PERS-TR-91-001

PERSEREC

CONTINUING ASSESSMENT OF CLEARED PERSONNEL IN THE MILITARY SERVICES: REPORT 1 - A CONCEPTUAL ANALYSIS AND LITERATURE REVIEW

Michael J. Bosshardt
David A. DuBois

Personnel Decisions Research Institutes, Inc.

Kent S. Crawford

Defense Personnel Security Research
and Education Center

January 1991

DEFENSE
PERSONNEL SECURITY
RESEARCH AND EDUCATION CENTER
99 Pacific Street, Building 455-E
Monterey, California 93940-2481

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S) PERS-TR-91-001
6a. NAME OF PERFORMING ORGANIZATION Personnel Decisions Research Institutes, Inc. 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION Defense Personnel Security Research and Education Center (PERSEREC)
6c. ADDRESS (City, State, and ZIP Code) 43 Main Street SE Riverplace, Suite 405 Minneapolis, MN 55414	7b. ADDRESS (City, State, and ZIP Code) 99 Pacific Street, Building 455E Monterey, CA 93940-2481
8a. NAME OF FUNDING/SPONSORING ORGANIZATION PERSEREC 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N00014-87-D-0717, Delivery Order 0005
8c. ADDRESS (City, State, and ZIP Code) 99 Pacific Street, Building 455E Monterey, CA 93940-2481	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)
Continuing Assessment of Cleared Personnel in the Military Services: Report 1 - A Conceptual Analysis and Literature Review

12. PERSONAL AUTHOR(S)
DuBois, David A., Bosshardt, Michael J., and Crawford, Kent S.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Technical Report	FROM 1/89 TO 5/90	January 1991	

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Continuing assessment, continuing evaluation, clearances, security, personnel security, security education

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This is Report 1 in a series of four reports examining the effectiveness of continuing assessment programs in the military services. It examines regulations and literature related to continuing assessment and has three primary objectives: (1) to conceptually define the meanings and objectives of continuing assessment programs as they exist in personnel security regulations, (2) to review available literature relevant to continuing assessment, and (3) to present ideas for improving continuing assessment programs.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	
22a. NAME OF RESPONSIBLE INDIVIDUAL Roger P. Denk, Director	22b TELEPHONE (Include Area Code) / 22c. OFFICE SYMBOL

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

PERS-TR-91-001 January 1991

CONTINUING ASSESSMENT OF CLEARED PERSONNEL IN THE MILITARY SERVICES: REPORT 1 - A CONCEPTUAL ANALYSIS AND LITERATURE REVIEW

Prepared by

Michael J. Bosshardt
David A. DuBois
Personnel Decisions Research Institutes, Inc.

Kent S. Crawford
Defense Personnel Security Research
and Education Center

Released by
Roger P. Denk
Director

Defense Personnel Security Research and Education Center
Monterey, California 93940-2481

FOREWORD

The continuing assessment of cleared personnel is at the heart of an effective personnel security program. The intelligence and security community asked PERSEREC to conduct research in this key area since there was a basic lack of empirical information concerning the current effectiveness of continuing assessment programs. In order to address this requirement, we contracted with Personnel Decisions Research Institutes (PDRI), Inc. to assist us in conducting a major study to review continuing assessment programs operating in the field. We had three objectives: (1) to gather baseline information necessary for developing future research projects in continuing assessment, (2) to identify problem areas that were impacting on the effectiveness of continuing assessment, and (3) to provide specific recommendations for improving continuing assessment both in terms of new approaches and suggested policy changes.

The project resulted in four reports that provide a complete review and assessment of continuing assessment in terms of the above objectives. Each of the reports has the opening title of *Continuing Assessment of Cleared Personnel in the Military Services*. The reports are then differentiated as follows:

Report 1 - *A Conceptual Analysis and Literature Review*. This report meets Objective 1 by providing a conceptual foundation for future research in continuing assessment and presenting a number of recommendations for specific research projects. The intended audience is primarily the research community.

Report 2 - *Methodology, Analysis, and Results*. This report meets Objective 2 through discussing the analyses and results from a large-scale survey of over 60 military sites worldwide. It describes how input from security managers, unit security managers, and unit commanders was combined to identify key problem and recommendation areas. It serves as the foundation for Report 3. The intended audience for this report is security personnel who are interested in detailed and specific data concerning the operation of continuing assessment programs in the different services.

Report 3 - *Recommendations*. This report addresses Objective 3 by outlining the principal findings and recommendations from the data collection effort described in Report 2. The specific objectives are to recommend policy changes and suggest approaches for improving the effectiveness of continuing assessment in military units. The intended audience is policymakers and security professionals.

Report 4 - *System Issues and Program Effectiveness*. This report also meets Objective 3 by taking a broader perspective and examining continuing assessment as a total system. This includes continuing assessment as it relates to other aspects of personnel security as well as

different aspects of continuing assessment (e.g., periodic reinvestigations, position vulnerability, legal issues, automation issues, etc.). The focus here shifts from primarily a field perspective to consideration of continuing assessment as one part of a total security system. Again, the intended audience is policymakers and security professionals, although the issues tend to be discussed with regard to longer-term initiatives as opposed to the more short-term focus of Report 3.

Numerous persons assisted in this research project. The authors would like to express appreciation to the individuals who served as points of contact at each of the survey sites. These individuals arranged the site visits and served as gracious hosts and fine coordinators. The excellent survey participation rates and high quality of the data obtained attest to their conscientiousness and hard work. Additional thanks go to the many installation security managers, unit commanders, and unit security representatives who completed survey forms for the project.

At the service headquarters, appreciation goes to Walt Mestre, Jim Baxter, Coy Williamson, and George Jackson who greatly assisted the authors in identifying and scheduling visits to the field units. Daniel McGarvey, at the American Institutes for Research, provided valuable assistance during the data collection phase. At PDRI, mention should be made of the efforts of Dr. Walter Borman, who assisted in the survey data collection efforts. Dr. Borman also served as a general adviser throughout the project. Special thanks also go to two PDRI staff members for their contributions in carrying out this research: Deb Skophammer for her skillful editing and typing of this report and Kathy Lillie for her assistance in the data analyses. Finally, at PERSEREC, James Riedel provided extremely helpful input during both the design and implementation phases of the project.

We believe that these four reports, taken as a whole, provide a solid foundation for both improving current DoD policy with regard to continuing assessment and for developing new products and approaches for improving continuing assessment.

Roger P. Denk
Director

EXECUTIVE SUMMARY

Continuing assessment of cleared personnel is a critical component of Department of Defense (DoD) personnel security systems. There is limited information available, however, to determine the effectiveness of these continuing assessment efforts. In order to address this deficiency, a project was initiated to evaluate how well continuing assessment programs are operating in the military services. The primary focus was on continuing assessment programs for individuals with collateral clearances (i.e., Top Secret, Secret, and Confidential). The principal project activities included a review regulations and literature related to continuing assessment and a survey of 60 Army, Air Force, Navy, and Marines Corps installations around the world to obtain detailed information about their continuing assessment programs.

This report is one of four project reports. It examines regulations and literature related to continuing assessment and had three primary objectives: (1) to conceptually define the meanings and objectives of continuing assessment programs as they exist in personnel security regulations, (2) to review available literature relevant to continuing assessment, and (3) to suggest ideas for improving continuing assessment programs. Findings for each objective are presented below.

Summary: Definition of the Meanings and Objectives of Continuing Assessment Programs

A major theme of this report is that the elements of the continuing assessment program can be usefully organized into a heuristic model of security-relevant behavior adapted from the applied psychology literature. This model consists of the following components: security criteria, informing, monitoring, evaluating/motivating, and controlling. The security criteria component describes security behaviors of interest. The informing component includes activities to ensure that cleared personnel understand their security-relevant duties. The monitoring component focuses on the methods and requirements for reporting security-relevant information. The evaluating/motivating component describes the procedures available for preventing or removing security risks and for maintaining the effectiveness of the continuing assessment system. Finally, the controlling component describes administrative and legal constraints of the continuing assessment program.

In addition to organizing the diverse elements of the continuing assessment program, this model provides several useful hypotheses for evaluating the effectiveness of the program's content and structure. For example, the model emphasizes the importance of precise specification of program objectives (i.e., security-relevant criteria of security compromise, suitability, and security duties) and of ensuring that the contents of the components are consistent with each objective. Additionally, the multiplicative structure of the model emphasizes that each component of the model (i.e., informing, monitoring, evaluating/motivating, controlling) must be effective in order for effective security-relevant behavior to occur.

A second theme of this report is that the continuing assessment program has three objectives: (1) to decrease the risk of security compromise, (2) to reduce the number of personnel who are unsuitable for access to classified information, and (3) to define the personnel security duties of all personnel. The personnel security program regulations specify general behavioral criteria that correspond to each of the three objectives. These three broad categories are in themselves complex sets of independent dimensions of security-relevant behavior. Strong empirical relationships among these behavioral dimensions are implicitly assumed, but remain undefined.

Comparisons of the Department of Defense and Director of Central Intelligence continuing assessment program regulations indicate that both are very similar in the methods employed to achieve the personnel security program objectives. Although some differences are evident from content analyses of the regulations (e.g., frequency of briefings and reports, access procedures), discussions with field personnel indicate the differences in practice are considerably greater than comparisons of regulations would suggest. Report Two of this series of reports provides detailed comparisons of operational differences between these two programs.

Four personnel reliability programs [Personnel Assurance Program (PAP), Personnel Security Assurance Program (PSAP), Personnel Reliability Program (PRP), and the Space Human Assurance and Reliability Program (SHARP)] are reviewed to identify features that might be incorporated into the DoD continuing assessment program. Some of the most promising features from these alternative programs include a thorough annual review, non-punitive personnel actions, and controls to protect individual rights (e.g., having counsel at hearings, anonymous files for personnel decisions). Incorporation of these alternative program components could increase the frequency and quality of information concerning the suitability for continuing access to sensitive information. Further review is warranted to examine the cost/benefits of these methods and to determine their relation to achieving personnel security objectives.

Summary: Continuing Assessment Literature

The continuing assessment literature is a diverse collection of expert opinion, narrative descriptions, and management analyses. The literature review highlights many research needs, identifies program obstacles, and yields additional ideas for program methods. This assortment of needs, obstacles, and ideas is organized and discussed in terms of the model of security-relevant behavior described above (i.e., continuing assessment criteria, informing, monitoring, evaluating/motivating, and controlling). Findings for each area are briefly described.

With respect to continuing assessment criteria, the literature review identified as the most critical research areas the need to clarify the relationships among the many security criteria and the need to specify empirically the linkages to compromise of classified information. The complexities of three broad categories of criteria--security compromise, personnel suitability, and personnel security duties--are described. A behavioral methodology for defining the interrelationships among these criteria is proposed.

Literature examining the informing component of the continuing assessment model indicates that security staff and cleared personnel are inadequately trained, and at least some staff are not trained at all. Insufficient reporting of security information by supervisors and commanders and the lack of studies evaluating training effectiveness suggests a need for comprehensive training needs analyses. This type of research would also help remedy another obstacle--adapting training to the needs of the locale and person. Alternative training methods are proposed to improve training outcomes.

Approaches to monitoring personnel for unreliable security-relevant behavior are discussed in terms of content and process issues. Recent research on credit reporting relevant to personnel security provides a model for future work in other important personnel security content areas. With respect to process issues, the need for research to define the reliability, validity, and utility of alternate assessment methods is emphasized. Recommendations for centralizing and automating recordkeeping and for identifying high risk groups are also discussed.

Discussions concerning the evaluating/motivating component of continuing assessment focused on approaches to improving adjudication of security-relevant information and accountability for performing continuing assessment duties. The application of statistical methods to adjudication is proposed as an approach to improving the quality, consistency, and timeliness of clearance decisions. Research on accountability suggests that providing formal consequences for performance is important.

Literature relevant to the controlling component primarily addressed two important constraints: access management and legal issues. Several sources recommend greater use of the need-to-know principle and the two-person rule in order to better manage access to classified information. With respect to legal issues, individual rights to privacy, due process, and equal protection have sometimes been cited as obstacles to effective continuing assessment. However, the possibility that improper implementation (rather than policy) of continuing assessment procedures and/or lack of understanding about the legal implications for the personnel security practice is considered as an alternative explanation for problems in this area.

Summary: Ideas For Improving Continuing Assessment

The analyses of continuing assessment regulations and review of relevant literature provide a rich source of ideas for improving continuing assessment. These ideas include suggestions for procedural improvements and for basic research. The ideas are grouped into seven category areas: security-relevant criteria, informing, monitoring, evaluating and motivating, managing constraints, program emphases, and program effectiveness. These are briefly summarized below.

With respect to criterion development, approaches for studying each major category of security-relevant behavior (security compromise, unsuitable conduct, security duties) are detailed, and the need for identifying the relationships between these categories is emphasized.

Regarding informing cleared personnel, possible approaches for improvement include conducting training needs analyses, developing standardized training modules, and utilizing innovative strategies to improve the transfer of training.

For monitoring cleared personnel, suggestions for improvement involve a range of information-gathering approaches, such as expanded drug and alcohol testing and developing new assessment methods such as psychological tests and annual security questionnaire updates. Research to provide validity and cost-effectiveness information on each of these monitoring methods is cited as important for selecting methods for monitoring personnel. Additionally, assessing the feasibility of centralizing and automating continuing assessment recordkeeping is mentioned as an important possibility for improvement.

With respect to evaluating cleared personnel, utilizing actuarial information in adjudicative decisions is presented as an approach to improving the validity and timeliness of clearance determinations. Ideas for improving motivation and accountability for performing continuing assessment duties include the use of incentives, performance appraisals, and inspections.

Regarding managing constraints, suggestions for improvement include the need for clarifying legal issues and for giving more emphasis to legal concerns and need-to-know principles in security education.

Ideas for improvement in two additional areas, program emphases and program effectiveness, also emerged from the literature review. With respect to program emphases, approaches to targeting scarce continuing assessment resources to high risk positions, individuals, and groups are presented. The need for evaluating, and changing if necessary, the priority given to continuing assessment in comparison to initial screening and to other areas of security is also discussed. Finally, proposals are made to develop and implement improved measures of program effectiveness.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

TABLES

FIGURES

APPENDICES

SECTION 1. INTRODUCTION

Problem

Keeping the United States' national security-related secrets is a problem of serious importance and immense scope. At the end of fiscal year 1989, there were over 2.8 million Department of Defense civilian, military, and contractor personnel with security clearances. Millions of others who have transferred, retired, or been terminated also know classified information. From the perspective of personnel security, the general problem involves screening individuals who are being considered for clearances, as well as monitoring and assessing the reliability of cleared individuals to prevent the compromise of sensitive information.

Recent history points to a need for improving personnel security practices. Espionage cases increased substantially during the 1980s, with public reports of more than 60 cases. A number of other individuals who engaged in espionage may have also been identified but their cases remain unreported for a variety of reasons (e.g., to protect sensitive intelligence operations and sources, or to avoid exposure of classified information) (Milberg, 1980).

The damage incurred by the compromise of classified information can be enormous. A report by the United States Senate (1986) assessed the damage from espionage in several ways:

- U.S. military plans and capabilities have been seriously compromised;
- U.S. intelligence operations were gravely impaired;
- U.S. technological advantages have been overcome in some areas;
- U.S. diplomatic secrets were exposed to the scrutiny of our adversaries;
- Sensitive aspects of U.S. economic life were subject to constant monitoring.

