DoD to promulgate policy that are independent of the authority of the Secretary of Defense. The Army, Navy, and Air Force each is defined as an agency under Title 5 U.S.C. and thus has independent authority to promulgate agency implementing policies. Secretaries of the armed services also have statutory authority to promulgate policies. The Joint Chiefs of Staff have statutory authority over policies relating to military training. Combat commanders have independent (from DoD policy) authority over personnel under their command. The Army, Navy, Air Force, Marine Corps, National Geospatial Intelligence Agency (NGA, formerly the National Imagery and Mapping Agency [NIMA]), National Reconnaissance Office (NRO), National Security Agency (NSA), Defense Intelligence Agency (DIA), and "other offices within the DoD for the collection of specialized national intelligence through reconnaissance programs" have intelligence-related authorities outside DoD.

The general system of DoD-level policy dissemination is by directive. This system is itself described by a directive: DoD Directive (DoDD) 5025.1, DoD Directives System, and its corresponding Manual. This is a complicated system that issues the following type of documents: directives, directive-type memorandums, instructions, administrative instructions, publications, catalogs, directories, guides, handbooks, indexes, inventories, lists, manuals, modules, pamphlets, plans, regulations, and standards. Issuances may be unclassified or classified. Not all types of issuances have regulatory authority. Mandatory compliance is not required for handbooks and guides. The JCS issue their own system of issuances in the form of JCS publications. In addition, each DoD component issues its own implementing guidance.

DoD has promulgated security issuances primarily in the 5200 - 5299 series of its system of directives. Many address personnel security requirements. This series is organized into the following components: 5200 General; 5205 Special Programs; 5210 Personnel, Facilities, and Classification Guides; 5215 Computer Security; and 5220 Industrial Security. Issuances in other areas also address personnel security policies such as DoDD 5105 that deals with the responsibilities of the Defense Security Service (DSS); DoDD 2000.12 DoD, Antiterrorism/Force Protection (AT/FP), that covers antiterrorism training; and DoDD 5160.54, Critical Asset Assurance Program (CAAP), that discusses training for CAAP personnel. As stated earlier, there are also directive-type memorandums that address security training. One example is Assistant Secretary of Defense (ASD) (C3I), DoD Memorandum: Security Training for Laboratory Personnel, May 5, 2000, that requires DSS to develop and provide tailored security training to DoD laboratory staffs.

DoD Personnel Security System Components

The personnel security program also addresses employment suitability and trustworthiness (including loyalty) issues, as well as access to specific sensitive types of information or activities, facilities, or duties. The implementation of these programs is contained in a number of issuances. In addition, personnel security is integral to the other major components of the DoD security system, i.e., physical security, information security, communication security, and computer security.

DoD Directive 5210.9, Military Personnel Security Program, first issued in 1956, established the military personnel security program, which requires the military to abide by the same loyalty standards as civilians. DoD Directive 5200.2, DoD Personnel Security Program, and its corresponding regulation have subsequently superseded it.

DoD Directive 5200.2 is also the primary implementing directive for Executive Order 10450, Executive Order 12958, and the personnel security elements of the Computer Security Act. DoD components implement the program through their own regulations to various degrees. Contractor personnel who are to be accorded access to classified information must be processed through DoD Directive 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoD 5220.22-M, National Industrial Security Program Operating Manual; and DoD 5220.22-R, Industrial Security Regulation.

Personnel security training and continuing education is a critical element of the personnel security program and is addressed in over 50 DoD issuances (Tippit et al., 2001). The linkages between the overall DoD personnel security system and requirements for the protection of nuclear weapon elements security are contained in DoDD 5210.42, Nuclear Weapons Personnel Reliability Program (PRP). The DoD PRP was created in 1962 in response to concerns about the appropriate handling of nuclear materials within existing and emerging weapon systems. Independent PRP programs are operated by each of the services in response to the overall DoD mission.

For military employees, entry to the personnel security system begins with prescreening, generally conducted by a military service component. DSS or the OPM then conduct personnel security investigations that enable adjudication offices to reach a determination on whether to grant eligibility.

Once inside the personnel security system, individuals are subject to continuing command evaluation and periodic reinvestigations (depending on their assignment) to determine their continuing eligibility. Throughout their career they are provided with continuing awareness training to ensure their vigilance against espionage and instill good security practices. Within the system, individual security status can be changed. The level of clearance or access often changes, and sometimes individuals lose their clearance if they no longer need one, or if derogatory information causes its revocation.

Government Organizations Participating in Personnel Security

There are a large number of organizations that make up the personnel security and intelligence communities. DoD is the largest of 13 federal agencies that grant security clearances. The others are the following:

- Central Intelligence Agency
- Department of Agriculture
- Department of Commerce
- Department of Energy
- Department of the Interior
- Department of Justice
- Department of State
- Department of Transportation
- Department of Treasury
- Federal Bureau of Investigation
- National Security Agency

Some of these organizations have their own procedures for conducting investigations, adjudicating the results of the investigations, and granting clearances. CIA and

DOE are examples. Some agencies use the investigative services of other agencies; for example, the following is a list of government entities that request personnel security investigations from DoD.

- Army
- Navy
- Air Force
- Marines
- Coast Guard
- Defense Office of Hearing and Appeals
- DIA: Defense Intelligence Agency
- NSA: National Security Agency
- JCS: Joint Chiefs of Staff
- WHS: Washington Headquarters Services
- White House (for DoD assignees only)
- DISA: Defense Information Systems Agency
- DISCO: Defense Industrial Security Clearance Office
- DLA: Defense Logistics Agency
- NIMA: National Imagery and Mapping Agency
- DeCA: Defense Commissary Agency
- DSCA: Defense Security Cooperation Agency
- DFAS: Defense Finance & Accounting Services
- DTRA: Defense Threat Reduction Agency
- DCAA: Defense Contract Audit Agency
- LOC: Library of Congress
- OSD: Office of the Secretary of Defense
- USMEPCOM: Military Entrance Processing Command
- DoDIG: Department of Defense Inspector General
- GAO: General Accounting Office
- DSS: Defense Security Service

Recent Key Research Efforts

A recent report (Lang & Herbig, 2002) discusses the current DoD personnel security research program and the relationship between the two main providers of personnel security investigations, DSS (DoD's designated investigation agency) and OPM. This report also compares the practices of five representative federal agencies that do background investigations or adjudications of security clearances: DoD's DSS, OPM, DOE, CIA, and NRO. Overall, the report found "several important differences in procedures and assumptions across federal personnel security programs, implying that there is a range of workable approaches to procuring a trustworthy workforce."

Kramer, Crawford, Heuer, and Hagen (2001) examined the productivity of sources contacted during the SSBI-PR to disclose potentially derogatory information for four government agencies (DoD, CIA, NRO, and NSA). Important information was obtained concerning the ways in which the different agencies conduct their investigations.

Another recent report (Herbig & Wiskoff, 2002) reviewed espionage of American citizens against the United States since the start of the Cold War. Data were obtained from public sources, with verification obtained in many cases by the government agencies whose information was compromised.

In 1996, PERSEREC was asked by the National Counterintelligence Policy Board to review the effectiveness of foreign intelligence threat awareness (FITA) programs in the Executive Branch and among government contractors. The resulting report examined the programs of 31 Executive Branch agencies or organizations. The agencies varied greatly according to size and mission. Protocols were received from 71 providers and surveys from 1,401 audience members. In addition, team members interviewed 60 senior representatives, mostly directors of security of companies contracted to the federal government. This study documented the effectiveness of FITA programs across the government and recommended methods to improve the quality and accessibility of threat information (National Counterintelligence Policy Board, 1998).

Professional Development of the Security Workforce

During the past 2 years initiatives have been under way to promote training and professional development in the security workforce to include all personnel who perform personnel security functions in the Federal government and its contractor community. The Joint Security Training Consortium (JSTC) was established in FY02 to address perceived deficiencies in security training programs. Its objective is to build a security workforce that possesses the skills needed to effectively address the contemporary security environment and that has recognized professional standing among other national security disciplines. The JSTC works to this end via four interrelated core functions:

1. Develop common policies for training and professional development
2. Evaluate and develop professional certification programs
3. Establish standards for and reciprocity among security training programs
4. Articulate training requirements and support their fulfillment

JSTC sponsors, DoD and the Intelligence Community, have identified $22 million to fund this program through FY07. PERSEREC had provided foundation research for this effort and is also supporting the development of on-line products to assist the security practitioners and agencies. One such product, a comprehensive catalog of government, academic, and commercial security training providers, is now located on the JSTC web site.

Researchers have identified and published a compendium of training mandates and their source issuances that apply to security professionals in DoD and the Intelligence Community. A guide for the development of national- and agency-level policy, for agencies lacking an established security training policy, is nearing completion.

Extensive work was also undertaken to describe and evaluate professional development programs for security personnel in several intelligence agencies, military departments, DoE, and in the government contractor community for the purpose of identifying program elements that work well as opposed to those that have been less successful. This was followed by efforts (through personal interviews with senior officials, focus groups with security practitioners, and a workforce survey) to determine preferences and priorities for professional development and certifications programs for the federal security community.

Findings from the survey in particular confirmed a strong consensus in favor of professional development programs as well as for a certification system for security practitioners. However, respondents were divided on whether they had access to appropriate training to do the work to which they were assigned. Focus group and survey participants expressed very positive views about their work in the security disciplines, but were uncertain about pursuing a long-term career in this field.

An early effort by the research team to define the security profession in terms of seven core disciplines and major functional areas has supported a concerted effort by JSTC to identify essential knowledge and skills required for proficiency in each discipline. A series of workshops and panels has led to the verification of skill standards for information security, physical security, and two functional areas in personnel security (background investigations and adjudications). In December of 2003, a panel of subject matter experts met in Monterey to identify skill standards for the remaining functions in the Personnel Security discipline. This work was a necessary first step to the identification of reciprocal standards for security training across the Federal government. The standards can be applied in the evaluation of existing training or in the development of new courses or training modules. Another application of skill standards may be seen in the writing of contract specifications and in the evaluation of contractor personnel who apply for support service positions (e.g., background investigations or personnel security management).

Work in other areas has led to a clearer understanding of the complexity of the security workforce and its developmental requirements. In one project, a research team documented the numbers of security practitioners designated by position title and occupational code in each agency and whether these individuals were federal employees or support service staff. In another study, researchers looked at career path models that would, where adopted and supported by employing agencies, attract entry-level security practitioners to longer-term commitments. In addition, the lack of career path planning surfaced as a major deficiency.

Automated Continuing Evaluation Systems (ACES)

Finally, the Automated Continuing Evaluation Systems (ACES) program is developing procedures for linking databases across many government agencies as input into personnel security investigations. A recent report (Chandler, Timm, Massey, & Zimmerman, 2001) evaluated the utility and costs associated with data sources not currently being used in the background investigation process. Information was obtained from 11 government and commercial data sources. The study helps lay the foundation for advancing personnel security through the use of computerized databases.

Efforts to Reform Personnel Security Programs

The present federal personnel security system dates from Executive Order 10450 issued in 1953 by President Dwight D. Eisenhower. All subsequent policy on personnel security is built on this order, which itself was a reform of an earlier program put in place by the Truman administration. Faced with criticism about Communist infiltration of the government in 1947, President Truman addressed the loyalty of federal employees by issuing Executive Order 9835. This order required background investigations of applicants, with decisions to be made by loyalty boards within regional Civil Service Commissions. In the postwar and early Cold War years, concern was intensifying about American citizens helping the Soviets with information. Revelations about successful Soviet espionage raised public awareness about an internal threat based on ideological commitment or association with enemy organizations by federal employees with access to that information. Those concerns seemed to be confirmed when the Soviets exploded their atom bomb in 1947, thereby demonstrating that they had made good use of the atomic secrets stolen for them during the war by American and British spies.

The Truman loyalty program encountered problems because its loosely defined standards for decisions about a person's loyalty allowed agencies wide discretion to reach a variety of conclusions, and the program made no effort to include due process or appeal procedures. In part to remedy these failings, in 1953, Executive Order 10450, Security Requirements for Government Employees, rescinded Truman's program and laid down the basic elements of the personnel security system that have remained in place to the present, with some modifications. These elements included the following:

- Designation of heads of departments and agencies as responsible for establishing and maintaining systems within their organizations to ensure that employment decisions were consistent with national security.
- Mandate for a background investigation for every civilian employee or officer of government, the scope to be based on the potential harm a person in the particular position could inflict.
- Minimum standards for background investigations that included national agency checks, fingerprint checks, local agency checks, contact with former employers and schools, and references.
- The option to have the FBI perform a "full field investigation" beyond the baseline investigation should facts arise that warranted one; the option to reinvestigate and readjudicate people already in positions of trust in 1953 so that all employees would have been judged by the same security criteria.
- The definition of standards by which to judge whether a person's employment would be consistent with the interests of national security. These standards included the following:

- Behavior, activities, or associations that showed a person to be unreliable or disloyal.
- Lying or omissions of fact.
- Criminal or immoral conduct, including excessive alcohol use, drug use, or "sexual perversion."
- Illness, including mental illness.
- Vulnerability to coercion.
- Committing or conspiring to commit acts of treason, espionage, or sabotage.
- Maintaining association with spies, anarchists, or secret agents of foreign powers.
- Advocating the overthrow of the government by force, or associating with those who do so.
- Intentional disclosure of secret information or disregard for security requirements.
- Acting for the benefit of a foreign power.
- Refusal to testify about alleged disloyalty to a Congressional committee.

