IV Personnel Security: Protection Through Detection

The personnel security system was put in place following World War II as a means of supporting the classification system and of implementing the Truman and Eisenhower Administrations' programs to investigate the loyalty of Federal Government officials. Over the past half century, a variety of directives and additional regulations have been issued to tailor the system to specific needs and respond to particular concerns (at times on an agency-specific basis), creating a layering of rules and, in turn, certain redundancies and other inefficiencies.

Even so, the fundamental standards and criteria around which personnel security policies and procedures are organized remain those set out in an executive order that is now nearly 44 years old. Although President Clinton's Executive Order 12968, issued on August 2, 1995, provides for common investigative and adjudicative standards to improve clearance reciprocity, strengthens appeal procedures, and improves the means of ensuring non-discrimination, it does not supersede Executive Order 10450, issued by President Eisenhower in 1953. Thus, in effect, it simply adds another regulatory layer to the personnel security system.

Personnel security in the future must be better integrated throughout the workplace, with managers and line officers accepting greater responsibility for security. High-profile examples of espionage arrests and poorly-administered procedures reduce confidence in the overall system and reinforce the Commission's view that the existing approach to personnel security is in need of substantial reform.

An updated personnel security system also must allocate more attention and resources to monitor, assess, and assist current employees, in particular those in positions of greatest sensitivity and those who have become at risk as a result of changes or difficulties in their lives. The Commission also believes that the personnel security process must be better understood. Many employees and applicants who have passed through the process have little understanding of what it actually involves. Greater security awareness and understanding should lead to a more secure working environment, as personnel become more knowledgeable about the key security concerns and significant threats, and what mechanisms exist to respond to these challenges.

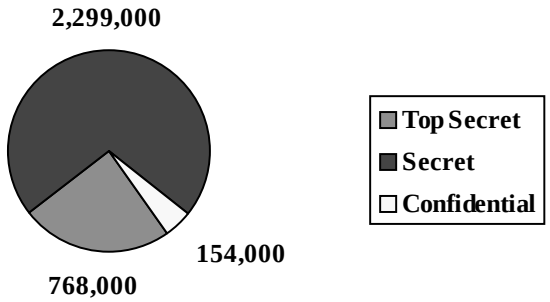
Overview of the Personnel Security Process

The Background Investigation

The chief objective of the personnel security process is to attempt to determine whether past behavior is a matter of concern for future reliability. Before prospective Federal employees (both military and civilian) and contractors' employees who work in the national security arena can have access to national security information, they must

undergo an investigation and adjudication to determine whether they should receive a security clearance. As Figure 3 shows, according to a 1995 General Accounting Office (GAO) report, more than 3.2 million government employees and contractors held security clearances in 1993 (the last year for which full data are available).[1]

Figure 3: Number of Federal and Contractor Employees with Clearances



Source: General Accounting Office, *Background Investigations: Impediments to Consolidating Investigations and Adjudicative Functions*, GAO/NSIAD-95-101 (Washington, D.C.: Government Printing Office, March 1995), 12.

A security clearance indicates that a person has been investigated and deemed eligible for access to classified information based on established criteria set out in regulations. Although in limited instances agency heads may grant a clearance without an investigation, employees normally receive access to classified information only when they have been "cleared" and a "need-to-know" justification has been provided. In practice, however, the "need-to-know" principle is seldom applied strictly, except in specific areas such as most special access programs (SAPs), which maintain access rosters.

The clearance process begins with the submission of a personal history statement detailing past residences, educational and employment background, criminal history, relatives, and other personal information. An investigation is then requested and conducted by a government agency such as the Defense Investigative Service (DIS)—which is the largest investigative agency in the Federal Government—or by a private contractor on behalf of an agency.

The length and complexity of the background investigation varies depending on the level of clearance (or the access) needed. In most agencies individuals are vetted for Confidential, Secret, or Top Secret clearances, and possibly for access to Sensitive Compartmented Information (SCI) as well. The Department of Energy (DoE) has a separate system pursuant to the Atomic Energy Act; most of its employees receive either an "L" clearance, which equates to a Confidential or Secret clearance, or a "Q" clearance, which equates to a Top Secret clearance.

Types of Investigations

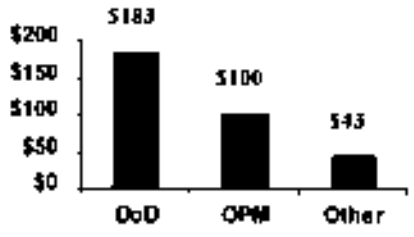
There are three types of personnel security investigations: a National Agency Check (NAC), which includes, but is not necessarily limited to, a check of FBI name and fingerprint records; Office of Personnel Management (OPM) investigations on all applicants for Federal service; and, when appropriate, review of Department of Defense (DoD) records of cleared military and civilian employees or contractors. The NAC has served as the basis for Confidential and Secret clearances, primarily for U.S. military personnel.

When the NAC is supplemented by a credit check and written inquiries, the investigation is termed a NAC with Written Inquiries (NACI). Written inquiries are sent to schools, employers, and local law enforcement agencies to verify information

submitted by the person under investigation. This has been the standard procedure required for Confidential and Secret clearances for Federal civilian employees in most agencies, as well as "suitability determinations" for applicants seeking Federal employment in positions not needing a security clearance. (It is notable that applicants for non-national security positions traditionally were subject to investigative steps for a "suitability" determination that *exceeded* those for military applicants who needed a Secret-level security clearance.) Those requiring access to Secret special access programs, however, usually require a review process similar to that for a Top Secret clearance.