The overall financial impact of espionage during the 1980s has been estimated to be in the billions of dollars. One report noted that the Soviet KGB assessed the wartime impact of these espionage activities as "devastating" (United States Senate, 1986, p. 104).

A personnel security program (Department of Defense, 1987; Director of Central Intelligence, 1986) is one of the principal approaches utilized by the Department of Defense to meet the threat of information compromise. This program has two major emphases. The first involves screening individuals who are being considered for initial clearances. The second emphasis, which is the focus of this report, is the ongoing or continuing assessment of cleared personnel.

The importance of continuing assessment is underscored by several factors. For example, examination of espionage cases during the past decade suggests that few spies enter government service with the intent to commit espionage. Instead, most individuals become spies

as a result of personal and environmental circumstances that occur after job entry and after an initial security clearance has been granted. This suggests that an effective continuing assessment program is a critical element to deterring espionage.

There are other factors which point to the importance of the continuing assessment program. For example, initial clearance screening methods, like all selection methods, are not perfect. In addition, some persons who merit a security clearance at time of initial screening may undergo personal or environmental changes that make them security risks at a later time.

Although formal personnel security programs have been in existence for many years, concern has been expressed about the quality of these programs (U.S. House of Representatives, 1988). The Stilwell Report (DoD Security Review Commission, 1985) assessed the overall security system as being "reasonably effective" (p. 7), although it cited numerous recommendations for improving the system. A top-to-bottom security inspection of the military services found several deficiencies with operational personnel security programs (Secretary of the Army, 1986; Secretary of the Navy, 1987).

Objectives/Approach

One primary objective of this report is to define conceptually the meaning and objectives of continuing assessment programs within the military services. In order to accomplish this objective, a general model of security-relevant behavior is presented. This model is used to organize and analyze the components of current military branch continuing assessment programs in terms of their guiding regulations and to identify procedures from other continuing assessment programs that might be incorporated into the continuing assessment programs of the military branches. Regulations for SCI access, as well as for collateral (i.e., Top Secret, Secret, Confidential) clearances, are examined. To accomplish this, the model is used to organize the literature relevant to continuing assessment programs. Finally, ideas for improving the continuing assessment program are presented in the last section.

This report (Report 1) is one of four project reports. It examines regulations and literature related to continuing assessment. Reports 2 and 3 describe the results of meetings with continuing assessment experts and surveys of installation personnel to obtain detailed information regarding continuing assessment programs. This included a survey of security personnel and commanding officers at 60 Army, Air Force, Navy, and Marine Corps installations. Report 4 examines several broad issues related to continuing assessment, assesses the overall strengths and weaknesses of continuing assessment programs in the military services, and makes several recommendations for improving continuing assessment.

The remainder of this section provides a definition of continuing assessment. Section 2 presents a conceptual framework for analyzing continuing assessment programs. Section 3 describes the major elements of DoD and military branch continuing assessment regulations in terms of this conceptual framework. Section 4 describes four alternative continuing assessment programs and identifies procedures that might be incorporated into DoD continuing assessment programs. Section 5 summarizes literature relevant to continuing assessment. Section 6 presents new initiatives for improving continuing assessment.

It should be noted that the discussion throughout this report emphasizes the conceptual and general behavioral meanings of the continuing assessment system. Detailed information regarding the operation of various continuing assessment programs is provided in Reports 2 and 3 in this series of reports.

Definition of Continuing Assessment[1]

Before presenting a model of security-relevant behavior, we should first define what is meant by a "continuing assessment program." The DoD personnel security program regulation (Department of Defense, 1987) states that continuing assessment is designed to evaluate on an ongoing basis "the status of personnel under their jurisdiction with respect to security eligibility" (p. IX-1). The major components of continuing assessment programs include security education, derogatory information detection and reporting procedures (including adjudication of this information), and periodic reinvestigations for individuals with Top Secret or SCI access (Crawford, 1988, pp. 1-2). In addition, the Director of Central Intelligence (DCI) Directive 1/14 outlines similar, yet more extensive components for persons with SCI access.

Consistent with this perspective, Fedor (1988) defined continuing assessment as everything with respect to personnel security that happens after the initial security clearance. This definition includes, in addition to the areas cited above, employee assistance programs, performance reviews, access suspensions, and other activities that are included in the program regulations. The need for this broader definition becomes apparent with a conceptual analysis of continuing assessment programs.

---

[1]To facilitate the discussion throughout the report, a glossary of common terms encountered in continuing assessment has been prepared. This glossary is presented in Appendix A. It should be noted that the terms "continuing assessment" and "continuing evaluation" are used synonymously within DoD.

SECTION 2: A CONCEPTUAL MODEL FOR DESCRIBING CONTINUING ASSESSMENT PROGRAMS

In this section we present a conceptual model of security-relevant behavior. This model will be used in subsequent sections to describe current continuing assessment programs, to identify potential deficiencies in the design of these programs, and to summarize literature relevant to continuing assessment. Our discussion for this section is organized according to two topics--a psychological model of work performance and strategies for influencing security-relevant behavior.

A Psychological Model of Work Performance

The selection of a psychological model of performance is an appropriate and useful approach because continuing assessment has as its focus behavior relevant to maintaining adequate security. This model of work performance, which was adapted from Campbell and Campbell (1988, p. 89), suggests that performance is the multiplicative result of four general factors or components: (1) personal characteristics, (2) knowledge, (3) motivation, and (4) constraints that affect performance. That is,

---

Performance =

Personal Characteristics x Knowledge x Motivation x Constraints

---

Each component is discussed briefly below.

Personal characteristics (e.g., cognitive abilities, temperament, vocational interests) have shown significant relationships to performance in numerous studies (e.g., Hunter and Hunter, 1984; Schmitt, Gooding, Noe, & Kirsch, 1984). In their review of the literature for predictors of job performance, Hunter and Hunter (1984) found that a battery of cognitive ability tests is the best predictor of entry-level performance across jobs. In a review of research on non-cognitive variables used in selection, Hough (1988) found several personality constructs predicted performance in a wide range of military jobs. Vocational interest variables were also shown to have significant relationships with performance criteria. Finally, background information, or biodata, has consistently predicted job performance across a variety of work settings (Rothstein, Schmidt, Owens, Erwin, & Sparks, 1990).

Knowledge is a second major determinant of job performance. This factor includes the technical knowledge and background required to perform a job, understanding job requirements, and knowledge of how to accomplish the work efficiently in that specific work environment. For example, research by Schmidt, Hunter and Outerbridge (1986) indicates that job knowledge is a major contributor to performance.

The effects of motivation on job performance have been shown in numerous studies. Three critical components of work motivation are direction, intensity, and persistence of effort. Researchers often conceptualize these components as choices: the choice to perform, the choice of performance level, and the choice of duration of effort (Campbell & Pritchard, 1976).

Environmental constraints are a fourth major influence upon performance. Research on this class of variables has considered the effect of situational constraints and obstacles to performance. Improper tools, supplies, and equipment (Peters & O'Connor, 1980; Peters, Chassie, Lindholm, O'Connor, & Kline, 1982) are examples of constraints that affect work performance. Olson and Borman (1989) recently discussed situational constraints as one half of an environmental facilitator-constraint continuum.

In addition to specifying the major influences on performance, this model emphasizes that performance is the multiplicative result of these four factors. This implies that if any of the four factors are deficient, overall performance will be poor. For example, even if someone is highly capable of performing a job (i.e., has the required personal characteristics) and has the knowledge to perform the job, overall performance will be poor if little effort is expended or if constraints to performance are great.

Strategies for Influencing Security-relevant Behavior

This model of work performance can easily be extended to a model of security-relevant behavior.[2] Figure 1 shows how each factor can be translated into general strategies for influencing security-relevant behavior.

We have translated the model adapted from Campbell and Campbell (1988) into general strategies for influencing security-related behavior. This was done for two reasons. First, our goal in developing a model of security-relevant behavior is not to predict behavior but rather to identify factors for influencing and controlling it. Second, this type of model will provide policymakers with a better understanding of those factors which they can modify to make improvements in the continuing assessment system.

---

[2]The label "security-relevant behavior" is preferred to "security performance." Consistent with prior usage (e.g., Campbell, Dunnette, Lawlor & Weick, 1970), performance connotes behavior authorized by the organization. As later sections will discuss, the activities targeted by the personnel security program include a wide range of behavior, some of which, such as espionage, are clearly not authorized or desired by the organization.

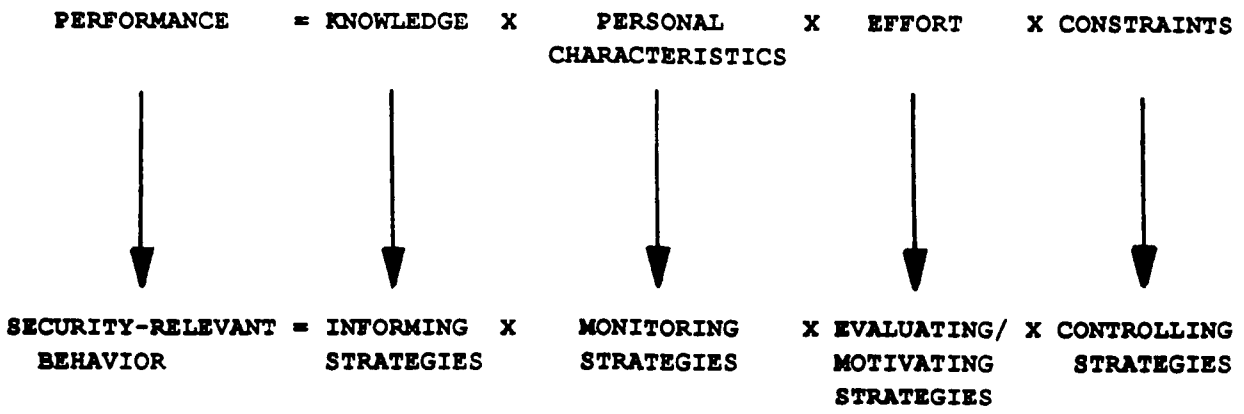

Figure 1. Strategies for influencing security-relevant behavior

The model presented in Figure 1 illustrates a simple set of relationships. In the context of personnel security, knowledge is obtained by informing personnel. This is accomplished through security education (e.g., briefings, indoctrinations, training), security awareness programs, and security counseling. More generally, this informing component includes strategies for ensuring that cleared personnel understand their security-relevant job duties and the importance of continuing assessment.

Referring to Figure 1, personal characteristics can be monitored. This is accomplished through the use of various derogatory information reporting and administrative procedures. Derogatory information reports can come from various sources (e.g., supervisors, commanders, coworkers, installation departments, outside agencies) via several reporting mechanisms (e.g., informal verbal reports, police reports, periodic reinvestigations, security interviews, polygraphs). Personal characteristics are also monitored through administrative, recordkeeping, and management information procedures that are in place to detect adverse information. To summarize, the monitoring component focuses on the sources, methods, and requirements for reporting adverse information.

The motivation of personnel can be evaluated and motivated using various administrative approaches. Cleared personnel are evaluated through procedures such as performance appraisals, inspections, and employee assistance assessments (e.g., financial or emotional/mental counseling) and, when derogatory information is obtained, through formal adjudication of the person's continuing eligibility to hold a clearance. Personnel are motivated by strategies such as sanctions (e.g., penalties, commendations), performance appraisals, and inspections. In general, the evaluating/motivating component includes the strategies for preventing or removing security risks and for maintaining the effectiveness of the continuing assessment system.

Finally, examination of Figure 1 suggests that constraints to effective security-relevant behavior can be controlled. This is accomplished through policy initiatives, administrative procedures, legal initiatives, and resource allocations. Representative examples of constraints on the continuing assessment system include position controls, access management procedures

(e.g., one-time access, limited access, downgrading access, suspending access), need-to-know requirements, legal considerations (e.g., privacy laws and freedom of information acts), and program resource allocations. More generally, the controlling component describes the administrative and legal guidelines under which the programs operate.

This model of security-relevant behavior provides a framework for describing this behavior, for diagnosing deficiencies in performance, and for identifying methods to improve in this domain. In Section 3, we apply this model to the regulations that govern continuing assessment programs to describe the general strategies used to achieve these program objectives.

Summary

This section presented a conceptual model of strategies for influencing security-relevant behavior. The model, which was adapted from a well-known model of job performance, suggests that security-relevant behavior can be influenced through the multiplicative result of four general intervention strategies--informing, monitoring, evaluating/motivating, and controlling. The informing component includes various strategies to ensure cleared personnel understand their security-relevant job duties and the importance of continuing assessment. The monitoring component focuses on the sources, methods, and requirements for reporting adverse information. The evaluating/motivating component describes the approaches available for preventing or removing security risks and for maintaining the effectiveness of the continuing assessment system. Finally, the controlling component describes the administrative and legal limitations under which the programs operate. This model provides a simple framework which will be used in subsequent sections to describe and analyze current and alternative continuing assessment programs.

SECTION 3: ANALYSES OF CONTINUING ASSESSMENT REGULATIONS

This section uses the model of security-relevant behavior developed in Section 2 to analyze the principal DoD and DCI continuing assessment regulations. We use these analyses to define the objectives of the continuing assessment program and the behavioral strategies used to achieve these objectives. We also compare these different continuing assessment program regulations to discover what changes in program details have been incorporated to adapt to variations in program context (e.g., sensitivity of the classified information).

Principal Continuing Assessment Source Documents

Two principal source documents govern continuing assessment programs in the Department of Defense: (1) the DoD personnel security program regulation, or 5200.2-R (Department of Defense, 1987) and (2) the Director of Central Intelligence Directive No. 1/14, or DCID 1/14 (Director of Central Intelligence, 1986). The 5200.2-R provides standards for access to Top Secret, Secret, and Confidential clearance information and is applicable to all DoD military, civilian, and contractor personnel (p. I-2). (Collectively, these access determinations are termed "collateral" clearances.) The DCID 1/14 outlines standards for access to sensitive compartmented information (SCI) and is applicable to all DoD military, civilian, and contractor personnel. Together. these two policy documents provide the foundation for all continuing assessment procedures in the military services.[3]

Organization of the Regulations

The major elements of the continuing assessment program regulations can be organized into the four strategies for influencing security-relevant behavior described in Section 2 (i.e., informing, monitoring, evaluating/motivating, and controlling). This organization of the contents or elements of the 5200.2-R and DCID 1/14 is displayed in Table 1.

The four general strategies for improving security-relevant behavior are listed in the first column following the criterion, security-relevant behavior. Note that monitoring is the second strategy in this model. This reflects its approximate temporal sequence in the continuing assessment program. That is, after individuals are granted a security clearance, they are first informed of their security duties, then monitored on various security-related criteria, and finally evaluated according to the security requirements of their jobs.

---

[3]It is interesting to note the comparative emphases given in the personnel security program regulations between initial clearances and continuing assessment. The portion of the DCI and DoD regulations that concern the continuing assessment of personnel is brief--3 of 19 pages in the DCI regulation and 5 of 134 pages in the DoD regulation. While the number of pages does not necessarily reflect policy emphasis, it does indicate how much specific guidance is given for implementing procedures.

