DEFENSE SECURITY SERVICE OVERSIGHT

HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

FEBRUARY 16, 2000

Serial No. 106–152

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

66–789 CC WASHINGTON : 2000

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
LISA SMITH ARAFUNE, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

MARK E. SOUDER, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
DAVID M. MCINTOSH, Indiana
MARSHALL "MARK" SANFORD, South Carolina
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
HELEN CHENOWETH-HAGE, Idaho

ROD R. BLAGOJEVICH, Illinois
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
JOHN F. TIERNEY, Massachusetts
THOMAS H. ALLEN, Maine
EDOLPHUS TOWNS, New York
BERNARD SANDERS, Vermont (Independent)
JANICE D. SCHAKOWSKY, Illinois

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
J. VINCENT CHASE, *Chief Investigator*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

CONTENTS

	Page
Hearing held on Febaruy 16, 2000	1
Statement of:	
Cunningham, General Charles, Director, Defense Security Service; and General Larry D. Welch, chairman, Joint Security Commission	36
Schuster, Carol R., Associate Director, National Security International Affairs Division, U.S. General Accounting Office; Christine A. Fossett, Assistant Director, National Security International Affairs Division, U.S. General Accounting Office; and Rodney E. Ragan, Senior Evaluator, National Security International Affairs Division, U.S. General Accounting Office	2
Letters, statements, et cetera, submitted for the record by:	
Chenoweth-Hage, Hon. Helen, a Representative in Congress from the State of Idaho, prepared statement of	118
Cunningham, General Charles, Director, Defense Security Service, prepared statement of	39
Schuster, Carol R., Associate Director, National Security International Affairs Division, U.S. General Accounting Office:	
Budget for investigations and other missions of the DSS	27
Contract costs for Personnel Security	29
DSS cost breakdown	31
Personnel Security Investigation workload	25
Prepared statement of	5
Welch, General Larry D., chairman, Joint Security Commission, prepared statement of	66

DEFENSE SECURITY SERVICE OVERSIGHT

WEDNESDAY, FEBRUARY 16, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS, AND INTERNATIONAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2247, Rayburn House Office Building, Christopher Shays (chairman of the subcommittee) presiding.

Present: Representatives Terry and Mica.

Staff present: Lawrence J. Halloran, staff director and counsel; J. Vincent Chase, chief investigator; David Rapallo, minority counsel; and Earley Green, minority staff assistant.

Mr. SHAYS. I call this hearing to order.

The Department of Defense [DOD], relies on personnel security investigations to determine whether individuals should have access to classified information. It is a process critical to safeguarding the national security. Currently, more than 2 million military, civilian, and Defense contractor/employees hold confidential, secret, and top secret security clearances; all of which require periodic re-investigation.

The agency responsible for policing access to national secrets, DOD's Defense Security Service, referred to as DSS, has encountered very serious, very persistent problems. In October, the General Accounting Office [GAO], reported that, "DOD personnel security investigations are incomplete and not conducted in a timely manner. As a result, they pose a risk to national security by making DOD vulnerable to espionage."

GAO reported a backlog of more than 600,000 re- investigations and deviations from investigative standards in the vast majority of completed cases. How did so vital an element of the national security apparatus fall into such disrepair? Based on a widely publicized case of espionage in 1997 by a DOD employee holding a clearance, our colleague, Representative Ike Skelton from Missouri, ranking member of the House Armed Services Committee, asked GAO to reassess the rigor and consistency of DOD's personnel security investigations.

Their findings portray an agency mismanaged and reinvented to the point of corrupting its core mission to provide timely thorough background investigations upon which clearance granting agencies could confidently rely. New leadership at DSS has a plan to address the backlog: increase the quantity and quality of personnel security investigations, and maintain investigative standards.

Today, we will examine the particulars of that plan, ask how realistic DSS projections are, what it will cost to implement them, and when we can expect to see real progress. Despite the end of the cold war, threats to our national security remain, more diffused, but no less determined to do us harm, our foes will seek to exploit any lapse in vigilance and any lack of caution.