A Single-Scope Background Investigation (SSBI), incorporating the NAC but using investigative interviews in lieu of written inquiries, is required for Top Secret clearances, for many SAPs designated Secret or Top Secret, for "Q" clearances, and for access to SCI data. As part of the background investigation process, investigators interview the applicant, current and former neighbors, character references, former educators, former spouses, and current and former employers; undertake local and national law enforcement record checks; and obtain credit reports and military and medical records. In addition, some agencies such as the CIA and the NSA require the applicant to undergo a polygraph examination, a medical examination, and a psychological evaluation.

Government employees and contractor personnel with security clearances are also subject to reinvestigations (covering the period beginning with the date of the last investigation) throughout their careers. The timing of reinvestigations can be random, but for Top Secret clearances they must be completed not less than once every five years. While the primary difference between initial investigations and reinvestigations is the period of time covered, some reinvestigation components may vary from the initial investigation. For example, during an initial polygraph examination, the NSA and the CIA cover counterintelligence issues (sabotage, espionage, and foreign intelligence) as well as additional issues such as possible use of drugs and any criminal activity, which are not included in subsequent tests. The Departments of Energy and Defense require regular in-house reviews as part of their "personnel reliability" programs for employees in extremely sensitive positions (such as those having access to nuclear devices); these reviews are conducted annually and consist of an interview, urinalysis, psychological testing, and a credit check.



Source: General Accounting Office, *Background Investigations: Impediments to Consolidating Investigations and Adjudicative Functions*, GAO/NSIAD-95-101 (Washington, D.C.: Government Printing Office, March 1995).

Investigative Costs

As shown in Figure 4, according to a March 1995 GAO report surveying 51 different agencies, the total cost of background investigations in 1993 (the latest year for which such figures are available) was $326 million.[2] The individual costs for a standard field investigation vary considerably, depending upon both the investigative agency and the priority of the investigation. OPM charges $3,425 for service within 120 days and $3,995 for 35-day service.[3] The Defense Investigative Service, in contrast, to date has not

been permitted to charge its customers for investigations or reinvestigations, although this restriction is now being reexamined.

The Adjudication

The information collected during the investigative process is then forwarded to an adjudicative office, where an adjudicator evaluates all of the data collected in order to make a clearance determination. This decision is based on established guidelines. An adjudicator who believes that the investigation is incomplete usually has the opportunity to request additional information from the investigator.

When an already cleared employee is transferred or detailed to another agency or special access program, that individual's file is reviewed again by an adjudicator at the receiving agency or by a program security officer prior to the acceptance of the employee's clearance. As a result, even though the individual's clearance may be up to date, additional security vetting is usually required before the clearance will be accepted by the receiving agency or special access program.

Improving the Current System

Modernizing the System's Cold War Foundations

Prior to the Cold War, the Federal Government's efforts to maintain a trustworthy and reliable civil service were based primarily on the Civil Service Act of 1883. The Act included a core principle of "suitability" for Federal employment, defining this as "a requirement or requirements for government employment having reference to a person's character, reputation, trustworthiness, and fitness as related to the efficiency of the service." Seventy years later, Executive Order 10450 imposed an additional requirement for Federal employment: "that all persons privileged to be employed in the departments and agencies of the Government, shall be reliable, trustworthy, of good conduct and character, *and of complete and unswerving loyalty* to the United States" such that ". . . *employment and retention . . . is clearly consistent with the interests of national security*." (Emphasis supplied.)

The criteria applied to "suitability" and "security eligibility" determinations today are largely redundant. All civilian Federal Government employees, regardless of whether they need access to national security information, must be found suitable for government service through use of at least a NACI. Those requiring access to national security information must also be found security-eligible as defined by Executive Order 10450. However, the two-step process of determining suitability and security eligibility is not applied uniformly across agencies, frequently involves duplicative steps and long delays, and is poorly understood by applicants and many agency officials alike. In addition, both the responsibilities and the criteria for suitability and personnel security determinations may differ from agency to agency. Some agencies place responsibility for both evaluations in the same office, while others maintain separate offices for making suitability and security determinations, at times with minimal coordination between the offices.

While the fundamental principles of the personnel security system remain based on Executive Order 10450, numerous other authorities have modified the specific language set out in the Order for issuing security clearances, either because the Order needed further amplification over the years or because it did not fit the needs of a particular agency. For example, the Order does not mention "classified information"

Table 2: Major Personnel Security Authorities Since EO 10450

The Atomic Energy Act	As amended in 1954, set out the restricted data classification system, with an entirely separate structure from national security clearances.
Executive Order 10865 (1960)	Established standards governing access for industry employees.
Title 5 of the Code of Federal Regulations	Authorized heads of departments to prescribe regulations for determining the suitability of applicants for Federal service.
Public Law 88-290 (1964)	Amended the Internal Security Act of 1950 to specifically address personnel security concerns of the NSA.
DoD Directive 5200.2-R (1979)	Combined all Department of Defense personnel security programs, including DoD Directive 5210.9, which established the military personnel security program requiring the military to abide by the same loyalty oath as civilians.
National Security Directive 63 (1991)	Established single scope background investigative standards for access to Top Secret and Sensitive Compartmented Information.
Executive Order 12829 (1993)	Created the National Industrial Security Program (NISP), a consolidation of Federal industrial security programs and relevant regulations.
Director of Central Intelligence Directive 1/14 (revised 1994)	Provided adjudication standards for access to Sensitive Compartmented Information.
Executive Order 12968 (1995)	Updated standards governing access to national security information.

or include the words "clearance," "access," or "need-to-know." Some of the many laws and regulations pertaining to the investigation of applicants and employees for suitability or security eligibility determinations are summarized in Table 2.