Lastly, Executive Order 10450 directed OPM to maintain a "security-investigations index" to track the background investigations performed on individuals across the government. This was an early effort to compile a database of security actions on individuals.

The demands of World War II had shaped many institutional approaches to personnel security that would be carried forward into subsequent decades. Each of the military services had developed programs to investigate and certify its own personnel for work with sensitive information. Defense contracting expanded dramatically in response to the war, and initially each military service vetted and certified its own contractors. To minimize the inevitable confusion, early in the war the Navy ceded to the Army all responsibility for handling aliens, control of subversives, fingerprinting, and military personnel security procedures. The office of the Army Provost Marshall General handled the wartime industrial security program, including security inspections of facilities, processing security questionnaires, and checking fingerprints. In an early step toward consolidation in 1948, an Army-Navy-Air Force Personnel Security Board assumed adjudicative authority over industrial contractors doing work for any of the three services. From 1949 through 1953, a section of the Munitions Board, the Industrial Security Division, analyzed the needs of the growing industrial sector. This Industrial Security Division framed the policies that became the initial combined federal industrial security program in June 1954.

During the mid-1950s through 1960, a series of DoD directives and executive orders gradually created a personnel security bureaucracy, in effect acknowledging that since the Cold War showed no signs of ending, for the first time security programs would have to become permanent features of the government. The Atomic Energy Act of 1946 had set up the Atomic Energy Commission to oversee nuclear development in the United States. In 1954, that act was amended to set up a restricted data classification system for nuclear materials, separate from and different than the classification system used for DoD information. The landmark Executive Order 10450 came out in 1953. In June, 1956, DoDD 5210.9 laid out the Military Personnel Security Program and specified that military and civilian personnel would henceforth take the same security oath. In 1960, President Kennedy issued Executive Order 10865 establishing uniform standards for access to classified materials by industrial employees; this was followed in 1965 with implementing policies in DoDD 5220.22, the Department of Defense Industrial Security Program, further revised in 1980. Finally in 1979, a major reorganization of 35 years of bureaucratic policy accretions came together in DoDD 5200.2-R, which combined all DoD personnel security programs and further regularized standards for access and due process policies that had been mandated by court decisions. This directive in turn became the basic policy document for subsequent fine-tuning of personnel security. Although revisions to DoDD 5200.2-R have been in the works for a decade, as of 2003 the revisions have not been issued as formally accepted DoD policy.

A rash of attempts at espionage by American citizens discussed in the press in the late 1970s and 1980s led to demands for personnel security reforms that could remedy what had became known as an espionage plague. Espionage by Americans seemed to increase during the 1980s, but this impression was in part caused by a change in federal policy on prosecution of espionage. Whereas before 1977 espionage was often quietly neutralized without prosecution in order to protect secrets from being revealed in open court, starting with Griffin Bell as Attorney General in the Carter administration, public prosecution for spies became the norm. Legislation to safeguard secrets in open court, including the Federal Information Surveillance Act (FISA) of 1978 and the Classified Information Procedures Act (CIPA) of 1980, created procedures to protect sensitive information and thus made this policy possible.

Responding to the serious damage inflicted by the Walker espionage conspiracy, major recommendations for personnel security reform came from the 1985 DoD Security Review Commission under General Richard Stilwell, Ret. The Stilwell Commission report (Department of Defense Security Review Commission, 1985), found that far too many security clearances were routinely issued, and it called for their numbers to be reduced immediately. It also suggested requiring specific justifications for all requests for clearances. DoD did reduce the number of its clearances over the next 5 years by more than one third, from roughly 4 million to less than 2.5 million. Other Stilwell Commission recommendations included:

- Creating a billet control system to ensure that Top Secret clearances were associated with a position, not an individual.
- Authorizing short-term temporary access to higher-level information.
- Expanding the investigative scope of Secret clearance to include a credit check and written inquiries to past and present employers (the genesis of a NACLAC-Credit, with Inquiries investigation).
- Encouraging more behavioral science research on personnel security procedures (PERSEREC was established in 1986 to perform this function).

- Plans for reducing the then-sizeable backlog in Top Secret and Sensitive Compartmental Information (SCI) accesses.
- Developing standardized mandatory training for adjudicators. Subsequent reform commissions would revisit many of these themes.

Working with these and other recommendations, the bureaucracy eventually formulated several major changes to the personnel security system in the early 1990s. National Security Directive 63, issued in 1991, established single-scope investigative standards for access to Top Secret and Sensitive Compartmented Information across the federal government. President Clinton issued Executive Order 12829 in 1993 that created the National Industrial Security Program, consolidating existing industrial security programs and regulations into a more coherent whole. As a result of a study (Crawford, Riedel & Carney, 1991) of issues in centralizing adjudications into one agency, the 18 facilities in DoD were combined into eight central adjudication facilities (CAFs) in 1993. The DCI issued a revision of DCI Directive 1/14 (it became DCID 6/4) in 1994 that provided uniform adjudication standards for access to SCI information. The tendency of these and similar changes during the 1990s was toward greater uniformity of standards and more consistency of policies across not just the DoD, the largest user of classified information, but across the entire federal government.

The Secretary of Defense and the DCI prompted a major reform effort in 1993 in creating the Joint Security Commission. This wide-ranging investigation found that many of the problems identified by the Stilwell Commission 7 years earlier still persisted. Needless clearances were requested only for access to areas of facilities; too many clearances were being requested; there was no standardization of forms, procedures, and standards; procedures took too long; and few agencies used available automated capabilities for databases and information processing. The commission's report (Joint Security Commission, 1994) listed many recommendations for change, some of which were adopted, including creating a standardized electronic personnel security questionnaire, changing the investigative scope for SCI access to include an SSBI with a-periodic reinvestigation in not less than 7 years, limiting investigators to neighborhood checks of the most recent residence within 6 months, and establishing a new central database to include conditions and waivers. Their recommendation to consolidate all DoD adjudication facilities into a single CAF (excluding only the National Security Agency) was not implemented.

In March 1995, the GAO issued a report on whether investigative and adjudicative facilities across the federal government should be consolidated (General Accounting Office, 1995). The GAO projected that benefits from such a move would probably include cost saving, simpler oversight, standard operating procedures and information systems, and more consistent application of standards. But in the end, the GAO did not recommend such a consolidation. They found that the loss of control over the process by the various agencies and departments would potentially reduce the system's ability to effectively supply requirements among the disparate organizations. One-size-fits-all did not seem the best way to approach personnel security, despite a perennial longing by the bureaucracy for consistency and standardization.

In a parallel initiative by Congress, the Commission on Protecting and Reducing Government Secrecy was created in April 1994 and asked to study secrecy across the Government, to include identifying its nexus with personnel security. Senator Daniel Patrick Moynihan chaired the commission and lent it his name.

While the Moynihan Commission was still researching, in 1994, the public learned of the long-term espionage by CIA case officer Aldrich Ames. Outrage over the revelations prompted a detailed study of that case for Congress, demands that annual financial disclosure forms be added to the security clearance requirements for certain positions, and calls for yet further realignment of the personnel security program. In 1994, President Clinton created the Security Policy Board to serve as an ongoing interagency body to frame and promote government-wide security policies. Congress also at that time amended the National Security Act to allow the President authority to establish uniform procedures across the Executive Branch for access to classified information. These changes resulted in Executive Order 12968, Access to Classified Information, issued in August 1995 and implemented in DoD in 1997. The order established uniform investigative and adjudicative standards for all U.S. military and civilian personnel, consultants, contractors, and anyone else who requires access to classified information. The goal in the mid-1990s was reciprocity across agencies, in which a background investigation and adjudication decision would be accepted for access in other agencies. This order mandated reciprocity, although the intelligence agencies only accepted it with reservations.

The Moynihan Commission's report came out in March 1997 (Commission on Protecting and Reducing Government Secrecy, 1997). In its chapter on personnel security, it applauded the recent Executive Order 12968 and reiterated the principles the commission felt that order advanced: open and clear standards for granting clearances; a balanced, whole-person approach that considered both positive and negative factors; reciprocity; nondiscrimination; and uniform procedures for due process for applicants. The commission criticized the decision to issue the executive order without rescinding any of the earlier directives, thereby adding another layer onto an already thick pile of overlapping, partly contradictory policies. The commission suggested that more research be done on security procedures and polygraph techniques, resources should be shifted from initial investigations to continuous monitoring of already cleared personnel, and streamlining the background investigation should be done. Many of the commission's recommendations, such as creating automated programs that could scan databases, financial, and travel records, are still being developed.

A series of audits and surveys of progress in implementing these reforms appeared in the late 1990s. A DoD Inspector General (DoDIG)'s report (DoDIG, 1997) looked at efforts to increase automation and information-sharing technologies in the investigative and adjudication agencies. The Defense Investigative Service (DIS), soon to become the DSS, had been developing and was then just adopting their Case Control Management System (CCMS). DIS' management hoped that CCMS would eliminate manual processing, automate functions such as code assignment and generating leads, and generally improve the quality and timeliness of DIS background investigations. The DoDIG sounded upbeat in its evaluation of the progress and potential of these reforms then underway.

A year later, however, in an April 1998 audit, the DoDIG was less sanguine about progress at the DoD CAFs (DoDIG, 1998). It found that the CAFs were neither consistent nor timely in their current procedures, and recommended reforms no matter whether the CAFs were consolidated into one body or left as eight separate entities. DoDIG recommended more standardization of forms, a peer review system for adjudicators, more training, and the ongoing development of the Joint Personnel Adjudication System (JPAS), which promised to improve communication and information-sharing among CAFs.

The Joint Security Commission reconvened 5 years after its first work in 1994 to evaluate progress in light of the accelerating revolution in electronic data systems and networks. Its report (Joint Security Commission, 1999) found some progress had been made toward reciprocity, but questioned the continuing disagreements over the value of neighborhood checks in investigations and the reporting of financial data. It urged research into these areas that, in part, prompted a program of research undertaken at PERSEREC to evaluate the productivity of various sources of information in background investigations. This research in turn led to the recommendation in 2001 to move to a phased PR.

Reform of the personnel security system seemed to hit a low point in October 1999, according to a critical GAO report (Government Accounting Office, 1999). The GAO evaluated background investigations being performed at DSS and that found 92% of them lacked information from one or more of the nine areas mandated by Executive Order 12968. Even worse, these inadequate investigations were taking much longer, since the changeover to the automated CCMS had been premature and resulted in a processing breakdown that lasted for some months. A large backlog in reinvestigations was building up. Federal policy required a reinvestigation of Top Secret/SCI clearances every 5 years, Secret clearances every 10 years, and Confidential clearances every 15. Because there had been a moratorium at DIS on receiving requests for any reinvestigations for several years, the backlog was mounting. A combination of newly relaxed standards and uncertainty about standards, elimination of quality control mechanisms in an effort to streamline the work, the unsuccessful implementation of CCMS, and a failure to train staff in the recent federal policies on investigations, all contributed to the problems at DoD's investigative service. A year later there was another GAO report saying that problems were being addressed (Government Accounting Office, 2000).

The backlog in reinvestigations provided the focus for a series of studies in the next 3 years trying to understand the situation and to efficiently turn it around. TRW evaluated CCMS in 1999 and found that the automated system was not a viable long-term solution. A year later TRW issued a progress report (TRW, 2000). It recommended replacing CCMS with an information system developed under a procurement office more experienced with information system acquisitions. In November 1999, the Deputy

Secretary of Defense created an Overarching Integrated Process Team (OIPT). The OIPT surveyed DoD agencies and contractors and estimated in its report that there was a backlog of 505,786 DoD reinvestigations (Personnel Security Investigations Process Review Team, 2000a). This became the figure used in later planning. The OIPT recommended outsourcing all Secret and Confidential investigations to OPM. The Office of the Secretary of Defense (OSD) had already begun diverting categories of investigations from DSS to OPM in October 1999 in an effort to allow DSS to finish implementing its automated system and return to normal operation. Both DSS and OPM began to contract with various private companies for background investigations, becoming supervisory contract offices themselves as well as continuing to provide investigations. The Office of the Assistant Secretary of Defense (C3I) (OASD [C3I]) became a broker of investigations between DSS and OPM for several years, shifting the distribution of types and numbers between the agencies, trying to maximize efficiency, and encourage DSS back to organizational health.