TABLE 1

CONTENT OF CONTINUING ASSESSMENT REGULATIONS

CONTINUING ASSESSMENT COMPONENT	PROGRAM ELEMENT	DCI Directive 1/14	DoD 5200.2-R
SECURITY-RELEVANT BEHAVIOR	PROGRAM PURPOSE/GOALS	2	1-1
	PERFORMANCE CRITERIA		
	Security Risk	12, Annex A, 5	2-200, Appendix I
	Suitability	12, Annex A	2-200
	Security Duties		
	Agency Heads (SOIC)	6, 14a	11-101, 9-204d
	Commanders, Base		9-204a
	Commanders, Unit		8-101a, 8-101
			8-102, 3-104ab
	EAP/Social Actions		
	Security Officer		8-101
	Security Manager	10a,b	11-101h, 9-102
			3-104
	Supervisors	14b3	9-102
	Co-workers		9-104
	Individual	11	9-103
INFORMING	SECURITY EDUCATION		9-200 thru 9-204
	Briefings/Indocs	14a, AnnexC1&3	9-101a
	Training	14b2	
	SECURITY AWARENESS	Annex C2	
	SECURITY COUNSELING	14b1	
MONITORING	*Types*		
	INDICATORS	14b3	9-101b, 9-102
	DEROGATORY INFORMATION	14b	8-101
	Sources		
	REPORTS		
	Self	14b1	9-103b
	Peer		
	Supervisor	14b3	9-102
	Security Officer/Mgr		3-104c, 11-102
	Commander		8-101
	Agencies(medical,etc)		
	Military Police		
	Hotline		8-101b
	Alternative Sources (drug tests, lists of insecurities, etc)		
	Methods		
	PERIODIC REVIEWS	14b4	
	PRs	10a	9-102
	Personal History Forms	14b4, 10b, 11	
	SECURITY INTERVIEW		
	POLYGRAPH (CI scope)		2-505
	Admin		
	COORDINATION	14b4	9-100
	RECORDKEEPING	14b4	9-203b
	MANAGEMENT INFORMATION		11-102
EVALUATING/ MOTIVATING	ADJUDICATION	12, Annex A	6-100 to 103
	Suspend/Revoke	14	8-102, 8-103
	SANCTIONS		
	Penalties		
	Awards/Commendations		
	EAPs	14b1	9-101B, 9-102
	PERFORMANCE REVIEWS		9-102d
	INSPECTIONS	14b4	11-101a3, 11-103
CONTROLLING	POSITION CONTROL		Chap 3
	ACCESS MANAGEMENT		
	One time access		3-407
	Suspend access		8-102
	Limited access (LAAs)		
	Downgrade/withdraw		7-103
	NEED-TO-KNOW	4b	7-102
	INDIVIDUAL'S RIGHTS	13, Annex B	8-200&201, 6-201.1 8-301, Chap10, 2-503

The specific program or content elements of the 5200.2-R and DCID 1/14 are presented in Column 2 of Table 1. These content elements were sorted by the first author into one of the five general components of the model using a rational sorting procedure.[4]

This approach is useful for identifying and describing the general meaning and structure of continuing assessment programs in behavioral terms. It is also useful for assessing the adequacy of current continuing assessment program elements for influencing security-relevant behavior and achieving program objectives.

The last two columns of Table 1 reference the element's chapter and section number in the 5200.2-R (column 3) or DCID-1/14 (column 4). Scanning through the pattern of references within each category in Table 1 provides a general sense of the emphases of these two continuing assessment programs.

We now provide a more detailed examination of these elements in terms of the model of security-relevant behavior presented in Section 2. The discussion is organized according to the five components of the model, and includes a general discussion of regulation elements followed by an examination of the most important differences between the 5200.2-R and DCID 1/14.[5]

Security-relevant Behavior: Components of the Work Performance Model

Security-relevant Behavior

General discussion. The strong but implicit assumption of both regulations (5200.2-R; DCID 1/14) is that the primary objective of personnel security is to prevent, or at least reduce, the compromise of classified information. For example, the 5200.2-R states that its purpose is to ensure that an individual's access to classified information is "clearly consistent with the interests of national security" (p. I-1). The standard for achieving this purpose is "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

---

[4]The reader should keep in mind that this organization of continuing assessment regulation elements is for heuristic purposes only. Some elements could be classified into more than one category depending upon their use. For example, inspections can serve as a means of motivating performance, informing personnel, or monitoring performance.

[5]Although tempting, it is misleading to use this approach to make precise comparisons between the 5200.2-R and DCID 1/14, or between any of the other program regulations discussed in this report. Such detailed comparisons are not appropriate since the regulations are organized differently, written at a general level, and may exclude more detailed information contained in supporting regulations. These regulations also reflect DoD mandates which in some cases have not yet been fully integrated in practice (due to the level of effort or resources required). For these reasons, precise comparisons between continuing assessment programs are more appropriately made on the basis of field research which describes the operational programs. This research has been conducted and is presented in Report 2 (Bosshardt, DuBois, & Crawford, 1991) of this series.

clearly consistent with the interests of national security" (p. II-1). This standard is operationalized as several separate adjudication areas. The adjudication areas for the 5200.2-R and the DCID 1/14, as well as for three alternative programs (which will be discussed in Section 4) are presented in Table 2.

A review of the adjudication areas shown in Table 2 and of the responsibilities described in the personnel security program regulations suggests that there are three broad, conceptually distinct categories of security-relevant behavior, rather than a single category. The first category includes unacceptable, security-relevant behaviors that indicate security compromise has occurred or contribute to the increased risk of security compromise. Representative activities for this category include espionage, unauthorized disclosure of classified information, disloyal activities, security violations, falsification of security-related information, and associations with foreign nationals from designated countries.

The second category of security-relevant behavior consists of negative actions that represent general unsuitable conduct. Representative behaviors for this category include drug use, excessive alcohol use, sexual misconduct, financial irresponsibility, unreliable behavior, and criminal activities. Behaviors in this category have a less direct link to possible security compromise.

A final category of security-relevant behavior includes the dereliction of security duties. This includes the failure to perform security activities such as reporting relevant derogatory information, checking identification cards, keeping classified documents locked at night, or discussing classified information only in secure areas. In addition to the one adjudicative criterion that includes performance of security duties, much attention is given in the program regulations to specifying security-relevant responsibilities. The focus of these activities is on maintaining the integrity and vigilance of personnel in the security system.

It is essential to understand the interrelationships among these different criteria and their relationships to the compromise of sensitive information. For example, do suitability behaviors predict later compromise risk? Does ineffective performance of security duties increase the risk of security compromise? If so, to what extent? Understanding the relationships between these criterion areas is important for several reasons--developing effective continuing assessment policies, developing operational procedures, describing the components of current continuing assessment systems, assessing the appropriateness of continuing assessment program components and elements, and evaluating the effectiveness of the continuing assessment system as a whole. This difficulty in defining and understanding the criteria of interest is known by applied psychologists as the "criterion problem" (Dunnette, 1963; Campbell & Campbell, 1988). The design and implementation of appropriate continuing assessment program elements depend upon clearly specifying and understanding the behavioral criteria which are to be managed.

TABLE 2
ADJUDICATIVE CRITERIA FOR SELECTED CONTINUING ASSESSMENT PROGRAMS

	DCI-D 1/14	DOD 5200.2-R	Personnel Security Assurance Program	Personnel Reliability Program	Space Human Assurance and Reliability Program
POSSIBLE SECURITY COMPROMISE	Loyalty Close relatives & associates Security violations Outside activities	Loyalty Foreign connections Disregarding security safeguards Foreign preference Falsification Refusal to answer	Loyalty Close relative & associatives Security violations Outside activities Falsification Refusal to answer		Disregarding security safeguards Noncompliance w/ requirements
POTENTIAL UNSUITABILITY	Sexual misconduct Undesirable character traits Financial irresponsibility Alcohol abuse Illegal drugs/ drug abuse Emotional/mental disorders Record of law violations	Sexual misconduct Falsification Financial matters Alcohol abuse Drug abuse Emotional/mental disorders Criminal conduct	Reliability (sexual misconduct, criminal conduct, financial problems) Alcohol abuse Drug abuse Emotional/mental/ medical disorders	Reliability alertness physical competence dependability flexibility stability sound judgment in emergencies positive attitude toward nuclear weapons duty Alcohol abuse Drug abuse Emotional/mental medical disorders Criminal conduct	Sexual misconduct Financial matters Alcohol abuse Drug abuse Emotional/mental medical disorders Criminal conduct
FAILURE TO PERFORM SECURITY DUTIES	Security violations	Disregarding security safeguards		Poor attitude/lack of motivation	Disregarding security safeguards Workplace behavior

An example may clarify this general point. Selling secrets to a designated country could result from access to important information (constraints), the choice to divulge it to foreign agents (motivation), knowledge of the means for doing so (knowledge), or the need for money arising from a divorce and/or disgruntlement with the employing organization (personal characteristics). This instance of espionage might have been prevented by a supervisor who was vigilant and conscientious in monitoring an employee's behavior (personal characteristics), was well trained to identify indicators of security risk (knowledge), referred the employee for employee assistance (motivation), or temporarily removed the employee from access to sensitive information until the personal crisis had been resolved (constraint). As illustrated in this example, each of the major contributors to performance (i.e., personal characteristics, knowledge, motivation, constraints) may differ in terms of the content of the variables considered and the strategies that impact these variables, based upon whether the focus is decreasing security compromises, managing unsuitable behavior, or performing security duties.

Comparison of DoD and DCI regulations. Examination of Table 2 indicates that the adjudicative criteria for the 5200.2-R and DCID 1/14 are very similar. Where differences appear (e.g., the DCID 1/14 lists "outside activities" whereas the DoD 5200.2-R lists "foreign preferences," "falsification," and "refusal to answer"), examination of the regulations shows that the behavioral contents are actually quite similar, but are organized into a somewhat different criterion cluster or have a different label. The 5200.2-R, however, does give greater specificity to its criteria by providing behavioral anchors ("disqualifying factors").

Informing

General discussion. The informing component of continuing assessment involves communicating to cleared personnel their security requirements and responsibilities. This includes such program elements as security education (e.g., security briefings, indoctrinations, training), security awareness, and security counseling. In general, these activities are intended to inform individuals of: (1) the purpose and need for security, (2) the mission of the department or organization, (3) the correct handling of classified information, (4) the indicators which signal matters of security concern, (5) "need-to-know" procedures, (6) foreign intelligence recruiting techniques, (7) prohibitions against disclosing classified information, (8) the penalties for security violations, and (9) ways of handling personal problems that are significant from a continuing assessment perspective. Briefings are mandated in special situations, such as travel to restricted countries (e.g., Soviet bloc countries), termination of employment, or employment absences of more than 60 days.

This component also includes specification of the responsibilities of various parties for ensuring personnel security. For example, commanders and heads of organizations are required to ensure that all cleared personnel receive initial indoctrination and periodic follow-up briefings on their individual security responsibilities (Department of Defense, 1987, p. ix-1).

Comparison of DoD and DCI regulations. There are three noteworthy differences in the informing component of the DoD and DCI regulations. First, the DCI regulation appears to give more emphasis to security awareness because it emphasizes adapting the program to meet the needs of the department and using current information and materials. Second, the DCID

1/14 mandates that personnel with SCI access receive security counseling from experienced security personnel when personal problems arise which have bearing upon their continued eligibility for access. Finally, for initial briefings, the DCI regulations specify informing cleared personnel about determining need to know before disseminating classified information.

Monitoring

General discussion. The monitoring component of the continuing assessment program focuses on procedures for gathering and reporting security-relevant information. The personnel security program regulations contain requirements for reporting information relevant to each of the three categories of security-relevant behavior: possible security compromise, potential unsuitability, and failure to perform security duties. For example, individuals must report attempts by foreigners to obtain sensitive information, report any contact with individuals from designated foreign countries, and report in advance any personal foreign travel. With respect to potential unsuitability, violations of security standards for alcohol and substance use, financial irresponsibility, sexual misconduct, criminal behavior, etc., must be reported to the unit commander or security office. Regarding failure to perform security duties, supervisors are often required to report the adequacy of the performance of these duties on subordinates' annual performance reviews.

The principal methods cited by the regulations for gathering this information are reports by cleared personnel, their supervisors and commanders on an as-needed basis, and the periodic completion of a personal history questionnaire by each cleared person with a top secret clearance or SCI access. When the periodic reinvestigation is being initiated, supervisors must review their subordinates' personal history statements and report any adverse information of which they are aware. Limited provisions are also made for using the polygraph as a method of discovering counterintelligence information.

The major sources of security-relevant information are cleared personnel, their supervisors and commanders. The regulations also indicate that information should be gathered from representatives from the personnel, medical, and legal departments (who usually provide relevant information to commanders) and that alternative means of gathering derogatory information (e.g., hotlines) should be used.

Administrative requirements for summarizing and reporting statistics relevant to personnel security include compiling information on the numbers and types of clearances issued, denied, and revoked, and the numbers and types of clearances and access authorizations currently in effect. This information is aggregated at several organizational levels (installation or command, major command, branch of service) and is reported annually to the Deputy Under Secretary of Defense (Security Policy).

Finally, it is important to note that although both regulations contain detailed information describing the adjudicative criteria, neither document provides explicit instructions for determining what individuals should report. For example, financial irresponsibility is an adjudicative criterion, but the level of detail and types of circumstances to report are not well specified.

Comparison of DoD and DCI regulations. For the monitoring component, the DCI regulations are somewhat more stringent than the DoD regulations. The DCI regulations emphasize a security review program to ensure that security-relevant information is exchanged in a timely manner, personal history information is kept up-to-date, and security files are continually reviewed. In addition, all SCI personnel (vs. only personnel with Top Secret clearances in the collateral program) are subjects of periodic reinvestigations every 5 years.

Evaluating/Motivating

General discussion. The regulations provide approaches for evaluating security-relevant behavior. Derogatory information relating to the possible compromise of classified information or to unsuitable conduct is referred to central adjudication for evaluation and possible administrative actions. The heads of DoD components are encouraged to provide programs to assist cleared personnel with personal problems (e.g., financial, medical, or emotional difficulties). The purposes of these employee assistance programs (EAPs) are to identify potential problems at an early stage, to help neutralize any vulnerability with respect to security, and to prevent long-term, job-related security problems.

There are approaches cited in the regulations for motivating and managing the performance of security-relevant responsibilities. Supervisors are required to comment upon subordinates' discharge of their security responsibilities on their regularly scheduled fitness and performance reports. The heads of DoD components are charged with the responsibility of including the personnel security program in their administrative inspection programs. Penalties or commendations may also be provided in certain cases.

Comparison of DoD and DCI regulations. Few differences for the evaluating/motivating component of the DoD and DCI continuing assessment regulations emerge directly from content analyses of the regulations. For example, both regulations emphasize the "whole person" concept for adjudication, although there is often limited information available on the positive aspects of the person. That is, fair and uniform evaluations must be based upon careful consideration of the recency, frequency, and mitigating circumstances of any derogatory information. However, this is probably the most significantly different component in practice. Field personnel report that the standards for minimum acceptable behavior are substantially higher for adjudicating SCI personnel. Other important operational differences are discussed in Report 2 of this series (Bosshardt et al. 1991).

Controlling

General discussion. Numerous constraints play an important role in the continuing assessment program. These constraints can be organized and discussed in two general classes: access controls and legal controls.

Access controls can take several forms. Position controls are set to minimize the number of persons with access/clearances. Even after an individual receives a security clearance, access to sensitive information is only granted on a need-to-know basis. Clearance levels can be administratively downgraded or access eligibility can be withdrawn when regular access is no longer required. One-time access above one's clearance level can be granted, as well as authorization for limited access. When significant adverse information is identified, security clearances can be suspended or revoked.