A 1988 RAND Corporation report, *To Repair or Rebuild*, identified some of the key problems in the current personnel security process. Among the important issues raised was how to define the *basic purpose* of the personnel security system; that is, should it focus on responding to the loss of secrets through espionage, or should it look more broadly at how to address behavioral problems of cleared personnel ranging from alcoholism and drug use to financial problems? According to the report, the broader the definition of personnel security, "the more difficult it becomes to separate personnel security problems traditionally associated with personnel management, or to prevent them from lapping over into other security areas, such as counterespionage or physical security." The report concluded:

> Modest changes and incremental improvements to the current program are not likely to produce a significantly more effective personnel security program. Major investments in improving the effectiveness or efficiency of current procedures should be deferred until the theoretical foundations of the program are thoroughly examined to provide a clearer understanding and more complete description of the personnel security problem.[4]

In the nine years since that report was issued, however, any changes have been modest and any improvements incremental in nature. It is essential that a personnel security system for the post-Cold War era include new guiding principles reflecting updated needs and priorities. These guiding principles must be common across the Government to help officials implement specific personnel security procedures that enhance both national security and the understanding of operational needs, that are sensitive to individual rights, and that are supportive of employees' needs.

Recommendation

The Commission recommends five guiding principles as the essential elements of an effective personnel security system. Most already are part of the current system (including under Executive Order 12968), but too often they are not actually practiced throughout the Federal Government. The Commission recommends that these standards be incorporated into a new statute or regulation that would supersede Executive Order 10450.

While specific processes and tools may change over time, there must be consistent guiding standards underpinning the overall system.

The five guiding principles are:

- **Openness and clarity of standards:** All applicants for government employment, as well as those seeking contractor positions that require government review, must be provided with clear information in writing about the security vetting process. Currently, applicants, employees, and contractors typically are provided little information on the process. Promoting a greater understanding of the process should help to improve overall accountability, both for employees and for those responsible for administering security programs. For example, creating a standard brochure to explain the clearance process and address the most common questions would bring greater clarity to the system for applicants, employees, and contractors.

- **Balanced, "whole-person" standards:** The goal of an investigation and adjudication should be to develop a balanced picture of the individual, based on both positive and negative factors, including evidence that past problems have been overcome.

- **Reciprocity for classified access:** When a government employee or contractor transfers or is detailed to, or is directly hired by another agency or private contractor, that individual's clearance should be accepted by the receiving agency if it is equivalent to or higher than that required for the new position and if the previous investigation and adjudication occurred within the established timeframe. Agency or program-specific supplemental forms should be eliminated.

- **Nondiscrimination principles:** Denials and revocations of access should not be based on arbitrary or capricious standards. The U.S. Government is not permitted to discriminate on the basis of race, color, religion, sex, national origin, disability, sexual orientation, or mental health counseling in granting access to classified information. Although Executive Order 12968 represents a significant step forward in this regard, it has not yet been fully implemented across the Government.

- **Assurances of due process:** Applicants and employees should be immediately informed in writing of the reasons for suspensions, denials, or revocations of clearances and access, and should be given the opportunity to appeal an adverse determination to a senior official or panel not involved in the original determination. A person who has been denied a clearance or had a clearance revoked should be allowed to reapply after a determined period of time.

Increasing Clearance Reciprocity and Standardization

Agencies often do not accept the clearances of government employees who transfer from one agency to another, or of contract employees who wish to work on projects

The Defense Department has estimated that by the year 2001, without additional resources or major system improvements, SSBIs will take an average of 278 days. Currently, DIS completion time for SSBIs is between 175 days and 220 days.

for multiple agencies. Agencies frequently criticize the quality of each other's investigations and adjudications. As one result, they insist on duplicating lengthy and costly procedures even though an individual's clearances are current. Representatives of industry have expressed frustration over the frequency with which contractors are investigated and adjudicated, with some citing cases in which individuals were reinvestigated repeatedly during a single year because they required access to multiple programs.

In order to improve clearance reciprocity between government agencies, the interagency Security Policy Board has agreed on minimum investigative standards across the Federal Government; these have been forwarded to the White House for review. However, a significant exception to this policy remains because these are only *minimum* standards. Thus, agencies are still permitted to retain specific additional security requirements, thereby limiting the extent to which there can be genuine reciprocity of clearances.

In addition to this lack of clearance reciprocity, the system is also made less efficient by the failure to standardize the personnel security questionnaires that are used. An April 1995 OMB memorandum prescribed one form, Standard Form 86, for use by Federal agencies in security clearance background investigations.[5] This new requirement has yet to be fully implemented, however, because the form was written for a background investigation covering seven years, while the standards for investigative components for a Top Secret clearance with access to Sensitive Compartmented Information (SCI) have since changed and now vary from three to ten years. As a result of these differences, several agencies continue to use agency-specific forms. The longstanding objectives of greater uniformity, reciprocity, and cost effectiveness in the clearance process appear to be a considerable distance from actually being realized.

Recommendation

The Commission recommends that individuals in both Government and industry holding valid clearances be able to move from one agency or special program to another without further investigation or adjudication. The single exception to this true reciprocity of security clearances shall be that agencies may continue to require the polygraph before granting access.

This approach would reduce the "dead time" often facing cleared employees and contractors when they transfer to other agencies or projects. The Government would no longer have to pay for employees to sit idle and there would be less likelihood of losing quality personnel who do not want to wait long periods for the completion of additional clearance procedures.