A DoDIG report (DoDIG, 2000a) provided details of what was becoming a CCMS debacle, the lagging investigation rate at DSS, the growing backlog of reinvestigations, and the contracting out to OPM and other private companies undertaken for FY00 and FY01. This report noted that there was no way to prioritize requirements for security clearances, and suggested that a team be formed to frame criteria for determining the highest priority missions and positions within those missions, and a way to relate requests for individual clearances to those priority positions. The Stilwell Commission in 1985 had described this need for a nexus between the security definition of a position and the individual who filled it, but the problem has proved to be subtle and complicated and not easily overcome.

Furthermore, in 2000, auditors released a group of studies demanding reform of the personnel security program. In April 2000, a group researching the insider threat in DoD published findings that included 60 recommendations to reduce the likelihood that insiders would compromise information security (Department of Defense Insider Threat Integrated Process Team, 2000). In May, the DoDIG issued an audit on the absence in DoD of any means to actually track security clearance requests (DoDIG, 2000a). It portrayed DSS in disarray; the agency seemed unable to tell how many cases were currently open or to project when a case would be done. The DoDIG's office recommended that DSS track each case from the time it was received and develop means to give progress reports to requestors. In June, the Under Secretary of Defense (Comptroller) reported on the backlog in a document that became known as the Spend Plan (Department of Defense, Under Secretary of Defense [Comptroller], 2000). This targeted September 2002, as the date for elimination of the backlog, set monthly targets for DoD components submitting requests, and divided types of investigations between DSS and OPM. In August 2002, the GAO weighed in with a report that criticized the estimating methods used to determine the size of the reinvestigations backlog (GAO, 2000). In October 2000, the DoDIG audited DoD adjudication facilities in anticipation that the backlog of cases would be moving from the investigators to the adjudicators (DoDIG, 2000b). The IG found that there would not be enough trained adjudicators to handle the coming rush, and it urged the OASD (C3I) to devote more resources to personnel security management.

The Secretary of Defense was required to report the personnel security investigations program including the adjudicative process as a material weakness under the Federal Managers' Financial Integrity Act, presumably to ensure that needed oversight was provided to effectively manage and monitor the personnel security process. This reporting requirement is still in effect as of November 2003.

Two important studies appeared in October 2000, from a group chartered by the Deputy Secretary of Defense, the Personnel Security Investigations Process Review Team (PRT). The first report assessed in May DoD's plans for eliminating the backlog and set stern milestones that clearance requestors, DSS, OPM, the CAFs, and the Assistant Secretary of Defense (C3I) "must" meet in order for the backlog to be whittled down on schedule (Personnel Security Investigations Process Review Team, 2000a). The second PRT report surveyed all major studies over the previous 15 years in a helpful compilation that documented recommendations made, those that had been implemented and those not implemented, and those in progress (Personnel Security Investigations Process Review Team, 2000b). The PRT made the point that further study of the personnel security system was hardly necessary since the problems and range of solutions already could be clearly described. Resources, management skill and determination, the will among agencies to cooperate with one another and to endure disruptive change to reach improvement—these underlying elements would be necessary to see progress in making reforms.

In February, 2001, a report from the OASD(C3I), Security Directorate, pulled no punches in its criticism of DSS' lack of progress against the backlog (ASD[C3I], 2001). The report presented statistics to argue that investigations were taking longer than ever and, at the current rate, the backlog was not going to disappear by the end of 2002 as mandated. The authors believed the situation threatened military readiness by preventing cleared personnel from taking their positions in a timely way. They proposed various specific changes to processing investigations and suggested how best to divide investigations between agencies doing them.

A May 2001 memo from General Charles Cunningham, Jr. (Ret.), Director of DSS, reminded his critics about aspects of the personnel security process over which DSS had no control. The military services, as the main requestors of background investigations for security clearances, had inadequate budgeting mechanisms that passed "sine wave funding" along to DSS. Far too many electronic personnel security questionnaires came in with errors or incomplete parts, forcing DSS to return them for revisions, sometimes repeatedly. The national standards for investigations, as set out in Executive Order 12968 in 1995, proved ambiguous when operationalized in the field, and this led to the follow-up of unproductive leads and a consequent decline in investigators' morale. Local law enforcement agencies refused to cooperate with DSS' security records requests, delaying cases or not responding to them at all, and charging high prices for responses. DSS had no authority to conduct investigations of overseas leads and so was forced to rely on personnel from other agencies stationed abroad. Also if these investigators performed the neighborhood surveys required by the standards, DSS would "literally be telling the foreign Government and foreign citizens that a U.S. citizen is undergoing an investigation for a security clearance"—and the counterintelligence issues this generated were incalculable. This memo offered a valuable corrective from those charged with actually putting into practice the advice and criticism.

In addition, a draft report in May 2001, from the Assistant Secretary of Defense (C3I) Integrated Process Team on the optimal mix for dividing types of background investigations between DSS, OPM, and private contractors summarized the vectoring of cases between agencies and the timing for eliminating the persistent backlog (Personnel Security Investigations Process Review Team, 2002). The report urged DSS to move to fee-for-service budgeting as soon as practicable and weighed the impact of the phased PR on workload decisions, since at least one year of notice is needed for budget decisions. The team wrote that a "new paradigm that encompasses the end-to-end process including the requirements for investigations and continuing evaluations, investigations, adjudications, and information technology will be needed." This reflected recommendations outlined in a concurrent research project that was published the following year, (Lang & Herbig, 2002) which proposed concrete structures to achieve such a paradigm for the next round of reforms to the personnel security system.

Finally, in February of 2003, DoD proposed to move and consolidate PSI functions and associated DSS employees under OPM. OPM, in turn, uses the United States Investigations Services (USIS) and other contractors to meet the majority of its PSI requirements. If approved by Congress in FY04, DoD and OPM expect that the consolidation will benefit DoD through greater PSI procedural standardization, use of a single PSI computer processing system, and reduced costs. Although DoD oversight responsibility will shift more toward contract monitoring, the overall challenge will remain: how to assess and ensure that PSI policies and operations are adequately serving personnel security goals and objectives.

Appendix B

Indirect Benefits of Personnel Security Programs

Indirect Benefits of Personnel Security Programs

In addition to direct benefits to national security, federal personnel security programs may yield important indirect benefits, such as reducing substance abuse, lowering crime, reducing attrition, and improving morale. Although indirect benefits may fall outside the stated goal of a program, such outcomes may be significant in evaluating the program's overall utility.

This appendix discusses several types of evidence that might be used to evaluate whether personnel security programs have such indirect benefits. The studies discussed generally use one of two types of outcome measures: (1) monetary estimates of program/procedure benefit, or (2) validity estimates that document the degree of relationship between a program/procedure and outcome measures. Although no systematic, quantitative studies were located that evaluated the full benefits of the federal government's personnel security programs, dozens of studies were found that speak to the issue of indirect benefits.

Limitations of the Studies

Most of the studies discussed in this appendix employed a research focus or methods that limit their generality to the federal personnel security context. First, many of these studies used forms that are different from (but conceptually related to) the forms used in personnel security programs for the federal government. For example, several studies used integrity tests, which are questionnaires designed to obtain information about counterproductive behavior or attitudes. Second, most of the studies utilized a single security procedure, rather than the full set of procedures used in the federal personnel security program. Third, some studies included physical security measures as well as personnel security measures. Thus, the independent effects of the personnel security measure are not known. As a result of these limitations, the findings in this section must be considered suggestive, rather than definitive.

The literature review below is organized into three sections: (1) Background Screening Studies, (2) Continuing Evaluation Studies, and (3) Other Evidence. These are followed by (4) Security Education and a brief discussion of its indirect benefits.

Background Screening Studies

Most organizations use some form of prescreening to screen out applicants who would not meet the adjudicative guideline standards. While prescreening procedures vary across organizations, most involve a review of the individual's personnel security questionnaire and interviews with the applicant (Bosshardt, 2000).

Background screening may indirectly benefit an organization in two ways: (1) increasing productivity or job performance and (2) reducing counterproductivity or negative work behaviors.

Gains in Productivity or Job Performance

Studies of the economic gains in productivity from employment hiring procedures suggest that hiring procedures have significant monetary benefits. For example, a review of 16 employment interview studies found that all showed positive economic benefits (Boudreau, 1991). Other research found that background questionnaires have substantial economic benefits when used for preemployment hiring (Lee & Booth, 1974; Schmidt & Hoffman, 1973).

Meta-analyses studies of the validity of employment selection procedures as predictors of job performance have consistently shown positive results. In their review of meta-analysis findings for employment hiring methods, Schmidt and Hunter (1998) reported mean corrected validities of .38 for unstructured interviews, .35 for biographical data measures, .26 for reference checks, and .41 for integrity tests for the criterion of overall job performance.

Can significant productivity gains be expected from the DoD personnel security program? Although no studies were located that directly addressed this question, two factors suggest that productivity gains from personnel security will be more modest than those realized from general employment screening. First, personnel security screening involves the incremental gains beyond those realized from general employment screening. Since many employment screening procedures also measure security screening content to some extent, the potential benefit from personnel security screening is reduced. A second limiting factor is that the economic benefits of screening procedures are substantially reduced when organizations are less selective. However, even in situations where most applicants are selected (as in personnel security screening), valid screening may have a positive monetary impact (Schmidt, Mack, & Hunter, 1984).

Reductions in Counterproductive Behavior

An effective personnel security program is also likely to reduce counterproductive behavior (Defense Personnel Security Research Center, 1998). Counterproductive behavior refers to employee actions or misconduct that negatively impact an organization (e.g., crime, violence, accidents, turnover, absenteeism, loss or compromise of classified or proprietary information). The following list includes several possible counterproductivity activities:

Absenteeism
Accidents
Aggression (e.g., sexual harassment, verbal abuse, endangering coworkers)
Alcohol use
Complaints/grievances
Credibility damage (i.e., damage to the organization's reputation)
Crime (work-related and nonwork-related)
Disclosure of classified or sensitive information (unintentional and intentional)
Disciplinary problems

Downtime
Drug use
Embezzlement
Espionage
Fraud
Financial irresponsibility
Health care costs
Insurance premiums
Job dissatisfaction
Lawsuits
Leaks to the press
Loss of life
Morale
Political deviance (e.g., showing favoritism, gossiping about coworkers, blaming coworkers, competing nonbeneficially)
Sabotage
Safety
Security infractions
Tardiness
Theft
Turnover
Vandalism
Workers' compensation claims
Workplace violence

Studies that examined the impact of security-related screening procedures on various counterproductive behaviors/outcomes are briefly summarized below:

Counter-Productivity (In General)

- Ones, Viswesvaran, and Schmidt (1993) found that when used for entry-level hiring, integrity tests had a mean corrected validity of .58 (255 correlations) for predicting admissions of counter-productivity.

- Ones, Viswesvaran, and Schmidt (1993) found that when used for entry-level hiring, integrity tests had a mean corrected validity of .32 (187 correlations) for predicting externally measured counter-productivity.

Unsuitability Discharges

- A 1966 Air Force study (described in Flyer, 1986) found that background investigations predict unsuitability discharges. Comparisons between a control group and approximately 12,000 Air Force enlistees whose background investigations had derogatory information found significant relationships between derogatory background information identified in background investigations and later attrition. Also, those with more serious derogatory background information were more likely to be later discharged for unsuitability.

- Crawford and Wiskoff (1988) compared the unsuitability discharge rates for military personnel who had and had not undergone security-related prescreening. They found that unsuitability discharge rates were consistently lower for prescreened groups (range: 5.8 percent to 19.2 percent) than for the groups who had not undergone prescreening (range: 13.4 percent to 21.2 percent).[27]

- McDaniel (1989) reported a combination of background inventory scales that measured areas covered in DoD background investigations (e.g., drug use, employment experience) had a modest correlation with unsuitability discharges for military applicants.

Turnover

- Popeyes Famous Fried Chicken and Biscuits introduced background checks for managerial and hourly workers in 1995 as a means of reducing employee turnover (Kapner, 1996). As a result, manager turnover decreased 15 percent and crew turnover decreased 20 percent.

- Schmitt, Gooding, Noe, and Kirsch (1984) reported that biodata measures had a mean uncorrected validity of .21 (28 coefficients) for predicting turnover.

- Hunter and Hunter (1984) reported that reference checks had a mean corrected validity of .27 (2 coefficients) for predicting tenure.

Absenteeism

- Hart and Cooley, a furniture manufacturer, introduced background checks as a means of reducing employee absenteeism (Harowitz & Hargreaves, 1997). They found that the absentee rate for the screened employees was one percent (vs. the plant average of 3.5 percent). Given the size of the company (2,000 employees) and an average absenteeism cost of $75 per day, the estimated dollar savings was $375,000 (2000 employees x 2.5 days per employee x $75) minus program costs (which were not specified).