The DSS stands guard at a critical post in the New World Order. It must be able to perform the mission. I would like to welcome all of our witnesses and guests today. In the months ahead, we will convene again to measure DSS progress against the goals and benchmarks that I think will be discussed today.

At this time, I would call our first panel and invite them to stand and be sworn in. Carol R. Schuster, Associate Director, National Security International Affairs Division, GAO; Christine A. Fossett, Assistant Director, same division; Rod E Ragan, Senior Evaluator, at the same division, if all three, thank you.

[Witnesses sworn.]

Mr. SHAYS. Thank you very much. I note for the record that all witnesses responded in the affirmative to that question. Ms. Schuster, we welcome your testimony. Thank you. The bottom line is we have 5 minutes. Then we will roll over another 5, and we will roll over again if we need to. So, you take what you need to. Our other witnesses will have that same privilege.

STATEMENTS OF CAROL R. SCHUSTER, ASSOCIATE DIRECTOR, NATIONAL SECURITY INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE; CHRISTINE A. FOSSETT, ASSISTANT DIRECTOR, NATIONAL SECURITY INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE; AND RODNEY E. RAGAN, SENIOR EVALUATOR, NATIONAL SECURITY INTERNATIONAL AFFAIRS DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Ms. SCHUSTER. Mr. Chairman, we are pleased to be here today to present our findings related to background investigations conducted on DOD employees by the Defense Security Service. With your permission, I would like to briefly summarize my statement.

Mr. SHAYS. I am very sorry. I am very sorry. We have a vote. I think rather than interrupting you, so you all have about 10 or 15 minutes if you want to go get a coffee or something, I will be back.

[Recess.]

Mr. TERRY [presiding]. We will come to order again. As I understand, we were just beginning testimony. We might have been a few sentences into it. Ms. Schuster, pickup where you left off, or start at the beginning, whatever you feel comfortable with.

Ms. SCHUSTER. All right. We appreciate this opportunity to present our findings on our background investigations conducted on Department of Defense employees by the Defense Security Service. With your permission, I would like to briefly summarize my statement and ask that the entire statement be submitted for the record.

Mr. SHAYS. Yes, please, without objection.

Ms. SCHUSTER. First, let me underscore that safeguarding sensitive national security information is one of the most important re-

sponsibilities entrusted to public servants. It is therefore critical that only those individuals who have passed the scrutiny of rigorous background investigations be granted security clearances.

While it now appears that DSS is making positive steps to improve the thoroughness and timeliness of its investigations, our review conducted last year found serious lapses in both the thoroughness and timeliness of these investigations. This raises questions about the risks such lapses pose to national security. First, let me briefly summarize the findings with respect to the completeness of DSS investigations.

A complete investigation should cover all of the investigative areas required by Federal standards. Following these standards is important to ensure uniformity among the many entities involved in investigations and to provide reciprocity among agencies that grant clearances.

Yet, we found from our detailed analysis of 530 personnel security investigations, that the vast majority did not comply with Federal standards, such as verifying residency, citizenship, and employment. For example, 92 percent were deficient in at least one of the required areas. Seventy-seven percent did not meet the standards in two or more areas and 16 percent contained derogatory information that was not pursued, such things as past criminal history, alcohol and drug abuse, and financial difficulties.

All 530 individuals were granted top secret security clearances. The primary areas where we identified lapses were in confirming residency, corroborating birth or citizenship of foreign-born subjects and their spouses, verification of employment, interviews with character references, and criminal record checks at the local level.

Of particular concern to us were the cases where leads were not pursued. For example, one individual working in the Joint Staff had a credit report that showed that his mortgage was $10,000 past due and foreclosure proceedings had begun. Because this subject denied knowledge of this matter, it was not pursued. In another case, the subject's credit report revealed a bankruptcy, yet there was no followup.