Enhancing Investigative Quality

Standards vary widely for the hiring, training, and continuing education of personnel security investigators, adjudicators, and security officers. This can contribute to inconsistent quality in both investigations and adjudications.

The standards for personnel security investigators and adjudicators have changed over time. At one point, the Justice Department's Bureau of Investigation (later the FBI) had the authority to conduct all investigations of those in sensitive positions, and almost all of its agents, who conducted the investigations, were required to have a degree in either law or accounting. As the number of personnel requiring background investigations rose substantially following World War II (pursuant to President Truman's Executive Order 9835 in 1947 and then President Eisenhower's Executive Order 10450 six years later), and as the chief responsibility for investigations shifted to the Civil Service Commission, hiring requirements for investigators were eased. Today, despite the great emphasis placed on the background investigation, standards for investigators and adjudicators are minimal; usually a bachelor's degree in any field will suffice, though it is not a requirement.

In addition, there are no common standards for training or continuing education: initial training usually consists of four weeks of classes and is followed by varying periods of on-the-job training. The Defense Investigative Service, for example, has had a hiring freeze since 1991 and only conducts sporadic training for its investigators. Although the DIS is reviewing its continuing education practices, senior DIS officials recognize that they face, as one acknowledged, "a crisis situation because we know our people are not receiving training."[6] The OPM has no continuing education requirements. And the Federal Government, because it recently privatized its investigations division, must monitor the standards set for hiring qualifications, training, and education by the successor to its Federal Investigations Service, the U.S. Investigation Service, Inc.

Reducing Inefficiencies in the Processing of Cases

According to a 1993 study by the Defense Department's Personnel Security Research Center (PERSEREC), over 96 percent of all DoD personnel security adjudications were favorable.[7] Even so, cases with either no or only minor derogatory information usually are reviewed closely by *two* officials: an adjudicative specialist and a supervisor. This procedure is applied even after a case has had an initial review for investigative sufficiency by two officials, the specialist directing the investigation and a supervisor, before being forwarded to the adjudication office. Because of large caseloads and first-in, first-out processing, even cases without derogatory information (termed "clean" cases) are sometimes held up behind cases with substantial derogatory information that take much longer to adjudicate.

Time delays can inconvenience applicants and waste significant resources. Both the Government and private industry can lose qualified applicants who do not have the patience or resources to wait, sometimes up to a year or more, to find out whether or when they can begin work. The GAO has estimated that these processing delays cost the Government $920 million a year in productivity losses;[8] these costs will only increase as delays worsen.

Derogatory Information

Minor Derogatory: Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative security clearance determination.

Moderate Derogatory: Information on the basis of which an unfavorable administrative security clearance determination may not necessarily be made, but which obligates the investigative agent to pursue its development.

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

To alleviate the delays in the clearance process, adjudicative offices should consider establishing fast-track procedures by handling clean cases first, rather than holding them in line behind cases with derogatory information that require more detailed analysis and processing. If the required level of investigation has been undertaken and no derogatory information has been revealed, the adjudicative office would issue a clearance immediately with only one review.

Establishing fast-track adjudications would eliminate a second adjudicative review, thus saving time and resources, reducing adjudicative backlogs (which are extensive and growing in several agencies), and permitting adjudicators to focus more time on serious derogatory cases. Expedited processing of clean cases would provide a good example of applying risk assessment principles in an era of diminishing personnel security resources. The NRO, for example, already uses this method successfully, contributing to its average processing time of under 60 days.

Addressing Transparency and Due Process Concerns

Most agencies make little effort to disseminate any information regarding the personnel security process to applicants, contractors, and employees subject to investigation or reinvestigation. These individuals thus remain largely uninformed with respect to basic, unclassified information concerning the overall process, the length of time it takes, the standards applied, and their own status.

For example, personnel security officials from one agency reported that approximately 10 percent of applicants withdraw from consideration after having applied for a security clearance—often because they can no longer afford to wait. Contractors also voiced concerns that the system is not accountable to its customers. For example, if the contractor calls to check on the status of an employee, the agency in question often cannot determine where the individual stands in the clearance process. In addition, those subjected to the clearance process often do not understand it. Some assume, for example, that they will be denied a clearance for reasons that are not actually grounds for rejection. Moreover, security officials in many agencies often do not know or understand the investigative or adjudicative processes of other agencies.

While Executive Order 12968 attempts to address other concerns about the fairness of the personnel security process, it does not include provisions that are designed to

improve the basic understanding and transparency of the process. Applicants or employees who have their clearances denied, suspended, or revoked, and who are not provided a reason, are effectively denied due process, even though Executive Order 12968 explicitly calls for improvements in this regard.

Allocating Resources More Effectively

Shortcomings in the initial screening process appear to account, at least in part, for the hiring of two spies: Karl Koecher, arrested in 1984, and Larry Wu-Tai Chin, arrested in 1985**,** both of whom were agents of foreign intelligence services when hired.[9] These cases, however, are the rare exception; other spies, including those responsible for the most damaging espionage incidents in recent years, turned to espionage only after many years of trusted Government service, and very rarely with ideological motivations.

Data from the PERSEREC and Project SLAMMER, a study of post-World War II espionage cases, confirm that few persons join the Government or begin contractor employment with the intent of committing espionage.[10] The main threat instead comes from trusted "insiders," those who already hold clearances and only much later in their careers decide to commit espionage. Even so, the personnel security system established under Executive Order 10450 consistently has allocated most resources to the initial clearance process, based on the once-prevailing concerns about the Soviet Union and its allies placing espionage agents inside the U.S. Government.