- Helm and Associates (1985) reported that integrity test scores predicted absenteeism and sick leave.

[27] It should be noted that in military settings recruits who are screened out of security-related occupations are usually placed into other (nonsecurity-related) occupations. Thus, while personnel security screening may reduce counterproductive behavior within security-related occupations, it may not significantly reduce the organization's overall counter-productivity if these recruits are retained in other occupations within the organization. The author thanks Kent Crawford at PERSEREC for pointing this out.

- Hough (1986) reported that biodata measures had median validities of .25 (15 studies) for predicting absenteeism and turnover, .26 (one study) for predicting absenteeism and substance abuse, .20 (three studies) for predicting absenteeism and delinquency, and .27 (one study) for predicting absenteeism and unfavorable military discharges.

Theft

- In the mid-1990s, Kroger Company initiated background checks and drug screening for job applicants in their Nashville stores due to a large increase in employee theft (Longmore-Etheridge, 1999). As a result, approximately 15 percent of the applicants did not report for drug screening, and of those who did report, about four percent failed drug screening and another four percent failed the background check. More importantly, the changes reduced internal cash theft by 65 to 70 percent.

- Jones, Slora, and Boye (1990) reported that the estimated monetary losses from theft in supermarkets were about half as large as for companies that used integrity tests than for companies that did not use such tests.

- In a meta-analysis study, Ones, Viswesvaan, and Schmidt (1993) reported that integrity tests had a mean corrected validity of .36 (152 correlations) for predicting theft.

- Barke, Gerstein, and Johnson (1987) reported evaluations from a short, prerecorded telephone employment interview (called the Integrity Interview) had modest correlations with subsequent employee theft.

Substance Abuse

- Barge and Hough (1983) reported that biodata had a correlation of .26 with a substance abuse measure.

Worker's Compensation Claims

- Winans and Cairns (1996) discussed how background checking can reduce workers' compensation claims. Using data from the National Council on Compensation Insurance, Inc., which showed that the average lost time claim exceeds $17,000, and that a state record search typically costs less than $12, they computed the return on investment for background checks under three scenarios. Assuming that approximately 10 percent of the applicants with negative background information are rejected, they estimated that the return on investment from implementing background checks would range from 4-to-1 (assuming an average workers' compensation claim cost of $5000) to 28-to-1 (assuming an average claim cost of $17,000) to 62-to-1 (assuming an average claim cost of $25,000).

Accidents

- Jones and Wuebker (1988) reported that integrity testing may predict future accidents.

Insurance Loss

- Regarding credit checks, the Insurance Information Institute (2000) noted a study by an actuarial consulting firm that found a high correlation between credit rating and (personal) insurance loss potential.

Deterrence Effects

Deterrence, an informal means of discouraging potential applicants from applying for a position of trust, is a cost-effective strategy because it saves the costs of a formal background investigation and training for those who would have been denied clearances. It also reduces the likelihood of accepting high-risk individuals for positions of trust where they may exhibit security- or suitability-related problems.

- Background investigations may also deter less suitable applicants from applying for security-related occupations. Data from a preliminary study using the Automated Continuing Evaluation System (ACES) suggest that the personnel security program may have deterrence effects (Timm, 2001). Using a retrospective research design that involved the analysis of more than 11,000 OPM reinvestigation cases, Timm found that the percentage of employees who resigned prior to adjudication for their initial background investigation increased as the level of seriousness of their issues increased. For example, 4.2 percent of those with "very minor" resigned prior to adjudication, compared to 13.7 percent of those with "moderate" issues, and 25.0 percent of those with "major" issues.

- Flyer (1986) estimated that up to one third of Army and Air Force recruits either drop out or are disqualified before their formal background investigations are initiated. If one assumes that the individuals who are most likely to drop out of the clearance process are those with questionable backgrounds, the economic gains of prescreening may be significant.

Continuing Evaluation Studies

Do continuing evaluation programs have indirect benefits? Results from one study suggest that security awareness may contribute to reductions in convenience store robberies. Over the past 20 years, 7-Eleven stores have made many security-related changes, including having employees attend seminars on violence avoidance and robbery deterrence, as well as several other security measures (e.g., keeping a minimal amount of money in cash registers, locating cash registers in the front of stores to improve visibility, changing outside lighting to improve employees' view of the parking lot, installing video cameras, alarms, and CCTV in stores, installing fencing and landscaping to prevent easy escapes, providing work stations for police in stores, and having police provide store coupons to persons who perform random acts of kindness). The robbery rate at 7-Eleven stores has dropped by about 70 percent since the program was initiated in 1976 (Lins & Erickson, 1998).

Hardee's initiated a loss prevention program in 1990 (D'Addario, 1993) that included background checks on managers who had access to missing funds, interviews with managers who were involved with multiple losses about their access to data, use of tighter cash controls, use of disposable bank bags, and witnessed money counts. Two-and-one-half years after the program was introduced, the bottom-line profit was estimated at $1.5 million and return on investment for preventing losses exceeded two dollars for every one dollar spent.

Data from Timm's (2001) preliminary study of an Automated Continuing Evaluation System (ACES) suggests that the continuing evaluation program may have deterrence effects. Based on an analysis of more than 11,000 OPM reinvestigation cases, Timm found that the percentage of employees who resigned prior to adjudication for their periodic reinvestigation increased as the level of seriousness of their issues increased. The results indicated that 1.0 percent of those with "very minor" resigned prior to adjudication, compared to 5.7 percent of those with "moderate" issues, and 11.7 percent of those with "major" issues.

Other Evidence

Several researchers have documented the high costs of various suitability problems in the workplace (e.g., Cascio, 2000; Heuer, 1998). For example, consider alcohol abuse. Shahandeh (1985) reported that alcoholics at General Motors (vs. a control group) had 16 times more absences, two-and-a-half times as many absences of eight days or more, five times more compensation claims, three times as much sick leave, and more than three times as many accidents. Although no studies were located that documented the benefits of the personnel security program for alcohol abuse, Shahandeh's findings suggest that background screening procedures that reduce the number of substance abusers or continuing evaluation procedures that treat alcohol abusers at an early stage may produce significant economic benefits for user organizations.

Security Education

Personnel security programs typically are linked with efforts to educate and train individuals and their supervisors and coworkers about their responsibilities for safeguarding security-relevant information and for reporting security-relevant issues.

Effective security education and awareness procedures should produce several benefits. First, such procedures should reduce the number of unintentional disclosures of security-relevant information. Second, such procedures should identify individuals who are experiencing personal problems at an earlier stage, reducing potential security- and suitability related issues. Third, such procedures should have deterrence effects.

Summary

This appendix examined several studies and related data to evaluate whether personnel security programs are likely to yield indirect benefits to national security, i.e., benefits beyond the stated program objectives. The studies that were examined related to background screening and continuing evaluation, along with other evidence. The indirect benefits of security education were also discussed. While the majority of the studies were not performed to specifically address the outcomes of federal personnel security programs, they do suggest that such programs are likely to yield many indirect benefits to national security.

Appendix C

Public Opinion and Support for Personnel Security Programs

Public Opinion and Support for Personnel Security Programs[28]

Introduction

Security policy is not developed in a vacuum. It exists within a social context. Ultimately, the people—through their elected representatives—must approve the kind of personnel security system that the government deploys and the kind of security measures it imposes.

With the end of the Cold War, counterespionage needs have become more complex. While traditional espionage challenges have not disappeared, both the intelligence community and the American people have had to adjust to broader and more varied threats in which many more players and many more issues affect national security. Our ability to meet these diverse challenges depends on the willingness of the American public to recognize these threats and to support adequate security measures to counter them.

PERSEREC Study of Public Attitudes to Personnel Security

The Defense Personnel Security Research Center (PERSEREC) undertook to assess the degree of public support for various national security issues.[29] PERSEREC collaborated with the National Opinion Research Center (NORC) at the University of Chicago to include questions on its 1994, 1996, 1998 and 2000 General Social Surveys (GSS). Questions were asked about the following issues:

1. Need for secrecy in various areas of government activity.
2. Government's need to collect information on individuals vs. people's privacy rights.
3. Public support for various security countermeasures.
4. Government's right to know mental health information.
5. Loyalty to employer vs. coworkers.
6. Punishments for various acts of trust betrayal.
7. Perception of threat to the United States.

Following is a table showing selected data from the PERSEREC/NORC study that relate directly to personnel security vetting issues.

[28] This Appendix draws on material prepared by Suzanne Wood (consultant to Northrop Grumman Mission Systems).

[29] Details may be found in Wood (2001).

Table C.1
Support for Specific Personnel Security Issues: Percentage of Respondent Agreement[a]

	1994	*1996*	*1998*	*2000*
	%	%	%	%
1. Government should have the right to ask questions about:				
Financial and credit history	82	79	74	77
Criminal arrests & convictions	98	97	96	96
Illegal drug use	96	96	96	95
Mental health history	95	95	94	93
Foreign relatives & friends	78	79	77	77
Alcohol use	93	93	89	89
Sexual orientation	47	49	44	44
Foreign business contacts	-	-	-	87
Foreign travel	-	-	-	81
Illegal or unauthorized use of computers	-	-	-	93
2. Government should contact others to verify information:				
Financial assets and liabilities	-	76	71	-
Spouse's financial assets and liabilities	-	66	62	-
Tax records	-	76	70	-
3. Government has the right to know:				
Nothing about individual's emotional or mental health	-	6	5	6
Whether individual is currently consulting a mental health professional	-	12	12	10
Whether individual has ever consulted a mental health professional	-	8	10	10
Whether individual has ever consulted a mental health professional, and general nature of diagnosis	-	26	27	24
Whether individual has ever consulted a mental health professional, the general nature of diagnosis and counseling, and specific information revealed in confidence to the mental health professional	-	42	38	43
Don't know	-	5	8	7
4. People with security clearances should be subject to the following measures:				
Periodic lie detector tests	-	-	75	78
Random drug tests	-	-	91	88
Wiretapping or electronic surveillance	-	-	38	-
Regular questions about financial assets				

	1994	*1996*	*1998*	*2000*
	%	%	%	%
& liabilities	-	-	49	47
Monitoring at work	-	-	50	-
Monitoring off the job	-	-	43	-
Computer checks of personal financial records	-	-	-	43
Computer checks of international travel records	-	-	-	64
Auditing of e-mail and Internet use at work	-	-	-	64
Auditing of e-mail and Internet use at home	-	-	-	30
Wiretapping of telephone calls at work	-	-	-	45
Wiretapping of telephone calls at home	-	-	-	20
Searches of briefcases and desks at work	-	-	-	48
Video camera surveillance in workplace	-	-	-	64

a "Strongly agree" and "Agree" responses have been combined.

The first three questions relate to the public's views on how intrusive the government can be when conducting background checks on employees applying for security clearances. Question 1 regarded the government's right to ask questions about a series of personal issues. Here the data are relatively stable over the years, with only minor shifts in support. Question 2 concerns the government contacting others to verify information provided by the applicant. The question was only asked in 1996 and 1998 and there were only slight changes between the responses in those two years: relatively strong support for checking a person's own finances and tax records; less for checking the spouses. Question 3 concerned the government's right to ask questions about emotional or mental health. Asked during three GSS rounds, the data are stable. In this case public approval appears to outrun security policy itself, in approving extensive investigation into mental health histories.

Question 4 relates to the public's opinion of the use of security countermeasures that might be applied to an employee once a clearance has been granted. Lie detectors and random drug tests are highly approved. Monitoring at the workplace is tolerated. But few approve of wiretapping of home telephone calls or auditing of home e-mail and Internet use, strategies that the public feels are too intrusive and an invasion of privacy.

Other data in the study (tables not shown here) suggest that between 1994 and 2000 the public was relatively consistent in its pro-security stance, with only minor shifts in support in recent years in certain areas. When given the choice of backing the government or protecting the personal freedoms of people with security clearances, the public leans towards the government. Also, asking questions about people's relatives and friends is not wholly supported, even though this is an area deemed by government investigators an important source of information on the person being vetted. The public believes that far too much information is being classified.

What We Do Not Know About Public Opinion

Since the general findings from the GSS have been relatively stable over the past several years, PERSEREC decided to defer gathering more data, at least for the next few years. Consequently, no recent or 9/11-related GSS data have been gathered on: (1) the government's need for secrecy, (2) the government's right to probe into personal matters when conducting background investigations on people applying for clearances, (3) the government's right to contact other people to verify information provided by the applicant concerning the person's tax records, personal finances and those of his/her spouse, (4) the government's right to know about the mental health of the person being vetted, (5) loyalty to one's employer vs. loyalty to a coworker, (6) the public's views of selected security measures that government might apply to individuals already holding clearances, (7) whether certain kinds of people, such as government computer network administrators, airlines screeners, etc., should undergo the same type of investigation as someone being investigated for a security clearance, (8) whether people believe that government should assume equal loyalty among all U.S. citizens, native born or naturalized, (9) the public's perception of the threat compared to 10 years ago (the response to a similar question in 2000 was an overwhelming belief—prophetic in nature—that the most serious threat now would come from terrorism by foreigners), and (10) the public's opinion on a variety of security issues, such as requiring U.S. citizens to carry an identification card, restricting foreign travel, conducting surveillance of scientific laboratories that conduct research on biological materials, and monitoring personal telephone and e-mails at home.