Several laws constrain continuing assessment programs. Laws protecting the personal rights and freedoms of individuals granted by the Constitution limit the methods and types of information that can be collected and the actions that can be taken. For example, rights to due process and privacy are addressed in continuing assessment programs to ensure fair and timely personnel decisions. Other laws provide administrative remedies and penalties for the unauthorized disclosure of classified information and for unsuitable conduct (i.e., driving while intoxicated, financial irresponsibility, theft or violence, etc.).

Comparison of DoD and DCI regulations. There are no major differences in constraints that are apparent from content analyses of the personnel security regulations. In other security institutions and in practice, however, there are several additional procedures, related to information and physical security, to ensure the security of SCI personnel and information. For example, the "two-person" rule (which requires that a second person is present anytime that SCI information is accessed), is enforced for SCI information. The need-to-know is carefully managed through compartmentation of information, and accountability for all documents. Finally, physical security is more stringent for facilities containing SCI information, including the use of special ID badges and strict access monitoring and control.

Other Differences in DoD and DCI Continuing Assessment Regulations

The general types of derogatory information collected in personnel security investigations are very similar for all levels of clearance. (See Table 2 for a complete list of derogatory information areas.) However, the scope and level of investigative effort increase with the level of clearance requested (see 5200.2-R, pp. III-6ff), as does the threshold for acceptable behavior. For example, to receive a secret clearance, a check of the records of several national organizations is conducted, including FBI records and fingerprint checks, Defense Central Index of Investigations (DCII), and possibly State Department records. Requirements for a Secret clearance for civilians extend these national agency checks to include written inquiries to previous employers covering a period of the last 5 years. Investigative requirements for a Top Secret clearance extend this coverage to include a credit check, a check of local law enforcement agencies and interviews with the subject, employment references, and character references. Finally, SCI access extends investigative coverage from a period of 5 years previous to 15 years, in addition to other special investigative coverages.

As mentioned previously, the content analyses of DoD and DCI regulations are inadequate for comprehensive comparisons between the collateral and SCI programs. Examination of operational similarities and differences for SCI access and collateral clearances are provided in Report 2 of this series.

The above discussion has focused on differences between SCI access and collateral clearances. However, it should be noted that there are few differences in continuing assessment program features among collateral level clearances. Aside from the differences in investigative requirements, the most significant difference is that periodic reinvestigations are conducted every 5 years for personnel with Top Secret clearances, but not for personnel with Secret clearances.[6] However, DoD is now initiating a limited number of update investigations for personnel with Secret clearances.

It should be noted that level of clearance access is only one of several contextual variables that might impact a continuing assessment program. Other possible variables include the nature of the local security threat, size of the local organization, and the specific vulnerabilities associated with demographic characteristics of the local cleared population (e.g., higher prevalence of criminal behavior among the youth, more bankruptcies among older personnel). None of these factors, however, is explicitly addressed in the continuing assessment program regulations. Future research is needed to assess the importance of these and other potential threats to continuing assessment program effectiveness.

Summary

The DoD and DCI regulations relevant to continuing assessment imply three distinct categories of security-relevant behavior: possible security compromise, potential unsuitability, and failure to perform security duties. To manage these behaviors, the regulations describe a range of continuing assessment activities that can be organized into program components of informing, monitoring, evaluating/motivating, and controlling. The informing component includes various educational activities to ensure that cleared personnel understand their security-relevant job duties and the importance of continuing assessment. The monitoring component focuses on the methods and requirements for reporting adverse information. The evaluating/motivating component describes the methods available for preventing or removing security risks and for maintaining the effectiveness of the continuing assessment system. Finally, the controlling component describes administrative and legal limitations under which the programs operate.

The DoD and DCI continuing assessment program features were compared. Results of this content analysis indicated that the regulations are very similar. However, several important features were found to distinguish continuing assessment programs for sensitive compartmented information (SCI) from collateral programs. These include differences in security counseling, security review, adjudicative standards, and access procedures.

---

[6]Although not discussed in this report, it should be noted that the basic content and behavioral approach of the continuing assessment programs for the Army, Air Force, and Navy are quite similar. This is not surprising since the 5200.2-R serves as the minimum requirement and guiding document for each military service branch regulation. Report 2 will provide detailed comparisons of the operational similarities and differences across these three military branch continuing assessment programs.

SECTION 4: ALTERNATIVE CONTINUING ASSESSMENT PROGRAMS

In this section we examine four alternative continuing assessment programs. These programs are oriented toward the identification of unreliable and unsafe job behavior. The section begins with a brief overview of these alternative programs. We then identify and discuss unique features of these alternative programs that might be incorporated into the DoD continuing assessment program.

Alternative Continuing Assessment Programs: General Overview

Descriptions of four personnel reliability programs with substantial continuing assessment components were examined. These programs were: (1) the Personnel Security Assurance Program (PSAP, known formerly as the Human Reliability Program), (2) the Personnel Assurance Program (PAP), (3) the Personnel Reliability Program (PRP), and (4) the Space Human Assurance and Reliability Program (SHARP). The PAP and PSAP are Department of Energy programs, whereas the PRP is a Department of Defense-wide program, and the SHARP is an Air Force effort. It should be noted that the PSAP is a proposed program while the SHARP is currently in the process of being implemented. Both programs could change prior to final implementation. The PAP, PSAP, and PRP were each designed to prevent accidents, loss, or inappropriate use of nuclear weapons, materials, or systems.[7] The SHARP was designed to minimize the risk of space launch and mission failures due to unreliable personnel. The PRP covers primarily military personnel, whereas the other three programs involve primarily contractor civilian personnel. Although these programs differ in purpose from the DoD personnel security program, many of the procedures used in these programs are relevant to continuing assessment programs in the military services.

The basic structure for these four alternative programs is similar to the DoD personnel security program--they each focus upon an initial investigation into certain behavioral criteria with adjudicative procedures for granting clearances, and contain continuing assessment procedures for evaluating the ongoing reliability of personnel.

Table 2, which was presented earlier, lists the adjudication areas for the PRP, SHARP, and PSAP programs, along with those for the 5200.2-R and DCID 1/14. A quick perusal of this table suggests there is considerable overlap in these adjudication areas, although there are noteworthy differences as well. For example, the PSAP does not include security duties criteria. The PRP does not include security compromise criteria, but places more emphasis on suitability

---

[7]These programs are described in Human Reliability Program Development in the Department of Energy (Enns, 1988). The PSAP is also described in An Overview of the Personnel Security Assurance Program (Center for Personnel Security Assurance, Research and Analysis, 1988) and in several Department of Energy brochures and programs, and briefing documents. It should be noted that an initial version of Space Systems Directive (SSD) 55-3 was examined for this report. The SSD 55-3 has now been formally issued by the Space Systems Command.

TABLE 3: CONTENT OF ALTERNATIVE CONTINUING ASSESSMENT PROGRAMS

CONTINUING ASSESSMENT COMPONENT	PROGRAM ELEMENT	PAP 5610.3	PSAP (HRP) 5631.6	PRP (1985) 5210.42	SHARP (1988) SSD 55-3 Draft
	PROGRAM PURPOSE/GOALS	II-1a	1,5a,9	A,D1,D12	1,3,4e3
	PERFORMANCE CRITERIA				
	Security Risk	Chap I	10 CFR 710	Enclosure 4	Attachment 2
	Suitability	Chap I	10 CFR 710	Enclosure 4	Attachment 2
	Security Duties				
	Agency Heads (SOIC)		8b&h	E2	
	Commanders, Base		8f&i		
SECURITY-RELEVANT BEHAVIOR	Commanders, Unit	II-3a,4a			4a&b
	EAP/Social Actions	II-3a,4a&b,2e	8d,e&j	5C	4i&l
	Security Officer		8h		4l,5e&f&g
	Security Managers				4p
	Supervisors	II-3b,4b	8k	5C2	4o,5c&d
	Co-workers				
	Individual	II-3a2	8l	5C4	4e2,4q,5b
	SECURITY EDUCATION	II-3a1	8b5,8c3,8d3,11a		5a
	Briefings/Indocs		10a4a2	5A4	
	Training		10a4b3	2-1&2	
INFORMING	Materials				
	SECURITY AWARENESS				
	SECURITY COUNSELING				
	Types				
	INDICATORS		10a4b		
	DEROGATORY INFORMATION	II-3b	10a4b	D12,5C2	5a
	Sources				
	REPORTS				
	Self			5C4	4q
	Peer				
	Supervisor		10a4b	5C2	4o6
	Security Officer/Mgr				4p4
	Commander				
	Hotline				
MONITORING	Medical/EAP/Personnel		10b,10a2	D10,2-3&4,5A2	
	Alternative Sources		8i2	5C1&3	
	(drug tests, lists of insecurities, etc)		10a1c,10c		
	Methods				
	PERIODIC REVIEWS		10a4a,10c		
	PRs				
	Personal History Forms				
	SECURITY INTERVIEW			D11,5A4	
	POLYGRAPH (CI scope)				
	Admin				
	COORDINATION				4b11
	RECORDKEEPING	II-7	11c	5C1	8a&d,9a
	MANAGEMENT INFORMATION		8b4	G, 6, 2-9	
	ADJUDICATION			D7	7
	Suspend/Revoke			5D	
	SANCTIONS				
	Administrative Chgs	II-3a&b,6	10d3&4	5D3	10
	Awards/Commendations				
EVALUATING/ MOTIVATING	EAPs				
	PERFORMANCE REVIEWS		10d2		
	INSPECTIONS		11b	E1c,F4	13b
	QUALITY CONTROL		11b	2-12	
	POSITION CONTROL		9		
	ACCESS MANAGEMENT				
	One time access				
	Suspend access	II-3a6&7	10a4c	4C3,5D2	8
CONTROLLING	Limited access (LAAs)				
	NEED TO KNOW				
	INDIVIDUAL'S RIGHTS	II-5	11c	5D,5E	6,7f3,9b&d
	RESOURCES			E2	

criteria than the DoD and DCI programs. The SHARP gives less emphasis to security compromise criteria than the DoD and DCI programs, but more emphasis to security duties criteria. These differences reflect the greater emphasis on personnel safety and reliability in these programs.

Although a primary focus of each alternative program is on initial screening, each program does include a substantial continuing assessment component. The continuing assessment component varies across these programs, as do the behavioral standards used, according to the special purposes and circumstances involved with each program.

Table 3 presents a graphic summary of the content elements of each of the four alternative programs. These can be compared to the elements in the 5200.2-R and DCID 1/14 shown in Table 2. Overall, the specific content elements in these alternative programs are quite similar to those in the DoD and DCI programs. However, the alternative programs do contain some unique features which might be considered for inclusion into the DoD continuing assessment program.

These unique features are listed below according to the five areas of our security-relevant behavior model.

Model Components

Security-relevant Behavior

Unique security-relevant behavior measures that are included in one or more alternative programs include:

- Physical illness/incapacity is included as a performance criterion. [SHARP]
- Workplace behavior is included as a performance criterion. [SHARP]
- Noncompliance with processing requirements is included as a performance criterion. [SHARP]
- Failure to meet certification criteria is non-punitive and does not adversely affect an individual's career; if derogatory information is uncovered, the individual is transferred to another job for which he or she is qualified with no damage to his or her career nor negative remarks in his or her personnel records. Where the derogatory information is punishable under other regulations such as the Uniform Code of Military Justice, penalties are assessed according to these regulations. [SHARP]

- Detailed specifications of continuing assessment responsibilities are provided to medical and legal personnel. [SHARP; PSAP] More specifically,

  - responsibilities for medical personnel include serving on the program advisory board, evaluating medical and dental records, conducting annual examinations, and making recommendations concerning the reliability of personnel.

  - responsibilities for legal personnel include serving as members and legal advisor to the advisory board, reviewing all suspension and denial/revocation notices, and coordinating responses to Freedom of Information requests, Privacy Act requests, or Congressional inquiries about the program.

Informing

One unique procedure relevant to the informing component that is included in the SHARP program is:

- Certified personnel are told what the reliability criteria are and how adjudication is done. [SHARP]

Monitoring

Unique monitoring procedures in one or more alternative programs include:

- An initial medical examination is required. [PRP]

- Medical and dental records of certified individuals are specially marked to ensure that any treatment (e.g., medications) that might affect their alertness is recorded and that appropriate personnel are notified. [PRP]

- Certified individuals who are absent from work for more than 5 consecutive days due to illness must receive recertification by a physician before returning to work. [PSAP]

- An annual medical examination, which includes screening for alcohol and drug abuse, is required. [PSAP]

- Annual updates of the personal history questionnaire, credit checks, and national and local criminal records checks are required. [PSAP]

Evaluating/Motivating

Unique evaluating/motivating procedures included in one or more alternative programs include:

- An annual review of each certified individual is performed; this review includes: (1) a review of work performance, (2) a medical assessment, (3) a management evaluation, and (4) a national agency check, and (5) a review by the approving official. [PSAP]
- Administrative procedures are used which permit temporary reassignment of suspended personnel. [PSAP; PRP]
- Program quality assurance provisions which include programmatic reviews, field office surveys, and management audits are conducted. [PSAP]

Controlling

Unique controlling procedures used in one or more alternative programs include:

- An extensive and detailed specification of the rights of certified individuals is provided [PAP]. For example,
- Individuals are provided with the right to counsel for revocation or denial hearings.
- Individuals are allowed to call witnesses on their behalf.
- Individuals are allowed to cross-examine witnesses testifying against them.
- All files sent for adjudication are anonymous (to ensure fair and consistent rulings and to protect the identity of the person). [SHARP]
- The "two-person" rule is used (this rule requires that all handling of nuclear materials, systems, or components must be done with at least two persons)[8]. [PRP]
- A quality control check is conducted on the appropriateness of the positions that are certified; this review determines if more restrictive administrative or physical controls should be used for removing some positions from the roster of critical positions. [PSAP]

---

[8]It should be noted that the two-person rule is a part of the SCI program regulation, but is not a part of the collateral program regulation.

- Procedures to ensure the program is legally defensible and sensitive to individual rights of privacy and due process, [PSAP] such as:
  - The personnel security clearance process is conducted by government (vs. line) officials.
  - No new security clearance criteria are introduced for the PSAP program that are additional to their existing and well-tested security program.
  - The appeals procedures provided by existing Department of Energy (DOE) regulations are used rather than other administrative procedures.
  - The process provides for temporary reassignment, should it be necessary.

Other Considerations

Enns (1988) noted that the ultimate responsibility for the reliability of personnel rests with the personnel security office in the PSAP and with the operations commander in the PRP. For the PSAP, this removes the potential conflict of interest that confronts supervisors and commanders in PRP (i.e., denying or revoking a clearance negatively impacts operational efficiency). Additionally, the PSAP has more stringent investigative requirements than the PRP (an SBI vs. NAC or BI). The PSAP medical assessment is more thorough, including screening for alcoholism and a psychiatric evaluation.

Another unique feature of the PSAP is the use of a single set of security criteria, applied across the board to persons in a wide range of positions. This approach "will ensure a more consistent implementation of the program and avoid many issues of equal protection and privacy which would otherwise result" (Center for Personnel Security Assurance, 1988, p. 4).

Summary

Four personnel reliability programs (PAP, PSAP, PRP, SHARP) were reviewed, using the model of security-relevant behavior, to identify features that might be incorporated into the DoD continuing assessment program. Several possible features were identified. The most promising include: informing personnel about adjudicative criteria, continuing assessment procedures, and assistance available for personal problems; a thorough annual review (including medical screening, a NAC, and a local agency check); non-punitive personnel actions; and controls to ensure individual rights (e.g., having counsel at hearings, anonymous files for personnel decisions).