The Difficulties of Talking to Neighbors

"The neighbors are never at home unless it is in the evening or on the weekend, and often do not want to talk to strangers, regardless where they say they are from. Single women often will not open their doors for someone they don't know, regardless of whether he or she has a badge. Possibly the biggest problem is that neighbors do not want to say anything that can potentially subject them to a lawsuit."

-- Intelligence Community Investigators

This focus on the initial clearance has shortchanged the allocation of resources and attention to reinvestigations and continuing assessment programs. Continuing assessment programs and reinvestigations often are the first areas subjected to budget cuts. For example, the DIS announced in 1995 that, due to diminishing resources, it could no longer conduct periodic reinvestigations on a routine basis and would establish an annual 5 percent ceiling on all counterintelligence-scope polygraphs for current employees. While this policy was later modified to place decisions on initiating reinvestigations with the heads of agencies (after senior NSA officials voiced concern), questions regarding the *quality* of reinvestigations have not been addressed.

In a period of declining resources, the Federal Government also should target its security dollars toward the most productive elements of the investigation: those that yield the most substantial information relevant to the clearance decision. The most productive source overall for developing derogatory information, according to a 1996 PERSEREC report, was the person under investigation: the report noted that in 81 percent of the cases in which incriminating information was uncovered, the individual subject provided such information through the interview or on the personnel security questionnaire.[11]

Some elements of an initial background investigation are much more productive than others; those that are the most productive include interviews with former spouses and employers, medical professionals, relatives, and listed or developed character references.[12] The least productive sources include neighborhood interviews, which are also the most expensive and time consuming.[13] Interviews with education references also are not productive, according to this and other studies.

The limited utility of neighborhood interviews should not be surprising. The practice of interviewing neighbors is based on a vision of America as it once was—with individuals living in the same geographic areas most of their lives, enabling investigators to glean useful information from local sources with relative ease. Today, this is less often the case, given greater personal mobility, privacy concerns, and the litigiousness of society. When the difficulty of gaining access to neighbors and the time and substantial expense of the procedure are also factored in, the notion that neighborhood interviews should be done routinely as part of every background investigation requires reassessment.

The Security Policy Board has implicitly acknowledged the limited usefulness of neighborhood interviews by agreeing to limit their scope to three years for Top Secret/SCI clearances. The Commission believes that the time has come to go further; in view of the limited resources often available and the need to prioritize, it is important to focus on the most productive elements of the personnel security investigation. The Commission recommends the following steps to reallocate investigative resources and focus on the most productive aspects of the investigation.

Recommendation

The Commission recommends that current requirements for neighborhood interviews and for interviewing educational references in every investigation be eliminated.

Under the above proposal, neighborhood interviews and checks of educational references still would be allowed where personnel security officials believe that the information yielded from these interviews would be productive; they simply would not be *required* in every investigation. This proposed approach is consistent with the critical objective of achieving increased reciprocity through greater standardization of personnel security procedures; it would promote common standards across the Government that make sense in view of existing resource constraints.

Greater attention needs to be directed toward making continuing evaluation programs more effective. For example, using existing public and private data bases—with the express advance permission of the individual under review—to periodically scan for criminal history, as well as for credit, travel, and business history, normally would provide more accurate information at less cost than standard field reinvestigations.

Personnel security professionals could monitor the behavior and activities of cleared personnel on a continuous basis in a more effective, cost-efficient, and nonintrusive manner. Given the evidence that there is little likelihood of catching spies through the current standard investigative or reinvestigative process, better continuing assessment programs could enhance the probability of deterring or identifying espionage activities.

Recommendation

The Commission recommends that greater balance be achieved between the initial clearance process and programs for continuing evaluation of cleared employees.

Most of the information needed is already available on existing databases; private industry experiences suggest that efforts to utilize automation to access such data can be very cost-effective as well as productive. Nevertheless, because some automated tools can be expensive, a cost-benefit assessment should be completed prior to utilizing them.

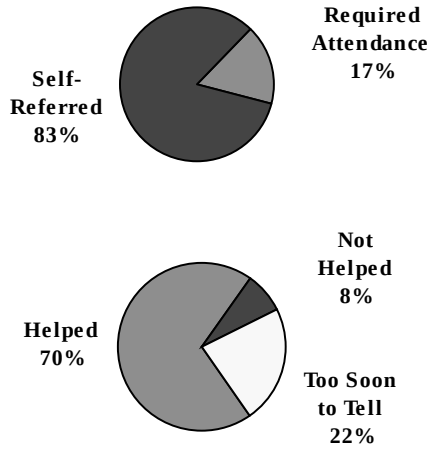
Resources should be focused on those individuals in the most sensitive positions or where there is some evidence of suspect behavior; in an era of diminishing resources and frequent budget cuts, more effective continuing assessment can be accomplished only by concentrating on the areas of greatest vulnerability. In addition, those holding what are identified as the most sensitive positions could be subjected to more frequent, "in house" reviews similar to the personnel reliability programs used by the Defense and Energy Departments, as described above. These measures provide a cost-effective way to monitor and assess employees with greater regularity and frequency, but without necessarily having to direct additional resources toward the traditional field investigation.

Strengthening Employee Assistance Programs

The focus on the initial investigation has also limited the attention and resources given to programs intended to assist current employees. These programs, generally termed Employee Assistance Programs (EAPs), are critical in ensuring that employees can receive professional assistance if they face serious personal problems. Despite a requirement in the Federal Employee Substance Abuse Education and Treatment Act of 1986, as well as evidence of their benefits, standards for EAPs across the Federal Government do not exist. Furthermore, it is often not clear to the employee whether attending an EAP would harm his or her career. Both the quality of such programs and the resources made available for them also vary widely from agency to agency. The Commission therefore supports efforts to strengthen these programs. According to 1994 figures, 79,742 employees turned to EAPs for help.[14] The cost for EAPs varies considerably, ranging from $8 to $50 per employee.[15] Although some

employees may never seek the help that they need, others may seek or can be directed to seek mental health or job counseling, as shown in Figure 5. While the number of individuals who did not commit espionage as a result of successful counseling is impossible to quantify, helping cleared employees cope with their personal problems almost certainly will deter some incidents of espionage and other major security breaches.