As for other materials regarding the public's opinion on personnel security, The American Enterprise Institute (2003) has published a report that touches on three matters indirectly related to personnel security: trust in the government, civil liberties after 9/11, and the question of whether we are safer now than before.[30] Another study, by the U.S. Merit Systems Protection Board (1993), dealt with a subject included in the 1994 GSS survey, that of coworker reporting. The board asked government employees if they had observed serious fraud, waste, or abuse behaviors in the workplace in the last 12 months and, if so, whether they had reported them. The study also examined why employees reported (or did not report), what they saw, and what happened after they reported the activity. Nothing was asked in this study about clearances or security positions. Yet the responses indicate that the public—in this case uncleared government workers—is interested in workplace ethics and the issue of loyalty to friends or coworkers vs. loyalty to the larger organization.

Summary

Taken together, the results of public opinion surveys and studies show consistent support, over time, for strong security, the need to balance personal privacy against national security, and for the goals and procedures of federal personnel security programs.

[30] See www.aei.org/docLib/20031002_Terror03.pdf.

Appendix D

Summaries and Recommendations From *An Assessment of the DoD Personnel Security Program: A Report to the Deputy Secretary of Defense*

Summaries and Recommendations From *An Assessment of the DoD Personnel Security Program: A Report to the Deputy Secretary of Defense*[31]

Summary and Status of Previous Recommendations to Reform the PSI Process, 1985-2000

The following tables summarize the recommendations made since 1985 by CODA (1999); DoD Inspector General (1997, 1998, 2000a, 2000b, 2000c), General Accounting Office (1995, 1999, 2000); DoD Insider Threat IPT (2000); Joint Security Commission (1994); Joint Security Commission II (1999); Commission on Protecting and Reducing Government Secrecy (1997); Personnel Security Overarching Integrated Process Team (2000); DoD Security Review Commission (1985); and TRW (1999).

Table D.1 Summary and Status of Stilwell Commission Recommendations

Recommendations	**Status**
Create a TS billet control system to ensure that TS clearances go with a position, not an individual.	No action
Require specific justification for requests for security clearances; prohibit requests solely for movement within a controlled area whenever exposure to classified information/technology can be prohibited.	Implemented
Authorize, subject to strict control, one-time, short-term duration access to specific information at the next higher level of classification to meet operation exigencies.	Implemented
Expansion of the investigative scope for a Secret clearance to include a credit check and written inquiries to past and present employers.	Implemented
Intensification of behavioral science research to improve the background investigation process and the effectiveness of subject interviews.	Action Being Taken (ABT)
Reduction of the backlog for TS/SCI accesses to 4 years and the development of a plan for eliminating the PR backlog by 1995.	Superseded
Conduct necessary research and other actions to develop more precise and effective adjudication standards.	ABT
Develop and conduct standardized mandatory training of all adjudicators	Implemented

[31] Excerpted from a report: “Personnel Security Investigations Process Review Team” (2000a, October).

Table D.2 Summary and Status of JSC I Recommendations

Recommendations	Status
Request clearances only for personnel who require actual access to classified information or technology.	Superseded
Require a NAC to determine suitability for facility access.	Superseded
Find a solution that will impose discipline at the requester level, while insuring the system accommodates essential clearance requests quickly and efficiently.	ABT
Institute a fee-for-service mechanism be instituted to fund the PSI process.	ABT
Formal prescreening of contractor personnel by government or an independent company hired by the government, not the company employing the personnel.	Implemented
No pre-screening without individual's knowledge or consent	Implemented
Adoption of the PSQ developed by the NISP	Superseded
Development of a standardized electronic personnel security questionnaire	Implemented
Development of a standardized prescreening form	ABT
Increased investment in automation to increase timeliness and improve efficiency of the PSI process and reduce costs.	Implemented
Change investigative standard for SCI access to an SSBI with a scope of 7 yrs.	Implemented
Investigators should not be required to conduct education and birth record checks in person	Implemented
Investigators should not be required to conduct neighborhood checks other than the most recent residence of six months or more.	Implemented
Change investigative standard for a Secret clearance to NAC with written inquiries (NACI) plus credit check with expansion of the investigation only if needed to collect information required to resolve issue in adjudication.	Superseded
Change investigation standard for a SCI to an SSBI, with PRs conducted on an aperiodic basis, but not less than once every seven years.	Implemented
Change investigative standard for a Secret clearance to a NACLAC and a credit check, with PRs on an aperiodic basis, but not less than once every 10 years.	Implemented
Establish Employee Assistance Programs (EAP) and ensure that similar programs or contractual services are available to employees, particularly those with access to specially protected information.	Implemented
All investigative, adjudicative, and appellate organizations begin an orchestrated process improvement program with the goal of continuing to ensure fairness and quality while improving timeliness.	Implemented
Establish measurable standards to access timeliness and quality of investigative and adjudicative processes.	ABT
As long as an individual has been investigated within the last 10 years, that an interim clearance may be maintained at the previous level of access based on a favorable review of the PSQ.	Superseded
Consolidate adjudication facilities, except NSA, into a single CAF.	No action
No further access determination for individuals with an existing clearance .	Implemented
Limit program managers to the following access determination prerogatives: verifying the requisite clearance and ensuring need to know	Implemented
Identify conditions and waivers using standard codes in a new central data base.	ABT

Table D.3 Summary and Status of Moynihan Commission Recommendations

Recommendations	Status
Openness and clarity of standards to ensure that all applicants are subject to government review clearly and in writing about the security vetting process	Implemented
Base investigation and adjudication on balanced "whole person" concept.	Implemented
Use of nondiscriminatory principles, denials and revocations of access should not be based on arbitrary or capricious standards	Implemented
Assurances of due process-applicants and employees should be immediately informed in writing of the reasons for suspension, denials, or revocations and given the opportunity to appeal an adverse determination.	Implemented
To facilitate reciprocity, employee's clearance should be accepted when equivalent or higher than that required by the new agency or position, and previous investigation was conducted within the established timeframe.	Implemented
Increase clearance reciprocity across government and industry (except for polygraph requirement).	Implemented
Achieve greater balance between the initial clearance process and programs for continuing evaluation of cleared employees.	ABT
Focus resources on those "at-risk" individuals in the most sensitive positions	ABT
Strengthen EAPs.	Implemented
Those holding the most sensitive positions could be subjected to more frequent in house reviews, thus saving resources directed toward the traditional field investigation.	ABT
Assess the value of financial disclosure.	Implemented
Eliminate the requirement for neighborhood interviews and educational references in every investigation.	Superseded
Target security clearance resources toward the most productive elements of the investigation, those that yield the most substantial information relevant to the clearance.	ABT
Conduct a cost-benefit assessment prior to utilizing automated sources of information.	ABT
Reevaluate the requirement to utilize a new financial disclosure form and consider staying its implementation until there is further evaluation concerning how it would be used and whether its benefits exceed its cost.	ABT
Review alternative approaches to improving data collection, including utilization of the expanded access to certain financial and travel records.	ABT
Make clearance process more efficient through automation.	ABT
Create computer programs that are capable of continually scanning different databases.	ABT
Develop an automated personnel security program.	ABT
Conduct more and advanced research on the accuracy of the polygraph.	ABT
Reduce inefficiencies in the adjudication process.	ABT
Establish a fast track adjudicative procedure with an emphasis on completing clean cases first and eliminate multiple adjudicative review.	ABT

Table D.4 Summary and Status DoDIG Recommendations for CAFs

Recommendations	Status
Implementation of peer review program within the DoD adjudication process.	ABT
Establish continuing education standards and a program to encourage the development and certification of professional adjudicators.	ABT
Require each CAF to show a clearance code rather than a facility-specific clearance code in the DCII.	Implemented
Arrange for a copy of an individual's investigation report to be provided with a letter of intent to deny or revoke a clearance.	Implemented
Standardize the request and report forms that customers must use for personnel security actions.	Implemented

Table D.5 TRW Recommendations for CCMS

Recommendations	Status
Provide sufficient funding to maintain, enhance or replace CCMS.	ABT
Establish experienced program management office (PMO) to assure success in sustaining CCMS and developing a replacement capability.	Implemented

Table D.6 JSC II Recommendations

Recommendations	Status
The Security Policy Board (SPB) should commission and fund a research to determine the efficacy of existing PSI policies and resolve issues about their effectiveness; SPB should monitor this effort, ensuring the proper assessment of its results, and use those results to develop appropriate policies.	ABT
DoD should reassign SRC to OASD(C3I).	Implemented
DoD Polygraph Institute (DoDPI) should be renamed the National Polygraph Institute (NPI) with the SPB designated the National Manager.	No action
Designate OASD(C3I) the Executive Agent for DoDPI.	No action
The DoD should begin to fully enforce the standards for reinvestigations and then, within 90 days, should screen all overdue PRs, to identify those whose positions and access suggest the highest risk, and should provide the resources to complete those reinvestigations promptly.	ABT
Establish a limit of 180 days for new interim clearances, requiring the completion of the requisite backlog checks and adjudication process within that period.	ABT
Screen all existing interim clearances and promptly close out those where positions and access suggest the highest risk.	ABT
SPB should continue to support the ESP, ensuring continued development, funding, and eventual operational status.	ABT
The SPB propose a new executive order to the NSC that addresses the suitability, reliability, and trustworthiness of persons employed in sensitive duties. This would include individuals working in any capacity, and based upon the sensitivity of the duties, regardless of access to classified information, A proposal from the SPB for such an order is consistent with its stated mission in PDD-29.	ABT

Table D.7 GAO Recommendations for Improving PSI Quality and Timeliness

Recommendations	Status
SecDef to direct C3I to report the PSI program as a material weakness under the Federal Manager's Financial Integrity Act (FMFIA) to ensure that the needed oversight and actions are taken to correct systematic problems in the DSS PSI program.	Implemented
SecDef to instruct DSS Director, with oversight by C3I to develop a corrective plan as required by the FMFIA that incorporates corrective actions and milestones for addressing material weaknesses in the DSS PSI program performance measures for monitoring the progress of corrective actions.	Implemented
SecDef to instruct DSS Director, with oversight by C3I to establish a strategic plan that includes agency goals, performance measures, and procedures for tracking progress in meeting goals in accordance with sound management practices in the Government Performance and Results Act.	Implemented
SecDef to instruct DSS Director, with oversight by C3I, to develop an overall strategy and resource plan to improve the quality and timeliness of investigations and reduce the number of overdue investigations.	Implemented
SecDef to instruct DSS Director, with oversight by C3I, to establish a process for identifying and forwarding to the SPB suggested changes to policy guidance concerning the implementation of Federal standards and other investigative policy issues.	Implemented
SecDef to direct all DoD CAFs to regularly communicate with the DSS about continuing investigative weaknesses and needed corrective actions.	Implemented
SecDef to direct C3I to improve the oversight of the DSS PSI program, including approving a DSS strategic plan.	Implemented
SecDef to direct C3I to identify and prioritize overdue PRs, in coordination with other DoD components, and fund and implement initiatives to conduct PRs in a timely manner.	Implemented
SecDef to instruct DSS Director, with oversight by C3I to review and clarify all investigative policy guidance to ensure that investigations comply with national standards.	Implemented
Establish formal QC mechanisms to ensure that DSS or contract investigators perform high quality investigations, including periodic reviews of samples of completed investigations, and feedback on problems to senior managers, investigators, and trainers.	Implemented
Establish training infrastructure for basic and continuing investigator and case analyst training.	Implemented