In still another case, the subject claimed to be a citizen of another country and a member of a foreign military service. Character references alleged that he had been involved in a shooting. None of these matters were pursued. With respect to timeliness, we found that DSS investigations simply take too long. Defense agencies and contractors want investigations done within 90 days to avoid costly delays.

We have found that over half of the 530 investigations we examined, took over 204 days to complete. Less than 1 percent took less than 90 days, and 11 percent took more than a year. There are several problems with this. First, contractors have to wait too long to begin their work. This jeopardizes meeting performance, cost schedules, and drives up costs.

Second, individuals having their clearances updated continue to work with classified materials, even though their personal circumstances may have changed, rendering them unfit to retain their clearances. Third, central adjudication facilities, who evaluate the collective information to decide whether a clearance should be granted or denied sometimes rule favorably, even though informa-

tion is incomplete, because it could take another 6 months if the case was sent back for further investigation.

Finally, the backlog of cases awaiting periodic reinvestigation, as you pointed out, Mr. Chairman, has grown to at least 500,000. At the time of our review, it was 600,000. To put this into perspective, the total number of Defense employees who have clearances is about 2.4 million. We found several weaknesses that we believe contributed to the incomplete investigations that we found.

For example, we found that DSS relaxed its investigative requirements to give investigators greater discretion in how they might meet Federal standards. Because this guidance was not always consistent with Federal standards, investigators became confused as to what constituted a thorough investigation. DSS also eliminated two important quality control mechanisms: supervisory review of completed investigations and its Quality Assurance Branch.

DSS also provided almost no formal training on the new Federal standards to its investigators between 1996 and early 1999. DSS spent $100 million to implement an automated case management system that simply did not work. The problems that ensued added to the already large backlog of cases waiting to be investigated.

Another $100 million to $300 million may be needed to correct the problems. Importantly, because DSS had been named a re-invention laboratory under the administration's Reinventing Government Initiative, DSS was allowed to operate with much latitude and without the normal degree of oversight that would normally be expected.

Our October 1999 report makes several recommendations to the Secretary of Defense to fix these problems. For example, we recommended that the Secretary increase oversight of DSS operations, provide the necessary funding and priority to deal with the case backlog, bring policy guidance on DSS investigations in line with Federal standards, establish effective quality control and training mechanisms, take corrective action on the case automation problems, and direct adjudication facilities to grant clearances only when investigative work is complete.

We also recommended that the Secretary report the DSS Investigative Program as containing material internal control weaknesses under the Federal Managers Financial Integrity Act, and that a strategic plan, with measurable goals and performance measures be developed.

I am pleased to say that General Cunningham began taking corrective actions on these matters the very moment he assumed leadership of DSS in June 1999. I will leave it up to General Cunningham to outline the specific actions his agency is taking to correct these problems and ensure the integrity of the investigative process.

This concludes my statement. I would be pleased to respond to any questions that you might have.

[The prepared statement of Ms. Schuster follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m.
Wednesday
February 16, 2000

DOD PERSONNEL

Inadequate Personnel Security Investigations Pose National Security Risks

Statement of Carol R. Schuster, Associate Director, National Security Preparedness Issues, National Security and International Affairs Division

GAO/T-NSIAD-00-65

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our recent evaluation of Defense Security Service personnel security investigations.[1] This evaluation was conducted at the request of the Ranking Minority Member of the House Armed Services Committee, who was concerned about espionage committed by Department of Defense (DOD) employees who held security clearances. From 1982 through September 1999, 80 individuals were convicted of committing espionage against the United States; 68 of these were DOD employees, and all had undergone personnel security investigations and held security clearances.

The Defense Security Service is the key investigative agency responsible for conducting investigations of DOD's civilian and military personnel, consultants, and contractors.

Today, I would like to discuss the results of our analysis of a representative sample of Defense Security Service investigations completed in January and February 1999. Specifically, I will discuss (1) the completeness and timeliness of the agency's investigations, (2) the factors that contributed to the deficiencies we found, and (3) our major recommendations. But first, let me provide a brief summary of my testimony.