Figure 5: Federal EAP Statistics



Source: Office of Personnel Management, *Fiscal Year 1994: Report to Congress Title VI of Public Law 99-570* (Washington, D.C.: Government Printing Office, September 1995), 5-7.

The maintenance of confidentiality is and should remain a key element of such programs. Employees having emotional and financial difficulties are less likely to seek counseling if there is a perception that confidentiality is either nonexistent or poorly maintained, and that reprisals from security officials are possible. For example, convicted spy James Hall reportedly had sought help for his alcoholism from a military EAP, but declined to return after a counselor warned that attending one could damage his career. Confidentiality policies for EAPs should include nondisclosure of files and information garnered during the course of counseling, except in cases where confidentiality is prohibited by law (such as when there is admission of child abuse, intent to do harm, or other criminal activity).

One additional issue with respect to EAPs is whether contractor employees should be eligible. Most government agencies are prevented under the Federal Employee Substance Abuse Education and Treatment Act of 1986 from offering any EAP services to contractor employees and their families. While some larger firms are able to fulfill this function in-house, smaller companies often do not have the resources to create an EAP. Because contractor employees may have access to the same national security information as Federal employees, agencies that work with them should have the option of offering the services of EAPs to contractor employees in certain circumstances (without being required to do so). NSA officials, for example, have said that they would like to be able to provide EAP services to contractor employees from smaller companies, but cannot do so at present because of the legal restriction.

Assessing the Value of Financial Disclosure

Under the 1995 Intelligence Authorization Act, all Executive Branch employees with access to "particularly sensitive classified information" must complete a financial disclosure form. In April 1995 (while what became Executive Order 12968 was still under interagency review), Acting Director of Central Intelligence William Studeman announced that all CIA employees and agency contractors would be required to submit annual financial disclosure forms. Executive Order 12968, issued in August 1995, requires that the "head of each agency" designate those employees (including industrial contractors, members of the Armed Forces, and civilian employees) who would be subject to this reporting requirement.

Studies, including Project SLAMMER, demonstrate that interest in financial gain is one of the leading motivations for espionage and other criminal activities.[16] Primarily as a

result of the Aldrich Ames case, the Congress (through the 1995 Intelligence Authorization Act) and the Executive Branch (through Executive Order 12968) determined that a new financial disclosure form was needed for those who have access to very sensitive information. The form would be used in addition to credit reports, other financial information collected, and the consent form that individuals sign, which allows access to an individual's financial information provided the investigator can show cause.

The requirement for a new financial disclosure form has generated considerable debate among those responsible for its implementation. For example, nearly all members of the SPB's Personnel Security Committee have expressed the view that using such a form would not meaningfully enhance personnel security and that the concerns raised over the past two years by industry (including cost, use of the data collected, and maintenance of the data's confidentiality) have not been addressed adequately.

While Executive Order 12968 provides fairly specific guidelines to assist agency heads in deciding who is required to fill out a financial disclosure form, agency officials, employees, and contractors have voiced concern over how officials will interpret the Order's provisions. They also are concerned that collecting the financial data by this method will be a costly endeavor with limited returns. The CIA and the Customs Service, two agencies that have been using a financial disclosure form, have not yet quantified the effectiveness of their forms. Furthermore, once the information has been collected, there is continued uncertainty over whether the Government has the resources or technical capability to analyze it in a meaningful way.

Finally, there is still considerable uncertainty concerning whether the financial information collected should be used as an analytical or investigative tool. If investigators use the form simply as an investigative tool, it may provide very little added value to the consent forms that all employees with security clearances already are required to sign. If it is used as an analytical tool, adjudicators would use that information in their security eligibility determinations, as they currently use credit reports and other available information.

Recommendation

The Commission recommends that both the Congress and the Executive Branch reevaluate the requirement to utilize a new financial disclosure form and consider staying its implementation until there is further evaluation concerning how it would be used and whether its benefits exceed its costs. The Congress and the Executive Branch should review alternative approaches to improving data collection, including utilization of the expanded access to certain financial and travel records provided for under Executive Order 12968.

Advancing Polygraph Research

Senior officials from agencies that use the polygraph see it as a significant tool because of its utility in generating admissions of wrongdoing, either during the pre-test, test, or post-test period. The polygraph saves time and money, and it serves as a deterrent by eliminating some potential applicants from seeking a highly sensitive position in the first place. The polygraph examination is conducted before the background investigation, saving additional resources should the applicant be rejected as a result of polygraph admissions. According to a May 1993 NSA letter to the White House, "over 95% of the information the NSA develops on individuals who do not meet federal security clearance guidelines is derived via [voluntary admissions from] the polygraph process."[17]

Because disparities exist in the procedural safeguards employed by different agencies for those employees requiring access to highly sensitive information, full reciprocity of security clearances between the agencies cannot be achieved. While the polygraph is used to screen employees at the CIA, NRO, DIA, NSA, and FBI (which resumed screening in 1993), the White House, NSC, State Department, and Congress have traditionally resisted adopting polygraph screening. Even among the agencies that use the polygraph, the scope, methods, and procedural safeguards may diverge.