Table D.8 CODA Recommendations

Recommendations	Status
Institute up-front screening processes to minimize the number of problematic cases that consume a disproportionately large amount of PSI resources.	No action
Use "likely disapproval" indicators to trigger suspension of clearance processing and decision on merits of continued processing.	No action
Evaluate PSI practices to manage people who have access to sensitive information.	Implemented
Create an environment in which people are more likely to report indications of life crises and security issues related to themselves and others.	Implemented
Make optimal use of electronic data collection.	ABT
Make integration of adjudication and case management an enterprise wide practice.	No action
Investigate automated tools for adjudicated scoring.	No action
Provide adjudicators access to a pool of expert consultants.	Implemented
Make clearance data universally accessible to PSI professionals.	ABT
Develop a common PSI information technology strategy to enhance communication and cooperation across the enterprise.	ABT
Replace CCMS with a system developed under the auspices of a strong, acquisition experienced program management office.	ABT
Make senior executives and program managers accountable for PSI performance.	ABT
Establish PSI as a distinct, professional, discipline.	Implemented
Institute an enterprise wide best practices migration program to ensure the transfer of good ideas.	ABT
Market PSI to Congress and senior executives.	ABT
Establish agreements of conduct that trigger termination if violated.	No action
Identify and share best practices to manage outsourced processes.	ABT
Institute an investments clearing house to facilitate enterprise partner communication of major planned or proposed PSI expenditures.	No action
Verify the nexus between psychological make-up and suitability.	ABT
Verify the nexus between personality type and counterintelligence risk.	ABT
Develop a common understanding of PSI performance by establishing common process performance measures.	ABT

Table D.9 DoD Personnel Security OIPT Recommendations

Recommendations	Status
Prioritize PRs based on reliability risk and positional risk; conduct random, aperiodic checks in the high risk applicants, using polygraph for very high risk personnel.	ABT
Review policy and procedures driving clearances.	ABT
Continue research on the Automated Continuing Evaluation System (ACES).	ABT
Standardize Interagency User Friendly EPSQ.	ABT
Send Secret/Confidential, non-overseas, investigations to OPM.	Implemented
Data mining Pilot Project investigating legal issues, appropriateness, reciprocity, and equivalency.	ABT
Foreign Travel Database Research.	ABT
Institute JPAS.	ABT
DoD components and agencies need to develop a process to adequately track the backlog.	ABT
Use of a Virtual Distributed Database.	ABT

Table D.10 DoDIG Recommendations for Security Clearance Prioritization

Recommendations	Status
ASD(C3I) establish an IPT to develop criteria for determining the highest priority mission-critical and high risk positions.	ABT
ASD(C3I) develop a process for relating individual clearance requests to those mission-critical and high risk positions.	ABT
DSS establish the process and metrics to ensure expeditious processing of personnel security clearance investigations in accordance with established priorities.	ABT

Table D.11 Insider Threat IPT Recommendations

Recommendations	Status
Establish as an investigative prerequisite for a favorable SSBI completed within the past five years for CAT 1 insiders.	ABT
Establish an investigation prerequisite, the requirement of a NACLC and credit check associated with Secret/Confidential access (or NACI for civilians by OPM) for CAT 2 insiders.	ABT
Conduct minimum PRs at a five-year interval for CAT 1 positions and a 10-year interval for CAT 2 positions.	ABT
Employ maximum use of data mining to enable continual online review of personnel security information.	ABT
Enforce policy that requires immediate information system access removal for separated employees.	ABT
Include appropriate questions in the SSBI to address online behavior for CAT 1 and CAT 2 insiders.	ABT

Table D.12 DoDIG Recommendations for Tracking Security Clearance Requests

Recommendations	Status
Track all security clearance requests from the time they are received until the investigative cases are opened. Security clearance requests that are not opened to investigative cases and those investigative cases that are opened without electronic requests should be included in the tracking process.	ABT
Post, weekly, the names and Social Security numbers (SSN) of all cases in process on the Extranet for Security Professionals. The entry for each name should include, at a minimum, the date the request was loaded into CCMS, the date that the investigative case was opened, and the date that the case was closed.	No action

Table D.13 GAO Recommendations for the Overdue PR Backlog

Recommendations	Status
SecDef direct C3I to design routine reports from the JPAS database to show the full extent of overdue update and those in process.	ABT
SecDef direct C3I to develop appropriate incentives to encourage agency security managers to keep information in the database current and to submit reinvestigation requests on time. Changes in existing regulations, policies, and procedures may be necessary to provide such incentives.	Implemented

Table D.14 Draft DoDIG Report on Resources of DoD Adjudication Facilities, August 2000

Recommendations	Status
The DoD CAFs should determine the personnel and resources required considering all the factors that affect the adjudication and appeals procedure.	Implemented
DoD components and agencies and contractors should provide personnel and resources to adjudicate and process appeals for the projected security clearance requests.	Implemented
C3I, in conjunction with the DoD CAF Directors and Chiefs should analyze the impact of the (SIC) and determine the appropriate implementation date for JPAS.	Implemented
USD(C) and C3I should review the DoD components budget submission to ensure that the DoD budget for FY 2002 and outyears enables the CAFs to meet forecasted workload requirements.	Implemented

Personnel Security Investigations Process Review Team (2000) Recommendation Summary by Responsible Action Office

SECRETARY OF DEFENSE:

(20) OBSERVATION: The current placement of the personnel security investigative mission and the associated oversight responsibility is appropriate.

- The Secretary of Defense maintain current organizational structure for the remainder of the recovery plan.

ASD(C3I):

(1) OBSERVATION: OPM and the Defense Security Service (DSS) use different methods and formats to collect data used as the basis for a personnel security investigation and to cancel or make changes to investigations.

- ASD(C3I) issue necessary formal direction to ensure DSS is fully engaged, resourced and committed to adopting the electronic SF 86, as soon as it is available and meets all user requirements, to replace the EPSQ and paper SF 86, eliminating request procedure inefficiencies.

- ASD(C3I) direct funding to accommodate enhancements to the electronic SF 86 to meet DoD specific needs, such as automated release and fingerprint forms and CCMS connectivity.

(2) OBSERVATION: There is no useable electronic archive capability for EPSQ data.

- ASD(C3I) issue necessary formal direction to ensure DSS is fully engaged, resourced and committed to adopting the electronic SF 86, as soon as it is available and meets user requirements, to replace the EPSQ and paper SF 86, eliminating request procedure inefficiencies.

- ASD(C3I) direct funding to accommodate enhancements to the electronic SF 86 to meet DoD specific needs, such as automated release and fingerprint forms and CCMS connectivity.

(3) OBSERVATION: DoD’s security investigation request process is only partly automated and requires hard copy forms to supplement electronic requests.

- ASD(C3I) direct a study to implement technological solutions to achieve electronic submission of all components of the personnel security investigation request.

ASD(C3I) Continued:

(5) OBSERVATION: DoD currently lacks a comprehensive system to prioritize Personnel Security Investigations (PSIs).

- ASD(C3I) implement new priority list.

(6) OBSERVATION: Varying and overlapping investigative policies and requirements may result in unnecessary investigations being requested.

- ASD(C3I) review the DoD 5200.2-R investigative requirements to ensure all investigative requirements are valid; specifically the SSBI requirements for DCII access and investigative support duties.

- ASD(C3I) review implementing policies to ensure adequate direction is provided so requests for PRs are based on validated access needs rather than to maintain established clearance eligibility.

(7) OBSERVATION: Current national investigative standards may not allow limited investigative resources to be focused on the most productive sources of information.

- ASD(C3I) establish a plan to conclude research on the productivity of sources. Evaluate findings against current standards and, if warranted, propose new investigative standards to the SPB for implementation.

(8) OBSERVATION: The DoD is not routinely acquiring information contained in certain government and commercial databases that may be relevant to personnel security determinations, and is not taking maximum advantage of automated data collection and assessment techniques within the PSI process.

- ASD(C3I) assess current research regarding automated techniques and the impact their implementation would have in the PSI process.

- ASD(C3I) establish a plan to conclude research, evaluate findings against current standards and, if warranted, proposed new national investigative standards to the SPB for implementation.

(9) OBSERVATION: DSS and OPM have experienced delays and inconsistent responses from local law enforcement agencies in accessing Criminal History Record Information (CHRI).

- ASD(C3I) support implementation of the current legislation regarding access to state CHRI.

ASD(C3I) Continued:

(10) OBSERVATION: PSI cases with overseas leads historically and currently take longer to complete.

- ASD(C3I) coordinate with the military services to establish performance standards for the completion of overseas leads.

- ASD(C3I) query organizations responsible for conducting overseas PSI leads to assess investigative priorities and current resources targeted to conduct PSI leads.

(11) OBSERVATION: DoD now utilizes contract investigators as a source for background investigations. The quality control efforts are not uniform for these contractors.

- ASD(C3I) ensure that there are sufficient quality controls in place for all providers of DoD background investigations and that national standards are met.

- ASD(C3I) ensure the DSS Standards and Evaluation or similar program is adequately funded.

(12) OBSERVATION: DSS is not currently meeting the needs of its customers in the area of personnel security investigations.

- ASD(C3I) continue the PERSEREC effort to evaluate current business practices of DSS and consider alternative methods to accomplish the mission.

- DSS identify its customer base, assess the component and contractor customer requirements for investigative products, and establish measurable goals to ensure that customer needs are met.

(13) OBSERVATION: OASD(C3I) does not consistently coordinate adjudicative policy issues with the component entity assigned responsibility for administering the personnel security program.

- ASD(C3I) coordinate with components' Senior Security Official on all issues impacting personnel national security suitability and security clearance determinations. Component policy representatives will coordinate accordingly with the CAFs as appropriate and provide a consolidated component response.

- ASD(C3I) direct the removal of paragraph 11-101(a)(4) of the 5200.2-R that assigns OASD(C3I) the responsibility to provide policy, oversight, and guidance to the component adjudication functions as this language is inconsistent with DoD Directive 5200.2 and usurps component prerogatives.

ASD(C3I) Continued:

(14) OBSERVATION: The standards to assess timeliness and quality of the adjudication and investigative processes are inconsistent.

- ASD(C3I) continue to monitor OPM and DSS timeliness and performance.

(15) OBSERVATION: The personnel security continuous evaluation program within DoD is ineffective.

- ASD(C3I) evaluate and, if warranted, implement a new continuing evaluation program, such as ACES, as soon as practicable, or other alternative methods of or enhancements to continuous evaluation.
- ASD(C3I) and the component Senior Security Officials review the findings and recommendations from the on-going research and propose changes to national standards as appropriate for periodic reinvestigations.
- ASD(C3I) and Senior Security Officials include plans for continuous evaluation emphasizing management and training in conjunction with the forthcoming DoD strategic plan for personnel security.

(16) OBSERVATION: OPM and DoD maintain automation solutions for PSI case management that are independent and incompatible.

- ASD(C3I) ensure that CCMS remediation efforts are adequately funded and provide management oversight sufficient to ensure that these actions are executed on schedule.
- ASD(C3I) negotiate with OPM and direct DSS to coordinate efforts to evaluate their respective PSI case management requirements, reach agreement on a common architecture and commence joint development of a future compatible system that will support all government investigative requirements.

(17) OBSERVATION: The JPAS will resolve many concerns regarding the PSI process and associated workload management, and it could provide a basis for further improvements.

- ASD(C3I) continue to support and fund current development and accelerate deployment plans for JPAS.
- ASD(C3I) seek participation of non-DoD agencies in the JPAS effort.

ASD(C3I) Continued:

(18) OBSERVATION: Changes in policy, which have increased workload, have not come with commensurate funding.

- ASD(C3I) ensure that all policy changes that increase workload are appropriately funded before implementation.

(20) OBSERVATION: The current placement of the personnel security investigative mission and the associated oversight responsibility is appropriate.

- ASD(C3I) not initiate or support any organizational changes affecting DSS or the CAFs unless analysis determines that a near-term decline in investigative or adjudicative productivity will not result.

(21) OBSERVATION: OASD(C3I)'s oversight of the personnel security program has not been effective.

- ASD(C3I) evaluate its current personnel security program oversight responsibilities and establish a new and comprehensive oversight strategy that reflects the level, extent and functions that are essential for support of the program.
- ASD(C3I) assign the specific oversight responsibilities to organizational elements that are sufficiently staffed and resourced for timely execution of these critical functions.
- ASD(C3I) ensure that all aspects of the new oversight strategy are executed as required.
- ASD(C3I) ensure that program decisions are appropriately staffed and coordinated to achieve accurate component response.

(22) OBSERVATION: There is no strategic plan, at the national or DoD level, for personnel security.

- ASD(C3I) commence development of a DoD personnel security strategic plan that is in concert with the SPB vision.

(23) OBSERVATION: Actions now underway to eliminate the PSI backlog will succeed only if multiple organizations achieve and maintain targeted levels of performance.

- ASD(C3I) ensure effective monitoring and status reporting, at least quarterly, to encompass the investigative performance of OPM and DSS.

- ASD(C3I) provide timely management intervention as needed to correct negative trends detected in OPM and DSS investigative performance.

ASD(C3I) Continued:

(24) OBSERVATION: Policy changes that result in increased workload or decreased productivity would jeopardize success of the Spend Plan.

- ASD(C3I) defer implementation of new "insider threat" investigative requirements – or any other new investigative requirements until the backlog problem is resolved, processing times are significantly improved, and data shows that the additional workload can be absorbed.

(25) OBSERVATION: There are varying investigative and adjudicative requirements and policies for civilian, military and contractor employees performing sensitive duties.