SECTION 5: LITERATURE RELEVANT TO CONTINUING ASSESSMENT

In this section we review literature relevant to continuing assessment. The section begins with a summary of the literature search procedures, followed by a brief discussion of the nature of the personnel security problem and its relationship to continuing assessment. Relevant literature is then discussed in terms of the model of security-relevant behavior presented in Section 2. Where appropriate, the discussion is augmented by ideas and approaches suggested by research in selected areas of industrial/organizational psychology. The section concludes with a discussion of other considerations pertinent to continuing assessment (e.g., cost/benefit considerations).

Literature Search Procedures

The literature search included examination of the security and psychological literatures, and included both scientific and applied perspectives. Computer searches of the psychological (PsychInfo) and technical (NTIS) literature were conducted. Telephone calls were made to security personnel and researchers in several DoD organizations. Bibliographies of relevant documents were also examined for additional sources.

The literature that is directly relevant to continuing assessment is small and consists primarily of narrative program descriptions, management analyses, and informed opinion. No empirical studies were found. The documents located can be organized into two groups--presentations and reports that directly address continuing assessment, and general reviews of the overall personnel security program which include discussions of continuing assessment (e.g., commission reports, Congressional hearings).

Literature Review Component Areas

Personnel Security Problem

One topic discussed in several reports is the need for a better definition of the nation's security problem. The Stilwell report (DoD Security Review Commission, 1985) noted the lack of information available upon which to base security policy and procedures. Builder, Jackson, and Starr (1988, p.viii) state that "theories about the information to be protected, human behavior, the processes that can lead to the loss of secrets, and the value of the secrets are limited, implicit, and mostly unvalidated." They devoted much of their report to this fundamental issue, citing the advantages of a solidly researched and well-defined problem. They suggested that a precise description of the security problem is the source from which program goals and strategy are set. This problem description also provides the basis for: evaluating the effectiveness of program procedures; assessing cost effectiveness; examining the relative emphases given to information, physical, and personnel security; and exploring alternative procedures, programs, and the tradeoffs among them.

Security-relevant Behavior

Related to the need for defining the personnel security problem, a major theme of this report is the need for more precise definition and understanding of the target criteria for continuing assessment programs. Earlier, three broad categories of security-relevant behavior were identified: possible security compromise, potential unsuitability, and failure to perform security duties. We now further explore these categories to detail the complexities of the criterion problem and to suggest how more precise knowledge of the interrelationships among these criteria can be used to improve continuing assessment programs.

Security Compromise Criteria. Throughout this report, security compromise has been treated as a single, general dimension of security-relevant behavior. This broad categorization includes several classes of distinct behavior. For example, compromise due to inattentive disposal of classified documents or careless telephone conversations can readily be distinguished from compromise due to espionage. Builder et al. (1988) discussed the possibility that espionage actually consists of several dimensions, each linked to a different theory of spying. They listed seven possible theories for espionage (including foreign preferences theory, ties theory, trait theory, situation theory, incentive theory, expectation theory, and moral ambiguity theory), each of which is supported to some degree by case histories. They suggested that these theories dictate different policies and strategies for reducing espionage. For example, foreign preferences and ties theories suggest the efficacy of procedures such as background and affiliation checks. Trait and situation theories indicate that assessing attitudes might be useful. Incentive theories suggest the usefulness of monitoring financial changes. Other classes of security compromise, such as carelessness, probably also require different approaches for reducing security risks.

The analysis above illustrates the need for basic research to identify the number and structure of behavioral dimensions underlying security compromise, and the prevalence of each type of compromise and personnel security risk in the cleared population. This research should also identify the optimum strategy, methods, and intervals for collecting this information on an ongoing basis. The history of post-World War II espionage indicates that the motivations and methods of unauthorized disclosure of sensitive information can change dramatically (Wood, Herbig, & Lewis, 1990). This information is required to ensure that continuing assessment programs adapt to these changing threats in an effective and timely way.

Suitability Criteria. The personnel security program regulations list several diverse suitability criteria, including financial irresponsibility, substance abuse, sexual misconduct, and criminal behavior. Although little is known about the relationships of these criteria with security compromise, some research has examined work-related reliability in sensitive settings. For example, Dunnette, Bownas, and Bosshardt (1981) identified 18 dimensions of job behavior related to employee reliability in nuclear power plant settings. These researchers developed behavioral rating scales for each of these dimensions and had nuclear power plant supervisors use these scales to rate 58 operators who had shown unstable job behavior. A factor analysis of the data yielded 6 dimensions of unreliable job performance: hostility toward authority, irresponsibility/impulsiveness, defensiveness incompetence, psychopathology, compulsive incompetence, and substance abuse.

The methodology used by Dunnette et al. (1981) offers two valuable points for continuing assessment researchers. First, it provides a simple approach for identifying the relationships among security-relevant criteria. As Barge, Hough, Dunnette, Kemery, Kanfer, Kamp, and Cardozo (1984, p.139) state in their review of the literature on behavior unreliability, "only by identifying the behaviors that precede or demonstrate unreliability in a particular organization can optimal selection and monitoring take place." Second, this methodology provides a rich source of behavioral information that can be used for developing effective continuing assessment procedures. For example, it can be used in developing assessment forms for monitoring key behaviors of cleared personnel or in developing early warning indicator lists for supervisors. It can also provide valuable information for training needs analyses for security staff or cleared personnel.

Security Duties Criteria. Performance of personnel security duties also involves a diverse, complex set of behavioral dimensions. While no research or job analyses could be located which directly address personnel security duties, this point is illustrated by Houston's (1989) study of the physical security job duties of Marine security guards. She identified 15 job performance dimensions and 10 personal characteristic dimensions, along with representative behaviors for each dimension/area. These are shown in Table 4. Similar job analysis efforts are needed to systematically describe the behaviors required for performing continuing assessment duties. Results of these efforts would provide a basis for improving the selection, training, and performance management of personnel security staff.

Other Considerations. Several reports recommended basic research to define and explicate security criteria (e.g., Abbott, 1987; DoD Security Review Commission, 1985; Builder et al., 1988; United States Senate, 1985). Such knowledge provides the necessary foundation for developing useful policies and for developing effective operational procedures in several areas (e.g., for screening personnel, providing comprehensive training, assessing job performance, rewarding effective performance). Abbott (1987) discussed the practical difficulties experienced by security personnel when the criteria are not sufficiently specified. One important consequence is that commanders and supervisors do not know what derogatory information to report, and consequently, fail to report relevant information.

Some researchers (Flyer, 1986; Builder et al. 1988) have also discussed the inappropriateness of combining security compromise and suitability criteria within the personnel security program. They suggest that combining these criteria may result in confused program priorities or neglect of one criterion area. Accountability for achieving program objectives may drift when different objectives become confounded.

TABLE 4

JOB PERFORMANCE DIMENSIONS FOR MARINE SECURITY GUARDS
J. S. Houston (1989)

Job Performance Categories	Personal Characteristics
CONTROLLING ACCESS o Makes positive identification o Prevents unauthorized entries	INITIATIVE/LEADERSHIP o Is persuasive & influential o Takes initiative
PERFORMING SECURITY INSPECTIONS o Performs thorough inspections o Initiates investigations	MOTIVATION/EFFORT o Sets high standards & achieves them o Persists frustrating situations
ESCORTING PERSONNEL o Escorts visitors o Monitors visitor activities	COOPERATIVENESS o Willing to work with others o Is a good team player
MAINTAINING LOGS/WRITING REPORTS o Keeps accurate, detailed log o Keeps logs up-to-date	SOCIABILITY o Is friendly & pleasant o Is outgoing
MAINTAINING ALERTNESS. o Is aware of suspicious activities o Sets correct priorities	EMOTIONAL STABILITY o Maintains calm in stressful situations o Is well adjusted
USE OF WEAPONS o Uses safe weapons procedures o Uses weapons only when appropriate	MATURITY/SELF-DISCIPLINE o Behaves responsibly o Exercises self-control
REACTING TO EMERGENCIES o Reacts quickly & effectively o Gives clear, complete information	HONESTY/INTEGRITY/ETHICS o Has high moral standards o Has strong sense of fairness
ADDITIONAL DUTIES o Performs extra duties conscientiously	DEPENDABILITY o Is timely & reliable o Respects laws & regulations
PHYSICAL FITNESS o Maintains physical condition	ATTENTION TO DETAIL o Is observant & alert o Attends to small details
PERSONAL APPEARANCE o Maintains well-groomed appearance o Wears proper attire	ADAPTABILITY o Adapts readily to new environments o Copes well with difficulties
KEEPING OTHERS INFORMED o Notifies others promptly	
INTERACTING WITH OTHERS o Acts in a firm but courteous manner o Handles confrontations calmly	
DRINKING BEHAVIOR o Drinks responsibly	
LIBERTY BEHAVIOR o Respects local regulations & customs	
OVERALL PERFORMANCE	

Informing

Security training and education programs play a pivotal role in continuing assessment effectiveness (Crawford, 1988). Personnel responsible for ensuring security must know what types of information to report and how to report it. Surprisingly, no studies that described or evaluated the effectiveness of security training content or procedures were found. However, results from a top-to-bottom inspection of security procedures within DoD suggested that training may not be achieving its objectives (Secretary of the Army, 1986; Secretary of the Navy, 1987). The inspection results indicated that training is inconsistent and is not tailored to the applicable threat or to the recipient's experience. Furthermore, the majority of security managers had received no training.

Several reports emphasized the need for research addressing security education issues (Abbott, 1987; Crawford, 1988; U.S. House of Representatives, 1988). This research should focus upon specifying the training needs, objectives, and content required to meet the continuing assessment program objectives for each of the three major areas of personnel security-relevant behavior: possible security compromise, potential unsuitability, and failure to perform security duties. For example, with respect to possible security compromise, training needs analyses may indicate a need to better inform cleared personnel of the risks and penalties associated with espionage. Concerning potential unsuitability, training needs analyses might point out a need to more clearly inform personnel of the standards for military conduct, the assistance available to persons experiencing personal problems, and the importance of help-seeking behaviors. With respect to failure to perform security duties, one important training objective might be to overcome the reluctance of personnel to report derogatory information.

After training needs, objectives, and content have been specified, research is needed to identify the methods most appropriate to achieve those objectives. For example, two approaches from the applied psychology literature, behavior modeling and realistic job previews, might be useful for addressing the training objective cited above for security duties (i.e., overcoming the reluctance to report relevant information). These approaches are discussed briefly below.

A behavior modeling approach to training (e.g., Latham & Saari, 1979) has several advantages in the context of reporting derogatory information. It involves providing trainees with clear objectives, an opportunity to practice the behavior, feedback on their performance, and written learning points to take with them to assist in transferring the skills back to the job. This approach addresses several impediments to reporting known derogatory information. First, it specifies the behaviors that are to be reported. Second, the role play exercises allow individuals to verbalize and resolve any issues they have with reporting sensitive information. Third, trainees have the opportunity to model the behavior required for security duties (e.g., how to refer individuals for counseling and assistance). Fourth, it promotes transfer and maintenance of the desired behavior through practice of the correct behaviors and through the availability of the learning points on the job. An important aspect of this approach is the emphasis upon specifying the precise content of training, one of the key conclusions of training research (Gagne, 1962; Campbell & Campbell, 1988).

The realistic job preview (Wanous, 1973) is another approach to informing cleared personnel of their security-relevant job duties. One purpose of this interview is to ensure that

individuals have a realistic expectation of their job duties. Research indicates that individuals who enter their jobs with realistic expectations tend to show greater job commitment and satisfaction. The realistic job preview is similar to the initial PRP subject interview conducted by the manager with each newly certified individual. This interview helps to ensure that the person is comfortable with the program purpose (for PRP, this involves working with or around nuclear materials) and security procedures. For example, within the context of personnel security, commanders or supervisors can personally emphasize the importance of conscientious handling of classified information with new personnel and discuss resources available to assist individuals who experience personal difficulties that increase their security risk.

Monitoring

Numerous criticisms and suggestions have been made with respect to monitoring cleared personnel and reporting security-relevant information. These comments can be organized into two categories: (1) content issues concerning the appropriate behavioral content to monitor and (2) process issues addressing the optimal methods of obtaining information and channels for reporting it. These issues are discussed separately below.

Content Issues. Content issues focus on what actions or information regarding cleared individuals should be monitored. We mentioned earlier the lack of clear criteria in the 5200.2-R and DCID 1/14 regarding the specific types of continuing assessment information that should be reported. Besides this, several reports (U.S. House of Representatives, 1987, 1988) have recommended improving the financial information that is collected on cleared personnel. They point out that financial pressures and/or incentives have been a primary motivation for espionage in recent years. Two obvious areas for which information might be collected are unexplained affluence and bankruptcies. An ironic and interesting fact is that bankruptcy information is publicly available, but employers are limited in using this information by the Privacy Act. For example, The Washington Post (Sinclair and Woodward, 1986) obtained 2,536 Washington D.C. bankruptcy files and identified 56 of these persons as working in intelligence or other sensitive positions. Presumably, hostile intelligence could as easily identify and target them, while security efforts to identify and assist these people remain inefficient.

Recent research (Defense Manpower Data Center, 1987a, 1987b, 1988a, 1988b, 1989) in this area has focused on obtaining credit information on cleared personnel using automated procedures in conjunction with computer databases of credit report services. This is especially useful because financial status can change quickly. In fact, research has indicated that 19 percent of the cleared personnel in one sample showed signs of financial deterioration within a year of receiving a background investigation, compared to 6 percent who showed improvements (Defense Manpower Data Center, 1989). In addition, automated credit reports permit more frequent monitoring than the current five year credit updates (for cleared individuals with Top Secret and SCI access) at a fraction of the time, cost, and paperwork involved in current investigative methods. Furthermore, collecting financial information at regular periods supports a proactive, rather than reactive, approach to the management of the vulnerabilities of cleared personnel. This is important both for decreasing security risks and for providing needed assistance to valued personnel in a timely manner.

The research efforts as cited above reflect an approach that can serve as a productive model for needed research in other security-relevant content areas, such as criminal behavior (DoD Security Review Commission, 1985) and emotional stability. This research has compared the effectiveness of automated credit reports to current investigative methods, examined alternative scoring algorithms for the credit information, discussed alternative sources of relevant financial information, and explored the temporal stability of credit status. Future efforts need to develop a financial profile of high security risk individuals that includes consideration of unexplained affluence as well as financial difficulties. This is a natural extension of recent research which has examined the viability for personnel security purposes of information in U.S. Customs databases concerning the foreign bank accounts, currency transactions, and international transport of currency of cleared personnel (Defense Manpower Data Center, 1987a). Additionally, research is needed to define the relationship of credit status to security compromise activities and to other unsuitable behavior (i.e., substance abuse, criminal activities, emotional distress, unreliability).

Financial information represents only one type of possible indicator of security risk. Several lists of other indicators have been developed through inspection of espionage case histories. These include suspicious work behaviors, certain foreign travel patterns, affiliations with organizations or individuals from countries with interests that are opposed to the U.S., etc. Alternatives to the indicators implied by existing adjudicative criteria or specified by examination of espionage case histories have also been proposed. These include having cleared personnel complete an annual life events inventory (United States Senate, 1985) and conducting annual physical exams to identify medical indications that affect reliability (DoD Security Review Commission, 1985).