Agencies that Use the Polygraph for Employment Screening

Central Intelligence Agency
Defense Intelligence Agency
Drug Enforcement Agency
Federal Bureau of Investigation
National Security Agency
National Reconnaissance Office

Although the polygraph is useful in eliciting admissions, the potential also exists for excessive reliance on the examination itself. A related concern is that too much trust is placed in polygraph examiners' skills, creating a false sense of security within agencies that rely on the polygraph.[18] The few Government-sponsored scientific research reports on polygraph *validity* (as opposed to its utility), especially those focusing on the screening of applicants for employment, indicate that the polygraph is neither scientifically valid nor especially effective beyond its ability to generate admissions (some of which may not even be relevant based on current adjudicative criteria).[19] Many senior intelligence community officials, however, have told Commission members that they believe the polygraph is scientifically valid.

A 1989 Department of Defense Polygraph Institute (DoDPI) study found that 60 percent of subjects were incorrectly cleared in a test that measured the subject's knowledge or guilt of a crime. The results of this test concluded that the ability to identify those guilty or knowledgeable of a crime "was significantly worse than chance."[20] The DoDPI study, however, was conducted in a controlled setting, and, therefore, may not accurately reflect the conditions under which a polygraph is normally taken. (Another report, a detailed 1991 FBI study entitled "Polygraph Examinations in Federal Personnel Security Applications," is classified in its entirety, and so the Commission cannot reference any of its substantive findings or recommendations in this unclassified report.)

Past commissions, an internal CIA working group, and several other studies have also called for additional research concerning polygraph accuracy.[21] However,

comprehensive research into the accuracy of the polygraph has not been funded, despite the fact that the President's Foreign Intelligence Advisory Board in 1988 recommended that the Director of Central Intelligence fund all future requests for studies on screening accuracy. Moreover, despite DoDPI's efforts to manage an effective research program in recent years, little support for it appears to exist within the broader scientific community, primarily because there is no open and objective peer review of DoDPI's research.

The Commission believes that the following would improve understanding of both the polygraph's utility and its scientific validity, thereby promoting better informed decisions concerning its use.

Recommendation

The Commission recommends that:
(1) the director of scientific research at the Department of Defense Polygraph Institute (DoDPI) establish a committee that includes cleared, outside scientific experts to develop a coherent research agenda on the polygraph; initiate and participate in a small grant program to stimulate independent research outside the Government; and review and comment on scientific progress and the quality of government-sponsored research in this field; and
(2) independent, objective, and peer-reviewed scientific research be encouraged as the best means to assess the credibility of the polygraph as a personnel security tool and identify potential technological advances that could make the polygraph more effective in the future.

Making the Clearance Process More Efficient Through Automation

Although steps have been taken to automate elements of the personnel security process within various agencies, there is no overall vision of how the personnel security system should operate in the Information Age. Most of the system still remains tied to a slow-moving, paper-based world, rather than functioning through a sophisticated system of interconnected computers.

Recently developed, and potentially very promising, innovations include the pre-screening software program "Military Applicant Screening System" (MASS), developed at the PERSEREC, which leads military applicants through a series of questions to determine whether or not they would be eligible for a clearance. If the applicant would be ineligible for a clearance, military recruiters can direct the applicant

to another position for which a clearance is not required, thereby saving scarce investigative resources.

Other new developments include PERSEREC's "Adjudicator's Desktop Reference Guide," which stores a broad array of guidelines, laws, and statistical information to help adjudicators make final clearance decisions. Under review within the Security Policy Board is a common identification badge that will allow personnel from one agency to travel to another agency without having to undergo the traditionally cumbersome process of passing clearances.

The Commission endorses these and other examples of automation of the personnel security system, and recommends a more coordinated approach to developing additional programs. For example, building on the progress already made, a "Personnel Assurance System" index could be developed to rank employees by the degree of harm they could inflict, based on the sensitivity of their position and an assessment of the relevant threat, as well as on their level of clearance. Those in the most sensitive positions would be subject to more frequent and more detailed adjudication.

In addition, improved computer programs could be created that are capable of continually scanning different databases (e.g., that of the Treasury Department, consumer credit reports, national criminal databases, and other commercially available databases) for suspect behavior or other indicators of potential problems. Existing public databases today include vast amounts of information on all facets of personal finances and holdings. Consistent with applicable privacy requirements, officials should use these databases as valuable open source information to assist in personnel security decisions.

The Commission believes that a more efficient, partially automated personnel investigative process could be created using already-available technologies. The Defense Investigative Service and the OPM Federal Investigations Processing Center already have embarked on multimillion-dollar projects that will automate much of the initial personnel security investigative process for civilian, military, and industrial contractor employees; the objective now is to find a way to integrate these automation projects into the entire personnel security process.

Conclusion

From the time of its inception following World War II, the personnel security process has remained vital to the protection of national security information. Unfortunately, the process has not evolved to meet current national security needs.

A number of problems prevent the personnel security system from operating efficiently and effectively. For example, the authorities governing the clearance process are disjointed and outdated, which leads to confusion both for the administrators and for customers of the process. Attempts to revamp the system have resulted in ad hoc or piecemeal solutions, such as the financial disclosure form inspired by the Aldrich Ames espionage case, that tend to address only the most recent high-profile espionage cases rather than the underlying problems of the system. Fewer government resources have led to a dangerous focus on initial investigations at the expense of

reinvestigations, even though recent studies have shown that individuals now typically turn to espionage only after years of government service. Moreover, too many of the remaining resources are being used for less productive investigation elements, such as neighborhood checks or redundant investigations for contractors and Federal employees who transfer between agencies.