- ASD(C3I) fund and direct a study of the varying investigative and adjudicative standards applied to civilian, military and contract employees performing sensitive duties for the DoD. The study would examine the rationale for each and determine which requirements best satisfy national security needs.

- ASD(C3I) direct the development of consistent investigative and adjudicative standards, based on the study results, for all civilians, military and contractor employees performing sensitive duties and sponsor a new executive order through the SPB to standardize these requirements to ensure national security concerns are consistently satisfied.

(27) OBSERVATION: There is a need to generate and guide research based on strategic plans and requirements, and to coordinate research efforts across the community.

- ASD(C3I) develop a strategic plan to guide DoD research programs, in concert with the national strategic plan for personnel security.

(29) OBSERVATION: Services do not have adequate representation on intelligence research committees and subcommittees.

- ASD(C3I) request military service representation on the PSMRP Senior Steering Group.

DEFENSE SECURITY SERVICE:

(1) OBSERVATION: OPM and DSS use different methods and formats to collect data used as the basis for a personnel security investigation and to cancel or make changes to investigations.

DSS continued:

- DSS work with customers to develop standard mechanisms for canceling or otherwise making adjustments to ongoing investigations.

(3) OBSERVATION: DoD's security investigation request process is only partly automated and requires hard copy forms to supplement electronic requests.

- DSS develop a tracking system for incomplete request packages showing source and problem.

- DSS coordinate with customers to develop procedures for returning incomplete request packages.

(5) OBSERVATION: DoD currently lacks a comprehensive system to prioritize Personnel Security Investigations (PSIs).

- DSS and Standard Systems Group (SSG) Program Management Office (PMO) update CCMS as planned to accommodate the new priority list.

- DSS deploy the EPSQ version 2.2.

- DSS establish a system to measure performance in processing priorities.

(10) OBSERVATION: PSI cases with overseas leads historically and currently take longer to complete.

- DSS develop a more efficient tracking system for overseas leads.

(16) OBSERVATION: OPM and DoD maintain automation solutions for PSI case management that are independent and incompatible.

- DSS and OPM evaluate their respective PSI case management requirements, reach agreement on a common architecture and commence joint development of a future compatible system that will support all government investigative requirements.

(19) OBSERVATION: DSS does not have a mature cost infrastructure to use for decision-making and pricing.

- DSS continue pursuing activity-based unit costing whether using JOCAS or some other accredited system, but ensure that the customer's billing requirements are met.

- DSS provide the services with an itemized bill that identifies investigative product by customer.

COMPONENT SENIOR SECURITY OFFICIALS:

(5) OBSERVATION: DoD currently lacks a comprehensive system to prioritize Personnel Security Investigations (PSIs).

- Component Senior Security Officials establish a system to accommodate priority adjudication.

(6) OBSERVATION: Varying and overlapping investigative policies and requirements may result in unnecessary investigations being requested.

- Component Senior Security Officials review the security investigation requirements associated with the various military occupational specialties to ensure the appropriate investigative level is assigned.

(10) OBSERVATION: PSI cases with overseas leads historically and currently take longer to complete.

- Component Senior Security Officials increase resources to overseas service components targeted for conducting PSI leads, if warranted based on results of the queries, or determine alternative means for conducting leads overseas (such as DSS conducting overseas leads, or expanded use of contractors).

(14) OBSERVATION: The standards to assess timeliness and quality of the adjudication and investigative processes are inconsistent.

- Component Senior Security Officials monitor the CAF quality review of investigative products to ensure it satisfies concerns regarding consistent investigative quality.

- Component Senior Security Officials monitor the timeliness of their respective CAFs to insure customer needs are met.

- Component Senior Security Officials ensure CAF peer review group activities include quality of adjudicative determinations as well as best practices for improved adjudicative timelines.

DOD POINT OF CONTACT FOR SCI POLICY:

(4) OBSERVATION: There is no standardized pre-screening process for individuals nominated for security clearance.

- The DoD point of contact for SCI policy develop a standardized prescreening format specifically for the SCI community.

OSD REPRESENTATIVES TO THE SPB:

(9) OBSERVATION: DSS and OPM have experienced delays and inconsistent responses from local law enforcement agencies in accessing Criminal History Record Information (CHRI).

- The OSD representative to the SPB Forum recommend that the SPB coordinate with the DoJ to develop incentives for local law enforcement agencies to comply with requests for CHRI (such as grants or federal funding to local agencies) and continue to press for the enactment of the two unresolved issues.

(22) OBSERVATION: There is no strategic plan, at the national or DoD level, for personnel security.

- The OSD representative to the Security Policy Forum propose to the SPB development of a strategic plan for the nation's personnel security program.

(26) OBSERVATION: The SPB has no formal recognized method of promulgating policy decisions.

- The OSD representative to the Security Policy Forum propose that the SPB establish formal procedures for the security community to introduce prospective changes to policies and procedures that are clearly communicated.

- The OSD representative to the Security Policy Forum propose that the SPB establish a policy directives system to issue SPB policy decisions by formal means, documented in "National Security Policy Decision" packages, similar to ISOO directives.

(27) OBSERVATION: There is a need to generate and guide research based on strategic plans and requirements, and to coordinate research efforts across the community.

- The OSD representative to the Security Policy Forum recommend the SPB develop a national level strategic plan for personnel security that can be used to guide research priorities.

(28) OBSERVATION: There is a need for greater sharing of personnel security research across government agencies.

- The OSD representative to the PSMRP recommend the completion of the central research data repository for personnel security research that can be accessed government-wide.

- The OSD representative to the PSC recommend that the Research Sub-Committee establish a series of workshops through which research personnel could share information on current research topics and efforts that are of general interest to the community.

DEFENSE PERSONNEL SECURITY RESEARCH CENTER:

(27) OBSERVATION: There is a need to generate and guide research based on strategic plans and requirements, and to coordinate research efforts across the community.

- PERSEREC coordinate with the PSC's Research Sub-Committee of the SPB to:
  1. Review and comment on personnel security policy papers, plans, findings and research reports submitted by individual agencies and centers.
  2. Synthesize common and unique research implications.
  3. Advise individual agencies and centers that use personnel security research on SPB suggestions for pursuing crosscutting and agency-specific research activities.

Appendix E

Comparison of Personnel Security Programs at Selected Federal Agencies

Comparison of Personnel Security Programs at Selected Federal Agencies[32]

The text and table in this appendix summarize the practices of five representative federal agencies, as of 2002, that do background investigations and adjudications of security clearances: DoD's DSS, OPM, the Department of Energy (DOE), the Central Intelligence Agency (CIA), and the National Reconnaissance Office (NRO). Several important historical developments are also noted. Across these agencies key differences include the:

- Volume of clearances that must be processed and how long processing takes.
- Co-location or physical separation of functional specialties within the system, and the consequent ease of interaction between specialists.
- Degree to which processing of clearances relies on information technology.
- Degree of reliance on federal investigators as opposed to contractor investigators.
- Degree to which "clean case screening" procedures are used.

The total volume of clearances varies greatly across agencies. In 2000, some 2.1 million DoD personnel held security clearances. DOE accounted for approximately 105,000 clearances, and roughly 80% of persons working at DOE facilities are contractors, not DOE employees. The size of the workforces at CIA and NRO remains classified. As discussed earlier in the main body of this report (see section "Comparison of Investigation and Adjudication Across Federal Agencies"), the volume of clearances processed per year affects what is operationally feasible.

The physical locations of the various personnel security specialists grew out of the circumstances of the organizations' founding and history, but these locations also express the relationships each agency assumes among the various functions. The most centralized structure among the agencies compared here is found at CIA, where a combination of in-house and contractor units do background investigations and in-house adjudicators make decisions based on those investigations.

In contrast, DOE exemplifies the most decentralized structure. DOE's personnel security program emerged from the need to ensure that only trustworthy employees handled restricted data or special nuclear materials at various sites across the country. A site-specific focus has persisted since the late 1940s. DOE invests 11 sites around the United States, some of which work with nuclear materials, with the responsibility for initiating and tracking security clearances for personnel at that site.[33] DOE has never been granted authority to conduct personnel investigations. Its background investigations are conducted either by OPM or, for certain high-risk positions, by the FBI. If in turn OPM or the FBI contracts for investigations, DOE does not have input into this decision. The DOE personnel security specialists at each site who compile records and track cases do a variety of tasks, and at small offices they may perform duties in addition to personnel security functions. Personnel security specialists at each location adjudicate clearances for personnel at that site (L. Gebrowsky, personal communication, August 2, 2002).

DSS and OPM are larger and more multifaceted organizations than either CIA or DOE, and their structures reflect these demands. Both operate from headquarters in the greater Washington,

[32] This appendix is a combination of text and appendix material from Lang and Herbig (2002). The text and table do not reflect the recent activities to transfer DSS PSI functions to OPM.

[33] The 11 sites are: Richland, WA; Idaho Falls, ID; Oakland, CA; Las Vegas, NV; Albuquerque, NM; Chicago, IL; Pittsburgh Naval, PA; Schenectady Naval, NY; Savannah River, GA; Oak Ridge, TN; and Washington Headquarters in Germantown, MD.

DC, area that are supported by regional and district offices distributed nationwide. DSS has five regional headquarters and some 80 field offices; OPM's current investigative provider, USIS, has four regional offices, 48 district offices, and 180 Investigator Duty Station offices.

The intent of the consolidation of DoD's resources for background investigation of its personnel into DIS in 1972 was to increase efficiency and improve the quality and timeliness of investigations. The goal was to create a single professional cadre of government civil servants who would investigate all DoD personnel who needed access to sensitive information. In 1980 further consolidation brought under DIS the Defense Industrial Security Program and its organizational expression, the Defense Industrial Security Clearance Office (DISCO), along with the DoD Security Institute (DoDSI) to provide training. This consolidation concentrated the burgeoning security program for contractors and the training of security personnel at DIS. In 1992 DIS added counterintelligence to its capabilities, and in 1997 it assumed the name Defense Security Services.

DoD procedures deliberately keep the investigator and the adjudicator organizationally and physically separate. In earlier periods this goal was not so clear-cut. Before the consolidation that produced DIS in 1972, both investigation and adjudication functions were handled within the military components in various configurations, and since 1965 industrial clearances were tracked and adjudicated, but not investigated, by DISCO.

In 1984 DoD launched an investigation into industrial security practices in response to the serious espionage cases by contractor employees Christopher Boyce and James Durwood Harper. The report by the "Harper Committee," published in December 1984 (DoD Industrial Security Review Committee, 1984), raised the issue of potential unfairness to the applicant if the agency doing the investigation (in this instance DIS) also adjudicated the clearance. Since DISCO did all adjudications for contractors, and since DISCO became part of DIS in 1980, in effect the same organization was then performing both functions, albeit with different personnel.

The report cited the Administrative Procedure Act (5USC 554d2) and the Attorney General's manual on this act, which characterized the law as "intended to maintain the independence of hearing officers, and as a practical matter this means that an agency's hearing examiners should be placed in an organizational unit apart from those to which investigative and prosecuting personnel are assigned…" (DoD Industrial Security Review Committee, 1984, p. 24). There followed a discussion of whether this applied to personnel security adjudication hearings or not, since all personnel security actions take authority ultimately from the Executive Order, while the law specifically refers to programs created by statute. The Harper Committee study suggested that would be better for DoD to be safe rather than sorry and to keep them separate, reasoning that "If the program is not within the scope of 554 American Psychological association, there may still be due process and functional concerns where an agency exercises both investigative and adjudicative functions." (DoD Industrial Security Review Committee, 1984, p. 25).

Following the Harper Committee's recommendations, DoD undertook several reforms in the mid-1980s that widened the separation between the investigation and adjudication functions based on the belief that the law required it and that it seemed desirable. For example, in June 1985, DISCO's Adjudication Division was transferred out of DIS and into a division in the DoD Office of General Counsel. This move created the desired organizational separation for adjudicators from DIS as the investigative agency. However, screening procedures for contractor employees on-going at DIS (now DSS) since 1984 still raised questions about whether the same agency doing investigations is also in effect doing adjudications, as noted in a DoD Inspector General audit of February 2001 (DoD Inspector General, 2001). Thus the supposed necessity to keep these functions separate and issues about how to disentangle them remain lively concerns in DoD.

Ostensibly both OPM and NRO handle background investigations similarly in that they use contractor investigators. Currently, USIS is OPM's sole investigation provider. However, due to the heavy workload, OPM is in the process of obtaining a supplemental provider. USIS regularly competes against other providers for business. Although USIS has operated as a private company for 6 years, many of its field agents came with previous experience as federal investigators for OPM and other investigative agencies such as the FBI. USIS, on behalf of OPM, conducts background investigations for approximately 100 federal agencies. DoD's personnel security investigations are only one of those 100 federal agency customers. USIS submits DoD background investigations to OPM, which forwards them for adjudication to one of DoD's eight CAFs.