Research is needed to evaluate systematically the predictive validity and utility of all these proposed indicators of security risk. The problems associated with locating an adequate sample present a difficult barrier to this research. Furthermore, careful specification of the criteria of interest is an essential first step that must be undertaken before the relative efficacy of these indicators can be assessed. Nevertheless, research specifying the validity of indicators of security risk provides a solid basis for reducing security risks and for further improving program effectiveness.

Process Issues. Process issues focus on the appropriate methods and sources for collecting security-relevant information and the channels for reporting this information. A wide range of alternative, or improved, methods for gathering derogatory information have been proposed, including both "direct" (i.e., obtaining information from the subject) and "indirect" (i.e., obtaining information about the subject from other sources) methods of assessment. For example, one direct assessment method that could be implemented is an annual questionnaire to identify any changes with respect to security criteria. The advantage of this approach is that security professionals have noted that the subject is typically the best source of information (Bossnardt, DuBois, Paullin, & Carter, 1989).

The counterintelligence-oriented polygraph has also been recommended as another method of obtaining information of security significance from subjects (U.S. House of Representatives, 1987). However, important questions concerning its accuracy remain (e.g., Saxe, Dougherty, & Cross, 1983). Furthermore, concerns have been expressed about possible over-reliance on this method (U.S. House of Representatives, 1987), leading to lax continuing

assessment practices based upon a false assumption that anyone who passes the polygraph will always be loyal. Other direct assessment methods that have been recommended include psychological inventories, life events questionnaires, security interviews, and increased drug and alcohol testing.

Indirect methods of gathering security-relevant information include utilizing existing computer databases, such as centralized criminal information, credit checks, and foreign travel records. Given the large number of cleared personnel, the principal advantages for indirect methods are realized through the efficiencies and costs savings of automation and of using existing archives of information.

The identification and utilization of the best sources of derogatory information is another important process issue. Supervisors and commanders are considered to be primary sources of adverse security information, but often fail to provide such information (DoD Security Review Commission, 1985; Abbott, 1987). There are several possible reasons for this, including lack of knowledge regarding what to report, fear of grievances, desire not to hurt a person's career, administrative burdens, and various disincentives for reporting (e.g., loss of cleared individuals, no replacement while the information is being adjudicated) (Crawford, 1988; DoD Security Review Commission, 1985; Abbott, 1987; Secretary of the Army, 1986). One recommendation for systematically obtaining this information is to require supervisory review of personal history questionnaires (DoD Security Review Commission, 1985). This is now a requirement for all Personnel Security Questionnaires used to initiate a periodic reinvestigation.

Several other obstacles in gathering and reporting derogatory information have been cited. Lack of reporting by departments within the organization and by outside organizations are two examples of these obstacles. Few legal and administrative mechanisms exist for exchanging relevant derogatory information between federal agencies (U.S. House of Representatives, 1987) and between the personnel security office and other installation departments (e.g., legal, medical, employee assistance) (Department of Defense Security Institute, 1989). Furthermore, procedures for reporting derogatory information outside of formal organizational channels are inadequate (DoD Security Review Commission, 1985), although efforts are underway to address this concern (Bowden, 1987).

A final deficiency in the monitoring process is the lack of systematic and centralized storage of information (Abbott, 1987; Fedor, 1988). Centralized, automated recordkeeping is one alternative solution to the problems presented by decentralized records. This alternative ensures that information is accessible and is not lost after transfers or changes of status.

Other Considerations. Some research in the area of job stress suggests that proactive continuing assessment efforts could be targeted to high risk groups. Organizational stress surveys have identified high stress groups that are associated with indications of behavioral unreliability, such as increased medical malpractice claims (Jones, Barge, Steffy, Fay, Kunz, & Wuebker, 1988). The stress paradigm has been proposed as one useful approach to interpreting and predicting personnel unreliability (Barge et al., 1984). If the relationship between organizational stress generalizes to other security-related outcomes of interest (e.g., substance use; carelessness with sensitive information), it could be a useful tool for directing scarce resources towards high risk groups.

Evaluating/Motivating

This component of the continuing assessment program addresses the evaluation of security-relevant information (adjudication) and approaches to ensure that continuing assessment duties are competently performed (motivation and accountability). Each topic is discussed separately below.

Adjudication. One critical element of the personnel security system is the adjudication of derogatory information. When derogatory information becomes available, it is clinically evaluated and a decision is reached based on "the adjudicator's sound judgment, mature thinking, and careful analysis" (Department of Defense, 1987, p. I-1). This clinical decision strategy is only one of several that might be used.

Sawyer (1966) outlined and compared six strategies for collecting and combining data, based on Meehl's (1954) distinction between clinical and statistical methods. Current adjudicative procedures would be described as "pure clinical" using Sawyer's taxonomy. That is, a clinical judgment (i.e., adjudication) is made using a clinical method of collecting the data (i.e., investigative reports). This is in contrast to a strategy that includes collection of both clinical information (e.g., investigative reports) and more objective information (e.g., credit reports) with a statistical (or actuarial) method of combining this data for an adjudicative decision. This latter strategy is termed a "mechanical composite." When these six methods were compared, the mechanical composite was clearly the best strategy of the six and the pure clinical method was clearly the worst in terms of predictive accuracy.

Attempts (e.g., Goldberg, 1987) to explain the superiority of statistical methods focus on the superiority of statistics in accounting for differential validities, differential metrics between predictors and criteria, consistency of forecasts, and amount of redundancy of information. Perhaps for these reasons, statistical decisions have consistently outperformed clinical decisions in a wide array of contexts. Use of statistical decision strategies in the security context deserve consideration for other reasons as well. Automating some of the adjudication function could substantially increase the speed, volume, consistency, fairness and accuracy of clearance decisions (while decreasing the costs and while permitting adjudicators to focus on unusual or difficult cases where human expertise is required and is more likely superior).

Motivation. There are many management tools available to reduce security and suitability risks and to ensure that security duties are competently performed. Employee assistance programs have been cited as a key component in identifying and preventing personal problems from becoming security risks (Department of Defense Security Institute, 1989). Including security in annual performance and fitness reviews has also been recommended (DoD Security Review Commission, 1985) and implemented (Department of Defense, 1987) as a measure to manage security-relevant behavior.

Regarding motivational concerns, the Stilwell report (DoD Security Review Commission, 1985) recommended use of financial incentives to increase reporting of relevant information. From the point of view of reducing espionage, installing the death penalty, and instituting cause for action for peacetime espionage in the Uniform Code of Military Justice have been suggested.

Accountability. Accountability for security responsibilities is essential if program objectives are to be achieved. There is limited evidence that personnel security responsibilities are currently being assumed (Crawford, 1988), especially for contractors (DoD Security Review Commission, 1985). This may in part be due to a lack of emphasis on program oversight or a lack of management information, such as the type of derogatory information reported or trends in reporting frequencies (Crawford, 1988).

Schlenker (1986) proposed a model of personal accountability that has direct implications for the structure of effective continuing assessment programs. Schlenker's model includes three components: outcome expectations, the expected value of the task, and the strength of the accountability linkages. Similar to expectancy models of motivation, determination is greatest when these three components are strengthened. In terms of personnel security, performance of security duties is a function of expected outcomes of performance and of the person's commitment to the goals of security (accountability linkage). Our review of continuing assessment literature suggests that performance of security duties may produce few rewards and failure to perform may result in few penalties. Given the low base rate of espionage, it is possible that most individuals do not have a high commitment to report seemingly minor derogatory incidents, especially when confronted with competing incentives for not reporting. Schlenker's model stresses the importance of providing consequences for security-relevant behavior. It also implies that nonpunitive approaches to clearance suspension or termination may facilitate accountability.

Controlling

A number of controlling mechanisms or constraints play an important role in continuing assessment. Literature addressing two primary types of controlling mechanisms is described below.

Access Management. Several security practices have been developed for controlling counterproductive security behavior. Proper use of the "need-to-know" principle for allowing access to classified information is one control for maintaining effective security. Unfortunately, it is not consistently used in practice (U.S. House of Representatives, 1987). One reason for this is the absence of disciplinary measures to enforce it (U.S. House of Representatives, 1987).

Use of the "two-person" rule is another control that should be considered as a security measure (Abbott, 1987), especially for the destruction of classified information. Group cohesion has also been suggested as a possible constraint on poor security practices (Abbott, 1987).

Legal Constraints. The legal authority for continuing assessment is embodied in existing legislation, executive orders, and case law. These laws sometimes create obstacles to effectively collecting security-relevant information (DoD Security Review Commission, 1985).

Some of the more relevant of these documents are listed in Appendix A.[9] Although it is beyond the scope of this report to discuss in detail the legal implications of the various elements of the continuing assessment program, two general legal issues are briefly considered below.

The major legal issues addressing individual rights that are relevant to continuing assessment involve considerations of due process, the protection of privacy, equal protection under the law, and protections against search and seizure. The motif that underlies each of these issues is establishing the appropriate balance between national security and individual rights. With respect to due process, expert opinion (Haag & Denk, 1988, p. 181) notes that no provisions of DoD 5200.2-R have been found to fail Constitutional scrutiny. However, it is noted that courts have overturned findings on security clearances based upon the implementation of the regulations. This finding emphasizes the need for adequate training and certification of security personnel and/or inspection of program operations to ensure proper implementation of procedures. Additional work is needed to clarify these issues with respect to continuing assessment programs and to make specific recommendations for improvement.

It seems clear (Haag & Denk, 1988) that there is no Constitutional right to a clearance. Merely meeting criteria for clearance does not automatically grant a right for access to classified information. With respect to adjudicating derogatory information identified through the continuing assessment program, the Personnel Security Program Regulation (DoD 5200.2-R, pp. VI-1 & I-2) states that any doubts should be resolved in favor of national security. On the other hand, continuing assessment program procedures such as administratively withdrawing access and/or clearances or reassignment to other duties involve legal issues that remain ambiguous.

Other Considerations

Some reports have addressed other issues related to continuing assessment. Two of the most important issues are identification of other deficiencies within the total personnel security system which impact continuing assessment and the costs and benefits of continuing assessment program components. Each issue is briefly discussed below.

Several deficiencies in the total personnel security process impact continuing assessment programs. Two frequently cited obstacles are the overwhelming number of cleared individuals and amount of classified information (e.g., U.S. House of Representatives, 1987). Recent efforts have been made to reduce the number of cleared individuals, although more could be done (DoD Security Review Commission, 1985). Many other deficiencies have been identified. These include too many emergency exceptions to clearance processes (Secretary of the Army, 1986) and insufficient attention to formerly cleared individuals (Abbott, 1987).

---

[9]One excellent reference which includes many of these documents is the Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community (U. S. House of Representatives, 1983).

Little is known regarding the costs and benefits of the continuing assessment program components. Only three studies were found. The General Accounting Office (1981) estimated the increased costs resulting from delays in processing security clearances to be nearly 1 billion dollars. These delays were also cited for weakening national security by delaying important contracts. Furthermore, poor quality investigations often result from the time and work demands caused by the increasing numbers of clearance investigations. Two other studies addressed the savings that could result from consolidating personnel security investigations (General Accounting Office, 1974, 1979). Results of these studies suggested that costs could be reduced by developing standards across federal investigative agencies for determining the scope of investigations and by the increased sharing of investigative resources among agencies.

Additional research examining the costs and benefits of continuing assessment components should be pursued. Such information is fundamental to assessing tradeoffs among program objectives and among procedural alternatives for accomplishing these objectives.

Summary

This section reviewed literature relevant to continuing assessment. In general, the available literature is limited to narrative descriptions of programs, management analyses, and informed opinion concerning problems and strategies for improvement. No systematic attempts to describe operational programs of continuing assessment or to scientifically validate program procedures and outcomes were located.

The available information identified several obstacles to program effectiveness and indicated where basic research is needed. With respect to security criteria, research is necessary to identify the number and structure of security-relevant criteria. Results of this research have major implications for selecting the most appropriate policies and strategies to reduce security threats. With respect to the informing component, training needs analyses are needed to tailor content to local threats and needs and to better utilize innovative approaches (e.g., behavior modeling) for training security personnel. With respect to monitoring cleared personnel, recent research on obtaining security-relevant financial information was described. The promising results of this research are a model for cost-effective improvements in obtaining information in other areas, such as criminal behavior. With respect to the evaluating/motivating component, research in several areas of psychology suggests that the use of statistical methods to assist adjudicators offers much promise for substantially reducing the costs of adjudication while also improving the validity of clearance decisions. Lack of accountability for performing continuing assessment duties was identified as an important obstacle to program effectiveness. With respect to the controlling component, obstacles discussed included the ineffective use of access management methods (need-to-know and "two-person" rule principles) and legal issues concerning continuing assessment.

SECTION 6: IDEAS FOR IMPROVING CONTINUING ASSESSMENT

Results of this review of continuing assessment regulations and literature suggest several approaches for improving continuing assessment. These ideas are briefly summarized below according to the five areas of the model of security-relevant behavior: security-relevant criteria, informing, monitoring, evaluating and motivating, and managing constraints, plus two topics which address general system considerations (program emphases and program effectiveness). For each topic area, one or more ideas for improving continuing assessment are listed.

Development of Security-relevant Criteria

This review identified three general areas of security-relevant behavior: possible security compromises, potential unsuitability, and failure to perform security duties. Empirical research is needed to better define these areas and to clarify the relationships among these areas. Such information is essential for answering basic questions such as do "unsuitable" behaviors such as excessive alcohol use predict security compromise as well as future espionage? This knowledge provides the foundation for formulating continuing assessment policy, validating adjudication standards, choosing program strategies, and developing new methods of assessment (e.g., risk indicators form, annual security questionnaire).

*A. **Conduct basic research to identify the number and structure of behavioral dimensions underlying security compromise.***

- Develop and test a taxonomy of types and motivations of security compromise (e.g., espionage, volunteered information, inadvertent disclosure, financial incentives, foreign ties, blackmail, disgruntlement, etc.). Estimate the prevalence of each type of compromise and motivation. Determine the implications for continuing assessment policies and procedures of each type of compromise and motivation.

- Conduct research to specify the behavioral indicators of these security dimensions and their usefulness for predicting espionage.

- Determine the theoretical/conceptual foundations of an effective continuing assessment program with respect to reducing security compromise. This conceptual analysis would also examine the methods from the applied science disciplines that could be adapted into continuing assessment. Such analyses would provide useful insights into the appropriate content and procedures for this program. This review of the security literature provides one framework. Other models are needed.

B. Conduct research and develop theories to identify the number and structure of dimensions underlying unsuitable behavior and to specify the relationship of suitability criteria to security compromise.

- Conduct research to identify profiles of unsuitable conduct that indicate risk for security compromise.

- Estimate the validity and cost effectiveness of alternate methods of preventing and providing early treatment for unsuitable behavior (e.g., excessive alcohol use, financial difficulties, emotional problems).

C. Perform job analyses of continuing assessment duties.

- Identify the behaviors of individuals who perform effectively their continuing assessment duties. Such information would provide valuable insights into the strategies that persons use for handling difficult security-relevant situations. Those strategies could then be incorporated into security education and awareness programs as a means of preventing future espionage. This information would also be valuable for improving the accountability of cleared personnel for performing their continuing assessment duties.

Informing

Improve education and training content and methods to better inform cleared personnel of their continuing assessment responsibilities.

This review suggests that existing programs for training security staff and for informing cleared personnel of their continuing assessment duties are inadequate. The ideas for improvement listed here are directed at enhancing program content and methods. The literature suggests that content can be improved by better specifying reporting requirements, clarifying legal issues, emphasizing need to know requirements, and adapting training programs to the experience level of the trainees. Training methodologies could be improved through the development of standardized, flexible modules (e.g., videotapes, correspondence courses) to ensure that training is available when it is needed. Additionally, training methods could be improved through the use of innovative strategies (i.e., behavior modeling) to enhance transfer of learning to the work environment.