Summary

Safeguarding sensitive national security information is one of the most important responsibilities entrusted to public servants. Therefore, it is critical that only those individuals who have passed the scrutiny of rigorous background investigations be granted security clearances. Unfortunately, our evaluation of Defense Security Service personnel security investigations revealed serious lapses in the thoroughness and timeliness of the investigations, raising questions about the risks such lapses pose to national security.

Our detailed analysis of 530 personnel security investigations showed that the vast majority did not comply with federal standards for conducting such investigations. All of the individuals investigated were granted top secret security clearances even though Defense Security Service investigators had not always verified such basic information as residency, citizenship, or employment. We also found that Defense Security Service investigations have not been completed in a timely manner and that there

[1] *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks* (GAO/NSIAD-00-12, Oct. 27, 1999).

is a current backlog of over 600,000 cases for reinvestigation. As a result of these conditions, some of DOD's 2.4 million personnel currently holding security clearances may be handling sensitive national security information without having been thoroughly screened. In addition, in 1994, the Joint Security Commission reported that delays in obtaining security clearances cost DOD several billion dollars because workers were unable to perform their jobs while awaiting a clearance.[2]

In examining the reasons for these deficiencies, we identified a series of ineffective management reforms at the Defense Security Service that occurred from 1996 through early 1999. We found that the Defense Security Service—in an effort to streamline operations and improve efficiency—relaxed its investigative guidance, eliminated key quality control mechanisms, inadequately trained its investigators, and ineffectively managed automation of its case processing system. However, the underlying cause of the Defense Security Service's problems is insufficient oversight of its operations by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). We believe that these factors led to incomplete investigations and exacerbated the growing backlog of uninvestigated cases.

Our report made a series of recommendations to improve the overall management of the personnel security investigation program. These recommendations include identifying the program as containing material internal control weaknesses in DOD's next report to the President and the Congress in accordance with the Federal Managers' Financial Integrity Act. We also recommended that the Secretary of Defense require the Defense Security Service Director to develop a strategic plan and performance measures to improve the quality of the investigative work and correct other identified weaknesses. DOD agreed with all of our recommendations and is in the early stages of making the necessary changes. However, because of the seriousness and breadth of the problems, it may take several years and many millions of dollars before all of the necessary improvements are made.

Background

Because of the importance of our methodology to our results, I would like to provide some background information on how we selected cases for our evaluation and how we determined whether investigations were complete. To obtain the most recent cases possible, we selected a random sample of investigations completed by the Defense Security Service (DSS)

[2]The Joint Security Commission was established in May 1993, by the Secretary of Defense and the Director of Central Intelligence to review security policies and procedures. It was convened twice and issued reports on its work in 1994 and 1999.

in January and February 1999. We drew our sample from DSS's four largest customers: the Air Force, the Army, the Navy, and the National Security Agency. Although our findings are projectable only to the investigations done for these four DOD components, these entities accounted for 73 percent of the investigative work done by DSS in fiscal year 1998. Therefore, our findings suggest systemic program weaknesses.

To ensure the objectivity of our analysis, we used the federal investigative standards approved by the President in 1997, which apply to all federal departments and agencies. All investigations must be conducted in accordance with these standards, which are designed to help determine whether individuals can be trusted to properly protect classified information. For top secret clearances, these standards require investigations in the following nine areas:

- corroboration of a subject's date and place of birth, and verification of citizenship for foreign-born subjects and their foreign-born immediate family members;
- corroboration of education;
- verification of employment for the past 7 years and interviews with supervisors and co-workers;
- interviews with character references and former spouses;
- interviews with neighbors to confirm residences;
- a national agency check on the subject and spouse or cohabitant, using files and records held by federal agencies (such as the Federal Bureau of Investigation);
- a financial review, including a credit bureau check;
- a local agency check of criminal history records and other public records to verify any civil or criminal court actions involving the subject; and
- a personal interview of the subject.