The solutions for these problems must come from a fundamental reevaluation of the personnel security system, rather than from temporary fixes. A successful security clearance process commences when an applicant applies for a security clearance, but it must continue with frequent and productive reinvestigations, better employee assistance programs for troubled employees, and improved general security awareness by managers and coworkers. Some recent innovations have demonstrated how automation can improve the system; a coordinated approach to developing further such programs is desirable.

The Commission believes that the proposals set out above will move the personnel security system in the desired direction. Guiding principles will lead personnel security officials to a better understanding of their mission and responsibilities. Increased reciprocity will allow employees to transfer more easily between agencies without redundant investigations. Reallocating resources based upon the need for greater balance between the initial clearance process and continuing assessment programs will provide more protection against "trusted" insiders who can cause serious damage to our nation's security. Finally, an evaluation of the tools of the personnel security system, such as the polygraph, will help ensure that they further the aims of the overall process.

---

[1] General Accounting Office, *Background Investigations: Impediments to Consolidating Investigations and Adjudicative Functions*, GAO/NSIAD-95-101 (Washington, D.C.: Government Printing Office, March 1995), 12.
[2] Ibid., 11.
[3] Office of Personnel Management, Federal Investigations Notice 95-4, 1 August 1995.
[4] Carl Builder, Victor Jackson, and Rae Starr, *To Repair or Rebuild: Analyzing Personnel Security Research Agendas*, R-3652-USDP (Santa Monica: RAND, September 1988), 11.
[5] Office of Management and Budget, Memorandum for Senior Information Resource Management Officials: Approval of Standard Suitability and Background Investigation Questionnaires (Office of Management and Budget, Washington, D.C., 11 April 1995).
[6] Defense Investigative Service Official, telephone conversation with Commission staff, 20 June 1996.
[7] Defense Personnel Security Research Center, *Report on Personnel Security* (Washington, D.C.: Department of Defense, 1994), 20.
[8] Comptroller General, *Report to the Congress of the United States: Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses*, GGD-81-105 (Washington, D.C.: General Accounting Office, 15 September 1981), ii.
[9] Department of Defense Security Institute, *Recent Espionage Cases: Summary & Sources* (Richmond: Department of Defense Security Institute, July 1994), 12, 15.
[10] Suzanne Wood and Martin Wiskoff, *Americans Who Spied Against Their Country Since World War II*, PERS-TR-92-005 (Monterey: Defense Personnel Security Research Center, May 1992), 26.

[11] Ralph M. Carney, *SSBI Source Yield: An Examination of Sources Contacted During the SSBI* (Monterey: Defense Personnel Security Research Center, 1996), 6.
[12] Ibid., 15.
[13] Personnel Security Working Group et al., *Evaluation of DCID 1/14 Investigative Requirements* (Washington, D.C.: Director of Central Intelligence, April 1991), 31.
[14] Office of Personnel Management, *Fiscal Year 1994: Report to Congress on Title VI of Public Law 99-570* (Washington, D.C.: Government Printing Office, September 1995), 1.
[15] Ibid., 12-20.
[16] Willis Reilly and Paul Joyal, *Project SLAMMER: A Critical Look at the Director of Central Intelligence Directive No. 1/14 Criteria* (Washington, D.C.: Director of Central Intelligence, 1993), 25-28. Project SHADOW is the name given to a current DoD Security Institute project to reinterview the subjects of Project SLAMMER and produce new videotapes for the purpose of developing better security education and awareness information. Department of Defense official, telephone conversation with Commission staff, 12 January 1997. See also Jeff Stein, "Treason on Their Minds: 'Project Shadow' Aims to Spot Moles Earlier," *Washington Post*, 12 January 1997, C2.
[17] National Security Agency, letter to Holly Gwin, White House Office of Science and Technology, 4 May 1993.
[18] House Permanent Select Committee on Intelligence, Report on *United States Counterintelligence and Security Concerns* (1986).
[19] See Office of Technology Assessment, *Scientific Validity of Polygraph Testing: A Research Review and Evaluation—A Technical Memorandum,* OTA-TM-H-15 (Washington, D.C.: Office of Technology Assessment, November 1983); House Permanent Select Committee on Intelligence, *United States Counterintelligence and Security Concerns*; Department of Defense Polygraph Institute, *Study of the Accuracy of Security Screening Polygraph Examinations.* For additional information and examples of studies that found the polygraph was scientifically valid in certain applications, see Department of Defense Polygraph Institute, *Bootstrap Decision Making for Polygraph Examinations,* final report of DOD/PERSEREC Grant No. N00014-92-J-1795 prepared by Charles R. Honts and Mary K. Devitt (Grand Forks: University of North Dakota, 24 August 1992); Charles R. Honts, *Theory Development and Psychophysiological Credibility Assessment* (Boise: Boise State University, 1996); Charles R. Honts, *1994 Final Report: Field Validity Study of the Canadian Police College Polygraph Technique*, Science Branch: Supply and Services Canada, contract #M9010-3-2219/01ST (Grand Forks: C. Honts Consultations, 1994); Christopher J. Patrick and William G. Iscono, "Validity and Reliability of the Control Questions Polygraph Test: A Scientific Investigation," SBR Abstracts, *Psychophysiology* 24, no. 5 (September 1987):604-05.
[20] Gordon Barland, Charles R. Honts, and Steven Barger, *Studies of the Accuracy of Security Screening Polygraph Examinations* (Fort McClellan: Department of Defense Polygraph Institute, 24 March 1989), iii.
[21] Office of Technology Assessment, *Scientific Validity of Polygraph Testing*, 102.