- Develop training modules which describe the indicators of security risk, security responsibilities, and reporting procedures for various program participants.

- Evaluate the effectiveness of existing security education procedures to determine which procedures are most useful.

Monitoring

Improve the validity and cost effectiveness of continuing assessment through the increased utilization of alternative strategies for gathering information.

The literature review identified a wealth of alternative approaches to gathering security-relevant information. The review also noted the lack of information on the validity and cost effectiveness of existing or alternative strategies. Based upon the research on security criteria and indicators described above, the next step is to assess the validity and cost effectiveness of existing and proposed methods for collecting continuing assessment information. Methods can then be developed and refined to ensure complete coverage of the relevant dimensions of security criteria.

- Incorporate procedures from other continuing assessment and reliability programs into the DoD program. Promising procedures include annual national and local agency checks and annual physical exams (including tests for alcohol and drug abuse, psychiatric problems).

- Develop new continuing assessment screening instruments, especially subject-provided information. Investigate the feasibility of subject-provided information using methods such as completion of questionnaires containing security-relevant activities, in-depth security interviews, personal history questionnaire updates, and standard psychological tests.

- Develop early warning systems for identifying cleared persons who have financial problems. One promising idea is gathering and computer scoring credit information on cleared personnel using automated databases of credit report services.

- Expand alcohol and drug testing for civilians. Such testing has been shown effective in reducing incidents of drug and alcohol abuse among military personnel.

- Identify better methods for coordinating security-relevant information among different command groups (e.g., personnel, medical, military police). One promising idea is the use of memoranda of agreement, which clarify the specific types of information that will be shared between departments.

- Create a non-punitive environment for administrative actions. For example, ensure that administrative downgrades or withdrawals of clearances have no adverse effects on the careers of affected personnel, whenever possible. The literature reviewed suggests that such actions increase reporting of derogatory information.

- Identify alternative methods for reporting derogatory information other than through formal command or organizational channels. Possible methods include drop boxes, post cards, and designated telephones. This was a major recommendation of the Stilwell Commission (DoD Security Review Commission, 1985).

- Assess the utility of a centralized, computer-automated security records center. This records center would provide a central source for the storage, retrieval, and dissemination of personnel security information. This data repository would facilitate the continuing assessment data gathering, data storage, data sharing, and adjudication processes.

Evaluating and Motivating

A. Improve the timeliness, validity, and cost effectiveness of adjudicating security-relevant information.

Reports addressing continuing assessment issues suggest that delays in adjudicating cleared personnel are a major barrier to program effectiveness. Furthermore, extensive psychological research suggests that the decision effectiveness and timeliness of existing methods could be substantially improved through the utilization of actuarial methods of decision making.

- Improve the clearance adjudication process by using actuarial methods to combine and weight security-relevant information from different adjudication areas according to carefully developed scoring rules. Partially automating this function would result in improved decision effectiveness, substantial cost savings, and considerable time savings.

B. Improve the motivation and accountability of personnel for performing their continuing assessment duties.

- Provide incentives for persons who demonstrate exemplary security-relevant behavior and have greater penalties for those who fail to carry out their continuing assessment responsibilities.

- Include continuing assessment as a performance appraisal area. This would draw attention to the importance of continuing assessment and would encourage accountability for performance in this area.

- Take actions to ensure quality control of the continuing assessment program (e.g., include continuing assessment in command inspections or in the IG).

Controlling

Improve the implementation of controls in the continuing assessment program.

The literature review indicates that two of the constraining factors, classified information access management and legal controls, may be inadequately implemented. Procedures for access management, such as use of the need-to-know principle, are available but are not adequately implemented. Similarly, while there have been no successful challenges to the legal grounds for the continuing assessment program, there has been considerable concern about the implementation of the program with respect to these issues. While additional research is warranted to better identify the availability and proper use of these types of constraints, the concerns identified earlier suggest the need for improvement in the implementation of these controls.

- Clarify the legal limitations of the continuing assessment process and provide security personnel and cleared individuals with explicit guidance on these limitations. Such knowledge would facilitate the reporting of derogatory information and result in more pertinent information.

- Include legal concerns and access management principles in security education and in procedures for accountability.

Program Emphases

A. Direct continuing assessment resources to high risk areas.

Given the importance of protecting classified information, the large number of cleared personnel, and limited resources for accomplishing program objectives, effective assignment of priorities for available resources is needed to ensure that the highest levels of security are maintained. Research and policy addressing appropriate strategies for allocating available resources are needed.

- Target continuing assessment efforts towards positions at greatest risk and/or highest position vulnerability. Possible position vulnerabilities include the individual's position, geographic location, nature of the local security threat, size of the organization, area cost of living, and selected work environment characteristics (e.g., percentage of coworkers having access to classified information).

- Target more continuing assessment effort towards those individuals at greatest security risk. Potential risk factors might be based on level of access and/or adjudication factors (e.g., financial, drug, alcohol problems). The analysis in Section 3 suggested that continuing assessment procedures (from the perspective of the regulations) show few differences across different clearance/access levels.

B. Reevaluate the appropriate priority of continuing assessment as compared to other types of security.

- Reevaluate the appropriate priority of continuing assessment compared to other types of security (e.g., information security, physical security) in terms of preventing espionage. Information about the costs and benefits of various types of security should be gathered and used to assign priorities to resource allocations.

- Reevaluate the appropriate emphases for initial screening and continuing assessment. Currently, initial screening receives greater emphasis than continuing assessment. Given that most individuals become spies after the granting of an initial security clearance and the costs and problems inherent in initial screening, the relative emphasis for these programs should be reevaluated.

Program Effectiveness

Develop and implement procedures to evaluate the effectiveness of the continuing assessment programs.

The systematic and ongoing assessment of program effectiveness is a critical component of the achievement of program objectives. History has shown that the motivations and methods for security compromise have changed dramatically in recent years. Similarly, changes in technology provide new, more valid and cost effective strategies for managing security risks. Security personnel need ongoing feedback on their performance to ensure the direction and quality of their efforts. For these reasons, a thorough and ongoing program for assessing program effectiveness is needed.

- Obtain systematic quantitative and qualitative information regarding the operation of current continuing assessment programs. Systematic assessment of the current continuing assessment programs is needed before program deficiencies can be identified and appropriate solutions can be recommended. Report 2 in this series provides an examination of the current system.

- Evaluate the overall effectiveness of continuing assessment programs in the military services. Available assessments of these programs are based on qualitative information and informed opinion (e.g., Abbott, 1987; U.S. House of Representatives, 1987). Systematic, empirical research is needed. Results of this research project (see Reports 2 and 3 in this series of project reports) provide such an assessment. Additional research is needed to develop better indices of program effectiveness.

- Evaluate the costs and benefits associated with different continuing assessment procedures. Because of scarce resources, developing program priorities in relation to the expected benefits is essential for maximizing overall program effectiveness. Methodologies for performing such cost/benefit analyses already exist (e.g., Delphi or nominal group methods).

REFERENCES

Abbott, P. S. (1987). *Personnel security continuing evaluation (CE) programs* (TR 87-01). Alexandria, VA: HumRRO International.

Barge, B. N., Hough, L. M., Dunnette, M. D., Kemery, E., 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.

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

Bosshardt, M. J., DuBois, D., Paullin, C., & Carter, G. W. (1989). *The investigative interview: A review of research and practice* (Institute Report No. 160). Minneapolis, MN: Personnel Decisions Research Institutes, Inc.

Bowden, C. (December 28, 1987). Army officials initiate 'dial-a-spy' hotline. *European Stars and Stripes*, p. 1.

Builder, C. H., Jackson, V. G., & Starr, R. (1988). *To repair or to rebuild? Analyzing personnel security research agendas.* (Office of the Under Secretary of Defense for Policy, R-3652-USDP). Santa Monica, CA: Rand Corporation.

Campbell, J. P., & Campbell, R. J. (1988). Industrial-organizational psychology: The goodness of fit. In J. P. Campbell & R. J. Campbell (Eds.), *Productivity in Organizations.* San Francisco, CA: Jossey-Bass.

Campbell, J. P., Dunnette, M. D., Lawlor, E. E. III., & Weick, K. E. (1970). *Managerial Behavior, Performance, and Effectiveness.* New York: McGraw-Hill.

Campbell, J. P., & Pritchard, R. (1976). Motivation theory in industrial and organizational psychology. In M. D. Dunnette (Ed.), *Handbook of Industrial and Organizational Psychology.* Chicago: Rand-McNally.

Center for Personnel Security Assurance, Research and Analysis. (1988). *An overview of the personnel security assurance program* (Technical report). Oak Ridge, TN: Oak Ridge Associated Universities.

Crawford, K. S. (1988, July). *Continuing assessment in DoD: An overview.* Monterey, CA: Defense Personnel Security Research and Education Center.

Defense Manpower Data Center. (1987a, December). *Cleared military personnel with financial data in Customs files.* Monterey, CA: Author.

Defense Manpower Data Center. (1987b, December). *Automated credit report assessment: DMDC matching and analysis of TRW credit reports*. Monterey, CA: Author.

Defense Manpower Data Center. (1988a, July). *Comparison of two automated credit scoring algorithms*. Monterey, CA: Author.

Defense Manpower Data Center. (1988b, December). *Comparison of alternate credit report strategies: Consideration of automated TRW reports as a replacement for the current multi-vendor approach*. Monterey, CA: Author.

Defense Manpower Data Center. (1989, May). *Short-term credit deterioration among DoD personnel with recent background investigations*. Monterey, CA: Author.

Department of Defense. (1987). *Personnel security program regulation* (DoD 5200.2-R). Washington, DC: Author.

Department of Defense Security Institute. (1989). The case for continuing 'aluation. *Security Awareness Bulletin*, pp. 1-89, 1-4. Richmond, VA: Author.

Director of Central Intelligence. (1986). *Minimum personnel security standards and procedures governing eligibility for access to sensitive compartmental information* (Directive No. 1/14, pp. 5-6).

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

Dunnette, M. D. (1963). A note on the criterion. *Journal of Applied Psychology, 47*, 251-253.

Dunnette, M. D., Bownas, D. A., & Bosshardt, M. J. (1981). *Prediction of inappropriate, unreliable, or aberrant job behavior in nuclear power plant settings* (Institute Report #62). Minneapolis, MN: Personnel Decisions Research Institutes, Inc.

Enns, J. H. (1988). *Human reliability program development in the Department of Energy* (AAI #88-8). Cambridge, MA: Abt Associates.

Fedor, W. (1988, July). *Introductory comments to the continuing assessment session*. Monterey, CA: Defense Personnel Security Research and Education Center.

Flyer, E. S. (1986). *Personnel security research: Prescreening and background investigations* (FR86-01). Alexandria, VA: HumRRO International.

Gagne, R. M. (1962). Military training and principles of learning. *American Psychologist*, 18, 83-91.

General Accounting Office. (1974). *Personnel security investigation: Inconsistent standards and procedures*. Washington DC: Author.

General Accounting Office. (1979). *Cost of federal personnel security investigations could and should be cut.* Washington, DC: Author. (NTIS No. PB-300 964)

General Accounting Office. (1981). *Faster processing of DoD personnel security clearances could avoid millions in losses.* Washington, DC: Author. (NTIS No. PB82-116468)

Goldberg, L. R. (1987). Human mind versus regression equation: Five contrasts. In D. Cichetti & W. Grove, *Festschrift in honor of Paul E. Meehl.* Cambridge, MA: Cambridge University Press.

Haag, E. V., & Denk, R. P. (Eds.). (1988). *Due process in matters of clearance denial and revocation: A review of the case law by John Norton Moore, Esq., Ronald L. Plesser, Esq., and Emilio Jaksetic, Esq.* Monterey, CA: Defense Personnel Security Research and Education Center.

Hough, L. M. (1988, April). *Personality assessment for selection and placement decisions.* Workshop presented at 3rd Annual Conference of the Society for Industrial and Organizational Psychology, Dallas.

Houston, J. S. (1989). *Development of measures of Marine security guard job performance and behavioral reliability* (Technical Report #171). Minneapolis, MN: Personnel Decisions Research Institutes, Inc.

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

Jones J. W., Barge, B., Steffy, B. D., Fay, L. M., Kunz, L. K., & Wuebker, L. J. (1988). Stress and medical malpractice: Organizational risk assessment and intervention, *Journal of Applied Psychology, 73*(4), 727-735.

Latham, G. P., & Saari, L. M. (1979). The application of social learning theory to training supervisors through behavior modeling. *Journal of Applied Psychology, 64*, 239-246.

Meehl, P. E. (1954). *Clinical versus statistical prediction: A theoretical analysis and review of the evidence.* Minneapolis, MN: University of Minnesota Press.

Milberg, W. H. (1980). *The U.S. intelligence community: Dilemmas of law and management.* Newport, RI: Center for Advanced Research, Naval War College. (NTIS No. AD-A093048)

Olson, D. M., & Borman, W. C. (1989). More evidence on relationships between the work environment and job performance. *Human Performance, 2 (2),* 113-130.

Peters, L. H., Chassie, M. B., Lindholm, H. R., O'Connor, E. J., & Kline, C. R. (1982). The joint influence of situational constraints and goal setting on performance and affective outcomes. *Journal of Management, 8*(2), 7-20.

Peters, L. H., & O'Connor, E. J. (1980). Situational constraints and work outcomes: The influences of a frequently overlooked construct. *Academy of Management Review, 5*(3), 391-397.

Rothstein, H. R., Schmidt, F. L., Erwin, F. W., Owens, W. A., & Sparks, C. P. (1990). Biographical data in employment selection: Can validities be made generalizable? *Journal of Applied Psychology, 75*(2), 175-184.

Sawyer, J. (1966). Measurement and prediction, clinical and statistical. *Psychological Bulletin, 66*, 178-200.

Saxe, L., Dougherty, D., & Cross, T. (1983). *Scientific validity of polygraph testing: A research review and evaluation* (Technical Memorandum OTA-TM-H-15). Washington, DC: U.S. Congress, Office of Technology Assessment.

Schlenker, B. R. (1986). *Personal accountability: Challenges and impediments in the quest for excellence* (Technical report). San Diego: Navy Personnel Research and Development Center.

Schmidt, F. L., Hunter, J. E., & Outerbridge, A. N. (1986). Impact of job experience and ability on job knowledge, work sample performance, and supervisory ratings of job performance. *Journal of Applied Psychology, 71*(3), 432-439.

Schmitt, N., Gooding, R. Z., Noe, R. D., & Kirsch, M. (1984). Meta-analyses of validity studies published between 1964 and 1982 and the investigation of study characteristics. *Personnel Psychology, 37*(3), 407-422.

Secretary of the Army. (1986, November 25). Command security inspections--Action memorandum. Washington, DC: Author.

Secretary of the Navy. (1987, June 22). Lessons learned from command security inspections. Washington, DC: Author.

Sinclair, M., & Woodward, R. (1986, June 8). U.S. security workers file for bankruptcy. *Washington Post*, p. 1, 18, 19.

United States Senate. (1985, April). *Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs*. Washington, DC: Author.

United States Senate. (1986, September). *Meeting the espionage challenge: A review of United States counterintelligence and security programs* (Report 99-522). Report by the Select Committee on Intelligence, 99th Congress, 2nd Session.