We employed several methods to ensure the accuracy of our review of DSS investigations. First, we developed a data collection instrument that incorporated the federal investigative standards and had it reviewed by officials from the office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) and the Army's adjudication

facility.[3] Second, two GAO staff reviewed each sampled investigation to ensure that no important investigative information was overlooked. Third, to ensure the accuracy of our work, we returned a random subsample of deficient investigations to the Air Force, the Army, the Navy, and the National Security Agency adjudication facilities for their review.

DSS Investigations Lacked Required Information

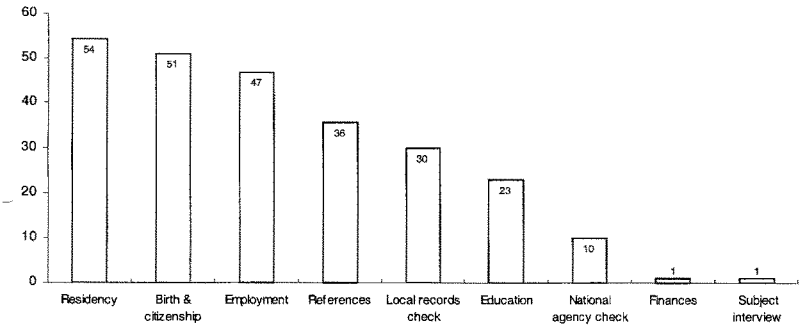
In the 530 cases we reviewed, DOD granted top secret clearances notwithstanding that

- 92 percent of the 530 investigations were deficient in that they did not contain information in at least one of the nine required investigative areas; and
- 77 percent of the investigations were deficient in meeting federal standards in two or more areas.
- The Air Force, Army, Navy, and National Security Agency adjudication facilities agreed with our findings.

As shown in figure 1, we found problems primarily in six of the nine areas that the federal standards require for a security clearance investigation. Frequently, DSS did not obtain the following information: confirmation of residency; corroboration of birth or citizenship for a foreign-born subject, spouse, or family member; verification of employment; interviews of character references; and a check of local agency records.

[3]An adjudication facility decides whether to grant or deny a clearance. In DOD, there are eight adjudication facilities.

Figure 1: Percent of Deficient Investigations in Nine Required Investigative Areas



Source: GAO sample of 530 DSS investigations.

In 16 percent of the investigations we examined, DSS did not pursue issues pertaining to individuals' prior criminal history, alcohol and drug use, financial difficulties, and other problems that its investigators uncovered. Any of these issues, if corroborated, could disqualify an individual from being granted a security clearance. Of particular concern is the failure to resolve issues pertaining to large outstanding debts and bankruptcy, since financial gain has been the major reason individuals committed espionage. The following cases illustrated these lapses.

- A reinvestigation for an individual working on cross-service issues revealed that the subject's credit report showed $10,000 past due on a mortgage and indicated that the lender had begun foreclosure proceedings. The subject denied knowledge of the matter, and there was no evidence that DSS pursued the matter further by contacting the lender.

- An initial investigation for an individual assigned to a communications unit revealed a bankruptcy on the subject's credit report. There was no evidence that DSS questioned the subject about the matter or made any further attempt to address it.

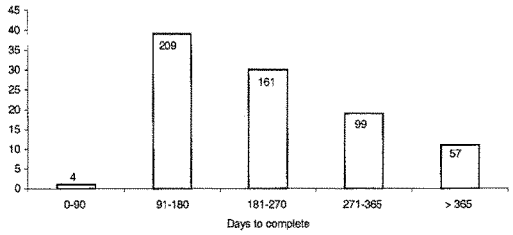
- A reinvestigation for an electronics technician contained no evidence that DSS attempted to verify the subject's claim to be a member of a foreign military service and to hold foreign citizenship. Further, although the investigative file indicated that the subject may have been involved in shooting another individual, we found no evidence that the matter was pursued by DSS.