The National Reconnaissance Office (NRO) is a hybrid agency that straddles DoD and CIA in its mission to manage the development and operation of intelligence satellites. Its funding and its personnel come from both DoD and CIA; staff members usually serve a tour of duty at NRO and then return to their sponsoring agency. Contractor employees are closely integrated with government staff at NRO due to the oversight the agency maintains over contractor companies supplying space technologies. NRO's approach to personnel security is also eclectic. All background investigations for NRO are contracted out, and since persons seconded to NRO from other agencies were usually issued access eligibility there, most of NRO's access determinations are for contractor employees. In-house adjudicators make decisions on access eligibility for NRO, and limited interaction between investigators and adjudicators occurs during the investigative process. NRO grants a "conditional clearance" in some cases in which issues arise, and then monitors the employee to ensure that conditions are being met. Through various mechanisms monitoring is a direction other agencies are taking as well. For example, the Washington Headquarters Service, a DoD CAF, may issue a warning letter in which a subject is told that although adjudication has granted the person a clearance, the investigation has noted questionable behavior, and that if the behavior continues, the clearance will be revoked.

Some agencies have evolved personnel security procedures tailored to their special needs. DOE, for example, offers an "Accelerated Access Authorization Program" (AAAP) that grew out of a situation in which particular personnel were needed quickly to respond to a rare clean-up of materials. The program proved useful as a method for ensuring that interim clearances for some sensitive positions are granted on the basis of additional information. It consists of a specified set of evaluations done at either Albuquerque, NM, or Oak Ridge, TN: a CI-scope polygraph, a drug screen, a psychological evaluation, an interview, a completed SF86 filled out at the site, and results received from an National Agency Check (NAC) into criminal history. The DOE Director of Security then grants an interim clearance, and the case is simultaneously sent for the typical background investigation followed by adjudication, since accelerated access is only an interim clearance. This AAAP clearance takes DOE about 17 to 27 days to complete, including two full days for the applicant on site plus waiting for the NAC, drug screen, and polygraph results. DOE processed roughly 150 of these AAAP clearances in 2000.

Both CIA and NSA have evolved accelerated or concentrated screening procedures that are tailored to the needs of each of those agencies. DoD CAFs also issue interim clearances (while an investigation is on-going) based on favorable checks of national agency databases. These interims are issued in a matter of days for lower-level clearances and in 30 to 45 days for an interim Top Secret clearance.

Table E.1 (below) summarizes key differences among the five agencies under discussion: DSS, OPM, DOE, CIA, and NRO. We compared the practices of five representative federal agencies that do background investigations or adjudications of security clearances: DoD's DSS, OPM, DOE, the CIA, and NRO.

Overall, we found several important differences in procedures and assumptions across federal personnel security programs, implying that there is a range of workable approaches to procuring a trustworthy workforce. Among the dimensions along which these procedures vary are: the co-location or physical separation of functional specialties within the system, and the consequent ease of interaction among specialists; the scale of the task, (i.e., the volume of clearances that must be processed by a given agency and how long processing takes); the degree to which processing of clearances relies on information technology; the degree of reliance on in-house investigators as opposed to contractor investigators; whether "clean case screening" procedures are used; and certain distinctive features of these agencies that affect their procedures.

Among these dimensions, the volume of clearances dictates general parameters for what is operationally feasible in a personnel security system. In 2000, some 2.1 million DoD personnel held security clearances, whereas DOE accounted for approximately 105,000; NRO and CIA are both smaller, though the size of their workforces remains classified. A relatively small agency focused on specific missions can approach the vetting and monitoring of its employees differently than can a large organization like DoD. DoD's need to track millions of cases, archive those data, and regularly communicate with far-flung local security managers makes its task different from an agency located largely in one building.

Nevertheless, DoD can learn from and adapt the relevant innovations of others. OPM is an even larger and more varied organization than DoD. OPM is responsible for vetting personnel for many agencies of the federal government. OPM achieves a relatively fast turnaround on background investigations done by USIS by relying on automated scoping routines performed by computer, automated data requests to national agencies, scan-able forms filled out by sources in the field to allow rapid capture of data into electronic form, field investigators equipped with laptop computers, and an information system capable of reliably generating various management reports and billing for an investigation as soon as it is scheduled (Office of Personnel Management Investigations Service, 1999). DSS is working to implement these kinds of automated processes as well. The ideal end-state in an improved personnel security system would feature an information technology office that was fully integrated into all parts of the system to support personnel security processes from "tooth to tail," from data collection in the field and integration of data from various sources, through investigative report, adjudication, notification of outcome, case tracking and archiving of data, to management reports and system oversight. The proposed personnel security system that we describe below includes such an office to integrate automated processes.

Secondly, DoD's practice of strictly separating investigators from adjudicators is not the only model used by these various federal agencies, and other models could be considered. Those who perform background investigations gain valuable insights into a subject that may be only partially captured in a written report. An adjudicator may have questions or concerns that could be most efficiently addressed in direct communication with the investigator. The advantages of closer interaction could be explored through the experiences with it at the CIA, for example. In addition, clean case screening by case analysts—e.g., for interim clearances at DISCO and as part of the 2002 pilot study of phased PRs at DSS—suggests that investigative staff can be relied upon to make limited adjudicative determinations.

The issues that DoD needs to sort out regarding potential interaction between investigators and adjudicators cluster around: (1) what the decisions by adjudicators represent, (2) what are the legal issues, and (3) how to limit the potential for interactions to add significant burdens for the investigative or adjudicative staff. Currently there is broad agreement in DoD that adjudication and investigation should be kept separate. So how should adjudicators be considered: are they like the members of a jury in a courtroom, weighing evidence and reaching decisions based on it, or are they more like clinical service providers who collect information about a client and make judgments about each client to decide on a course of action? Should adjudicators continue to be kept apart from the investigator, who in the courtroom model is like a police detective who gathers evidence about a defendant, or should investigators and adjudicators be encouraged to consult with each other as a clinician would consult a psychologist, teacher, parents, and whoever else had insights about their client?

Thirdly, DoD can learn from the mere fact that there are such a variety of personnel security procedures at different agencies. Things can be done successfully in more than one way and, more importantly, different agencies need somewhat different procedures to best accomplish their personnel security. Calibrating a balance is necessary between further consolidation, with its promise of efficiency, standardization, and parsimony, and continued component control, with its assurance of responsiveness, closer fit with unique needs, and control over resources.

Table E.1
Comparison of Federal Personnel Security Programs

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
Composition of PSI personnel: what are the people called who are on the team?	• Personnel Security Assistant (PSA) • Case Analyst (CA) • Special Agent (SA) • CAF adjudicator	• Data Transcriber • Reviewer • Adjudicator • Investigative Inquiry Specialist • Special Investigator • Record Searcher / Record Specialist / Record Courier	• Personnel Security Specialist (PSS)	• Investigator (several branches) • Records Manager • Case Manager (who serves as the adjudicator) • Personnel security administrators. • Personnel security experts.	• Customer Relations Specialists • Investigative Management Systems personnel • Contract Field Investigators • Special Actions Staff • Special Investigations.
Locations of the PSI personnel: where is everybody?	• DSS personnel are at DSS HQ in Alexandria, VA, and in Linthicum, MD; at the PIC in Ft. Meade, MD; at DISCO in Columbus, OH; or at DSS field throughout the United States and in Puerto Rico. • Contractor investigation companies located in DC area, with field offices elsewhere • CAF adjudicators are at 8 CAFS in the Washington D.C. area and in Columbus, OH.	• OPM-FIPC personnel are in HQ office in Boyers, PA • USIS, a "sole-source contractor," consisted in 1996 of 400 federal Investigators who turned into a private company. HQs in Annandale, PA, with 4 regional offices, 48 district offices, and 180 investigator duty station offices	• At 11 offices around the country, personnel security specialists initiate, adjudicate, and track clearances at the sites for which they are responsible. • DOE personnel security investigations are performed by either OPM or the FBI	• All personnel security staff are domestically located.	• Adjudicators are located at the NRO Personnel Security Division along with the Investigative Management Systems personnel who initiate and track cases • All investigations are contracted out • NRO staff members come from other agencies. NRO straddles DoD and CIA, with staff from both.
Extent of interaction between investigators and adjudicators: who talks to whom?	• No interaction is structured between the adjudicator and the case analyst, or the adjudicator and the special agent.	• The contract company USIS does personnel security investigations, and no interaction with DoD adjudicators is structured.	• There are no DOE investigators because DOE does not hold authority to conduct personnel investigations. • Personnel security specialists adjudicate cases.	• When feasible, interaction between investigators and adjudicators is facilitated.	• The contract company does investigations, and no interaction with adjudicators is structured.

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
Timeliness for completing PSIs: how long does it now take, for example, to get a TS clearance?	• 330 days [2000]	• OPM has four service type categories; 35/75/120/180 days. The timeliness service requested by the customer dictates the applicable completion time category.	• Q clearances: 60 days at Albuquerque, • 90 days on average across the 11 sites	• No information	• No information.
Number of Clearances Currently held	• FY2000: roughly 2.1 million total in DoD • Confidential: 74,795 • Secret: 1,571,780 • Top Secret: 211,566 • TS-SCI: 263,599 • Total: 2,121,740*	• DoD figures, see DSS	• 105,000 in DOE, 70,000 Q 35,000 L	• [classified]	• [classified]
Use of capabilities of information technology: how are computers, automated decision systems, etc. used?	• CCMS used for tracking cases, as the database of info from investigations, and for report generation • CCMS does autoscoping, but the CA also reviews this to add or delete leads ased on prior files, and to reflect special project demands. • Field investigators print out paper "Action Lead Sheets (ALSs)" from the electronic file sent in the "Field Investigation Management System," which converts CCMS data into leads. Use of ALSs facilitates data entry while doing personal interviews	• Case tracking in PIPS allows requestor to query status on-line • Automated decision logic in PIPS opens case, does scoping, generates automated data requests to other agencies, generates scannable investigation forms, and generates reports • Field investigators use laptops to generate and submit electronic ROIs	• Each of the 11 sites enters cases into a regional database using an IT system, and this information feeds into a central adjudicative database.	• Automated case tracking. • No information on system specifics.	• In-house NRO database and tracking of cases • No information on the specifics of what system they use or details of its use.
"Clean case screening": is it done, and in what circumstances?	• Yes: for industry cases only, DSS CAs at the PIC uses a screening guide to identify "clean cases"	• No information on clean case screening.	• The personnel security specialist reviews the investigation report and screens it for derogatory	• No information on clean case screening	• No information on clean case screening. • NRO grants "conditional clearances" with a

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
	which are entered into CCMS, archived, and sent to DISCO for a second review, then for issuance of clearance, unless an issue is found that demands adjudication by DOHA.		information. Cases with no derogatory information are adjudicated. The personnel security specialist follows up cases with derogatory information. After adjudication has been made, an appeals procedure is available. Appeals go to the Director of Security.		monitoring program to ascertain whether conditions are being met
Extent of reliance on in-house vs. contractor investigators	• DSS uses both in-house and contractor investigators. • DSS has approx 1400 in-house field investigation agents, and 1900 total in-house employees •DSS also uses six contractors providing PSIs in FY01: Dyncorps, Mantech, GBSG, MSM, OPM/USIS, Omniplex	• OPM relies entirely on contractor investigators, and USIS is the sole source • 2,067 employee field investigators and 507 contractor investigators work for USIS, performing all Special Investigator functions.	• DOE does not hold authority to conduct personnel investigations. By law its investigations are performed by OPM or, for certain high-risk positions, by the FBI.	• Not available.	• NRO relies on contractor investigators.

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
Distinctive aspects	• DSS, as an agency of the federal government, is one expression of the government's "stake" in personnel security; the CAFS are a second.	• OPM advances completed investigative case material to customers "closed pending" when certain source information is still pending. This allows the customer to make risk management decisions based upon the bulk of the timely, completed investigative material • PSIs are only one fraction of OPM's personnel investigations for many federal agencies, and security is only one of OPM's personnel functions for the federal government.	• DOE's approach to personnel security was shaped in part by its history as an agency that controls nuclear materials at various locations. A decentralized system of 11 regional offices has evolved. • DOE uses an Accelerated Access Authorization Program that allows interim clearances to be granted more quickly while a regular investigation and adjudication is ongoing.	• Much smaller than DSS's universe in DoD or USIS's universe in OPM. Has a specialized intelligence-related mission. • The hiring process includes a thorough medical examination of one's physical and mental fitness to perform essential job functions.	• NRO is much smaller than DSS's universe in DoD or USIS's universe in OPM, and NRO has a specialized space R&D mission. • Almost all of their personnel come from other federal agencies. • 80% of all clearances granted at NRO are for contractors. • NRO is an example of a DoD agency that contracts directly with a PSI provider.