U.S. House of Representatives. (1983). *Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community*. Prepared for the use of the Permanent Select Committee on Intelligence. Washington, DC: Author.

U.S. House of Representatives. (1987). *United States counterintelligence and security concerns - 1986.* Report by the Permanent Select Committee on Intelligence (Report 100-5). Washington, DC: U.S. Government Printing Office.

U.S. 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.

Wanous, J. P. (1973). Effects of a relistic job preview on job acceptance, job attitudes, and job survival. *Journal of Applied Psychology*, 58, 327-332.

Wood, S., Herbig, K. L., & Lewis, P. A. (1990). *American Espionage, 1945-1989.* Unpublished manuscript. Monterey, CA: Defense Personnel Security Research and Education Center.

APPENDIX A

Glossary

GLOSSARY

(Compiled from DoD 5200.2-R unless otherwise noted.)

Access. The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

Adverse Action. A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction in pay, or furlough of 30 days or less.

Agent.* In intelligence usage, one who is authorized or instructed to obtain or to assist in obtaining information for intelligence or counterintelligence purposes.

Background Investigation (BI)*. A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in DoD, PSP, App. B., par.3, covering the most recent five years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least the two years are covered and that no investigation will be conducted [for the years] prior to an individual's 16th birthday.

Classified Information.* Official information or material that requires protection in the interests of national security and that is classified for such purposes by appropriate classifying authority in accordance with the provisions of Executive Order 12356. Official information which has been determined to require, in the interests of national security, protection against unauthorized disclosure and which has been so designated.

Communications Intelligence. This is technical and intelligence information derived from foreign communications by other than the intended recipients.

Communications Security (COMSEC). COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications related to national security and to ensure the authenticity of such communication. Such protection results from the application of security measures to electrical systems generating, handling, processing, or using national security information and also includes the application of physical security measures to COMSEC information or materials.

Compromise. Compromise is the disclosure of classified information to persons not authorized access thereto.

CONFIDENTIAL. "CONFIDENTIAL" is the designation that shall be applied to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Counterespionage. That aspect of counterintelligence designed to detect, destroy, neutralize, exploit or prevent espionage activities through identification, penetration, manipulation, deception and repression of individuals, groups, or organizations conducting or suspected of conducting espionage activities.

Counterintelligence.* That aspect of intelligence activity which is devoted to destroying the effectiveness of inimical foregoing intelligence activities and the protection of information against espionage, individuals against subversion, and installations or material against sabotage.

CNWDI. CNWDI is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, fusionable, and high-explosive materials by type. Among these excluded items are the components which DoD personnel, including contractor personnel, set, maintain, operate, or replace.

Critical-Sensitive Position.* A civilian position within the Department of Defense meeting the following criteria (a) access to Top Secret information; (b) development or approval of plans, policies, or programs that affect the overall operations of the Department of Defense or a DoD Component; (c) development or approval of war plans, plans or particulars of future major operations or special operations of war, or critical and extremely important items of war...(f) duties falling under Special Access Programs (or others).

Critical Technology. Militarily-significant technology that is not possessed by potential adversaries and which, if acquired by them, would permit a substantial advance in their military capabilities, much to the detriment of the U.S. National Security. Critical technology satisfies one or more of the following criteria:

a. it contributes to the superior characteristics (performance, reliability, maintainability or cost) of current military systems;

b. it relates to specific military deficiencies of a potential adversary and would contribute significantly to the enhancement of their military mission;

c. it is an emerging technology with high potential for having a major impact upon advanced weapons systems.

(The Military Critical Technologies List (MCTL) is a reference document to be used in making this judgment.)

CRYPTO. CRYPTO is a marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying national security-related information. (The CRYPTO marking also identifies COMSEC equipment with installed hardwired operational keying variables.)

Custodian. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information is the custodian.

Declassification. This is the determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

Defense Central Security Index (DCSI). An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DoD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DoD officials, Congressional comr ittees, the General Accounting Office and other authorized Federal requesters.

Department of Defense. DoD refers to the Office of the Secretary of Defense (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities).

Derivative Classification. This is a determination that information is in substance the same as information currently classified and the application of the same classification marking.

DoD Component. Includes the Office of the Secretary of Defense; the Military Departments; Organization of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands.

Downgrade. To downgrade is to determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a lower degree of protection.

Emission Security*. The component of communications security which results from all measures taken to deny unauthorized persons from deriving information of value from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

Entrance National Agency Check (ENTNAC). A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

Espionage.* Actions directed toward the acquisition of information through clandestine operations.

Facility. A facility is a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above.) For purposes of industrial security, the term does not include UA installations.

Facility Security Clearance (FCL). This an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

Foreign Interest. The term refers to any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S., or its possessions; or any form of business enterprise organized or incorporated under the laws of the U.S., or a state or their jurisdiction of the U.S., which is owned or controlled by a foreign government, firm, corporation, or person. Included in this definition is any natural person who is not a citizen or national of the U.S. (An immigrant alien as defined in paragraph 1-237 is excluded from the definition of a foreign interest.)

Foreign Nationals. All persons not citizens of, not nationals of, nor immigrant aliens to the U.S. are foreign nationals.

FORMERLY RESTRICTED DATA. This is information removed from the RESTRICTED DATA category upon joint determination by DOE (or antecedent agencies) and DoD that such information related primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as RESTRICTED DATA.

Head of DoD Component. The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands; and the Directors of Defense Agencies.

Illegals.* Trained intelligence officers sent abroad, often with false identities, who maintain no overt contact with their government.

Immigrant Alien. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

Industrial Security. That portion of internal security which is concerned with the protection of classified information in the hands of U.S. industry is industrial security.

Information Security. This refers to the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of foreign operations and which is immediately or potentially significant to military planning and operations.

Interim Security Clearance. This is a security clearance based on lesser investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

Internal Security. This refers to the prevention of action against U.S. resources, industries, and institutions and the protection of life and property in the event of a domestic emergency by the employment of all measures, in peace or war, other than military defense.

Limited Access Authorization. Authorization of access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (Paragraph 3, Appendix B).

Minor Derogatory Information. Information that, by itself, is not of sufficient importance of magnitude to justify an unfavorable administrative action in a personnel security determination.

National Agency Check.* A personnel security investigation consisting of a records review of certain national agencies such as prescribed in DoD, PsP, App. B., par.1, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

National Agency Check Plus Written Inquiries (NACI). A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

DoD National Agency Check Plus Written Inquiries (DNACI). A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to SECRET information consisting of a NAC, credit bureau check, and written inquiries to current and former employers (see paragraph 2, Appendix B), covering a 5-year scope.

National Security. National security means the national defense and foreign relations of the United States.

Need-to-know*. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

Noncritical-Sensitive Position.* A civilian position within the Department of Defense meeting the following criterion: (a) access to Secret or Confidential information (or others).

Nonsensitive Position.* All civilians' positions in the Department of Defense not designated as Critical-Sensitive (i.e., requiring access to Top Secret information) or Noncritical-Sensitive (i.e., requiring access to Secret or Confidential information).

Officers (Corporation, Association, or Other Types of Business or Educational Institutions). This definition includes persons in positions established as officers in the articles of incorporation or bylaws of the organization, including all principal officers; that is, those persons occupying positions normally identified as president, senior vice president, secretary, treasurer, and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibilities, and authority as officially recorded by the organization.

Official Information*. Information which is owned by, produced for or by, or is subject to the control of the U.S. Government is official information.

Operations Security (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. Section X of this regulation contains a detailed discussion of OPSEC and UA responsibilities pertaining thereto. See JCS Pub 28 for further terms and definitions related to OPSEC.

Periodic Reinvestigation (PR). An investigation conducted every five years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs 3-700 through 3-710. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed character references and will normally not exceed the most recent five year period.

Personnel Security.* A composite activity consisting of (1) the security discipline concerned with protecting classified information through measures appropriate for persons who (a) are seeking, (b) have, or (c) have had authorized access to classified information; and (2) selected aspects of personnel suitability of (a) acceptance and retention of personnel in the Armed Forces, and (b) the assignment of DoD personnel to sensitive positions not requiring access to classified information.

Personnel Security Investigation (PSI). An investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations or affiliations with subversive organizations, suitability information, or hostage situations (see paragraph 2-403) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

Physical Security.* That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, facilities, material, and documents,and to safeguard them against espionage, sabotage, damage, and theft.

Restricted Area. This is a controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in paragraph 16, ISM, but which is capable of being stored during non-working hours in accordance with paragraph 14, ISM, (see section IV, ISM).

RESTRICTED DATA. All data (information) concerning: (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see §11y, Atomic Energy Act of 1954, reference (o), and paragraph 1-233, ISR, on FORMERLY RESTRICTED DATA).

Sabotage.* An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, and national defense or war material, premises, or utilities to include human and natural resources.

Scientific and Technical Intelligence.* The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: (a) foreign developments in basic and applied research in applied engineering techniques; and (b) scientific and technical characteristics, capabilities and limitations of all foreign military systems, weapons, weapon systems, and material, the research and development related thereto, and the production methods employed for their manufacture.

Scope. The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

SECRET. "SECRET" is the designation that shall be applied only to information or material, which the unauthorized disclosure of could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

Security. Security refers to the safeguarding of information classified as TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

Security Clearance. A determination that a person is eligible under the standard of this Regulation for access to classified information.

Senior Office of the Intelligence Community (SOIC). The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service: Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army, Assistant Chief of Staff for Intelligence, U.S. Air Force; and the Director of Naval Intelligence, U.S. Navy.

SENSITIVE COMPARTMENTED INFORMATION. This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in Section 22, Public Law 83-703, Atomic Energy Act of 1954, reference (o).

Sensitive Position. Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in paragraph 3-101.

Significant Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

Special Access Program. This refers to any program imposing "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; material dissemination restrictions; or special lists of persons determined to have a "need-to-know."

Special Background Investigation (SBI). A personnel security investigation consisting of all the components of a BI plus certain additional investigative requirements as prescribed in paragraph 4, Appendix B, this Regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

Special Investigative Inquiry. A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provisions of this Regulation.

Spy.* According to the Hague Convention of 1899, "One who, acting clandestinely or on false pretenses, obtains, or seeks to obtain, information in the zone of operations of a belligerent with the intention of communicating it to a hostile party." This definition would eliminate intelligence analysts, code and cipher clerks, and other in intelligence who are not operatives. More generally, one employed by a government to obtain secret information or intelligence about another country, especially with reference to military or naval affairs.

Telecommunications. The transmission, communication, or processing of information, including the preparation of such information thereof, by electrical, electromagnetic, electromechanical, or electro-optical means.

TEMPEST. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations (see paragraph 1-217.1)

TOP SECRET. "TOP SECRET" is the designation that shall be applied only to information or material, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital material defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific and technological developments vital to national security.

Transmission Security. Transmission security is that component of security which results from all measures designed to protect communication transmissions from interception and traffic analysis.

Unfavorable Administrative Action. Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations as defined in this Regulation.

Unfavorable Personnel Security Determination. A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this Regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge from the Armed Forces when any of the foregoing actions are based on derogatory information of a personnel security significance.

United States Citizen (Native Born). A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

Upgrade. To upgrade is to determine that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

* indicates the following source: Builder, C. H., Jackson, G. V., Starr, R. (1988). *To repair or to rebuild: Analyzing personnel security research agendas*, Appendix B, Prepared for the Office of the Under Secretary of Defense for Policy, R-3652-USDP.

APPENDIX B

Selected Documents Related to Continuing Assessment Issues

SELECTED DOCUMENTS RELATED TO CONTINUING ASSESSMENT ISSUES

Date	Title	Reference	Description
	LEGISLATIVE		
1947	National Security Act	50 USC 413	Establishes National Security Council & CIA
1954	Atomic Energy Act	42 USC 2011	Protection of atomic energy information
1961	Foreign Assistance Act	22 USC 2422	Hughes-Ryan Amendment
1974	Privacy Act	Sect 552a, Title 5	See especially punishment for disclosure
1974	Freedom of Information Act	Sect 552, Title 5	Public access to government information
1976	Foreign Intelligence Surveillance Act		Established special court to deal with secret matters
1978	Civil Service Reform Act		Transfers investigative responsibilities to OPM
1978	Ethics in Government Act	5 USC App	Public access to financial disclosure reports; exemptions
1980	Classified Information Procedures Act	18 USC App	Procedures for criminal cases involving classified
1980	National Intelligence Act		
1985	National Security Protection Act		
	The Espionage Act	18 USC 793	Gathering, transmitting, or losing defense information
		18 USC 798	Disclosure of classified information
		18 USC 1902	Penalties for disclosure of crop information
		18 USC 1905	Penalties for disclosure of trade secrets
		50 USC 783	Offenses & penalties for espionage
		56 USC 783	Espionage offenses
		Title 5, USC 7532	Grants agency heads authority to suspend/remove
		Part 9, FAR	Authority to suspend, debar contracting, for cause employees in the interests of National security
	EXECUTIVE		
1951	Exec. Order 10207		Internal Security & Individual Rights
1953	Exec. Order 10450		(18 F.R. 2489)
1960	Exec. Order 10865		Safeguarding classified info in Industry
	Exec. Order 11905		Minimum personnel security standards
1978	Exec. Order 12036		U.S. Intelligence Activities
1978	Exec. Order 12065		National Security Information
1979	Exec. Order 12139		Exercise of authority for electronic surveillance
1981	Exec. Order 12334		Establishment of Intelligence Oversight Board
1982	Exec. Order 12356		National Security Information
1989	Exec. Order, Proposed		Access to classified information
	JUDICIAL		
1959	Greene v. McElroy		Establishes need for due process in personnel security
	Matthews v. Eldridge		Provides criteria for due process
	U.S. Navy v. Thomas Egan		Due process & individual liberties

SELECTED DOCUMENTS RELATED TO CONTINUING ASSESSMENT OF PERSONNEL SECURITY (cont.)

Date	Title	Description
	REGULATIONS	
	Intelligence Agencies	
	DCID 1/14	Personnel Security Standards & Procs (SCI)
	Department of Defense	
	DoD 5200.1-R	Information Security Program
	DoD 5200.2-R	Personnel Security Program Regulation
	DoD 5220.22-R	Industrial Security Regulation
	DoD 5240.6	Requirement to establish counterintelligence awareness program
	SERVICE BRANCH	
	Air Force	
	AFR 200-7	SCI Security System
	AFR 205-32	Personnel Security Program
	AFR 205-25	Safeguarding SIOP information
	AFR 205-57	Reporting & countering hostile intelligence threats
	AFR 123-2	Investigations for SSFs
	AFR 10-1	AFSCO status reports
	AFR 12-35	Privacy Act Program
	AFR 12-50	SIOP procedures, disposal of SSFs
	AFR 35-32	Unfavorable information
	AFR 35-99	Personnel Reliability Program
	AFR 40-716	Medical evaluation to recertify after drug use
	AFR 40-732	Processing of SSFs on civilian personnel
	AFR 40-750	Civilian penalties for failure to report CI information
	AFR 56-11	COMSEC Duties
	Army	
	AR 380-67	Personnel Security Program
	Navy/Marines	
	OPNAV 5510.1H	Personnel Security Program
	OPNAV 5530 B	COMSEC Regulations
	NCPC 5521.1	Civilian Personnel Procedures
	OTHER RELATED DOCUMENTS	
	DOE Order 5631.2A	Personnel Security Program
	OPM Manual Supplement 731-73	
	British Official Secrets Act	