Untimely Investigations Created Costly Delays and Backlog

DSS investigations take too much time. Although DOD components and contractors want investigations completed in 90 days to avoid costly delays, half of the 530 investigations we reviewed took 204 or more days to complete. In 1994, the Joint Security Commission reported that delays in obtaining security clearances cost DOD several billion dollars in fiscal year 1994 because workers were unable to perform their jobs while awaiting a clearance. In February 1999, representatives of several contractors wrote to the DSS Director complaining about the time taken to clear personnel scheduled to work on defense contracts and pointed out that the delays were threatening to affect some facilities' ability to effectively perform on contracts and meet cost schedules. The representatives noted that 64 percent (1,426) of the 2,236 investigations they had requested were pending for more than 90 days, with 76 investigations pending since 1997. In addition, adjudication facility officials said that they frequently made decisions to grant or deny clearances based on incomplete investigations because it would take too long to have DSS obtain the missing information. They considered this a judicious weighing of the risks entailed. Figure 2 shows that DSS completed only 4 of the 530 investigations we reviewed—less than 1 percent—under 90 days, whereas 11 percent took more than 1 year.

Figure 2: Calendar Days Needed to Complete Investigations

Percent of days



Source: GAO sample of 530 DSS investigations.

About 600,000 DOD individuals holding clearances are overdue for reinvestigations.[4] This backlog resulted, in large part, from quotas imposed by the Assistant Secretary in 1996 (and that continue today) on the number of reinvestigations that DOD components could request in a given year. In 1994 and 1999, the Joint Security Commission reported that delays in initiating reinvestigations create risks to national security because the longer individuals hold clearances the more likely they are to be working with critical information systems. Also, the longer a reinvestigation is delayed, the greater the risk that changes in an individual's behavior will go undetected. DOD is currently initiating several efforts to reduce this large backlog.

[4]The 1997 federal investigative standards require a periodic reinvestigation of individuals granted access to classified information. Clearances are outdated if a reinvestigation has not been initiated in the past 5 years for top secret clearances, 10 years for secret clearances, and 15 years for confidential clearances.

Ineffective Management Reforms and Inadequate Oversight Led to Deficient Investigations

The deficiencies in DOD's personnel security investigation program are due to DSS's ineffective management reforms and inadequate program oversight by the Assistant Secretary of Defense (Command, Control, Communications, and Oversight). DSS relaxed its investigative requirements against the advice of the Security Policy Board, eliminated critical investigative quality control mechanisms, did not adequately train its staff on the new federal investigative standards, and ineffectively managed the implementation of a new $100 million automation effort.[5] DSS's actions were undertaken as reinvention efforts ostensibly based on the National Performance Review, which called for improving government at less cost.[6] However, DSS's actions did not achieve this result.

DSS Relaxed Investigative Guidance Contrary to Security Policy Board's Advice

From August 1996 through February 1999, DSS relaxed its investigative requirements through a series of policy letters. Several of these letters gave investigators greater discretion in how they would meet the federal standards or pursue investigative issues that might be significant. For example, although the federal standards require credit information to be obtained on a subject, DSS eliminated the requirement to contact creditors about debts revealed by the subject. DSS also eliminated its practice of routinely verifying disputed credit accounts. Although the federal standards require investigators to obtain character references on the subject, DSS gave investigators "broad leeway" in deciding whether to obtain references from the subject's neighborhood. DSS also did not require that local agency checks for a subject's prior criminal history be done if local jurisdictions charge a service fee, an exception not provided for in the standards. Similarly, although the standards require verification of divorces, bankruptcies, and other court actions, DSS only required that divorce records be routinely reviewed. These policy changes caused much confusion among agency staff. In responding to our survey of nearly 1,300 DSS investigators and case analysts, 59 percent of the investigators and 90 percent of the case analysts said that the policy guidance had confused them about what investigative requirements they were to follow.

In 1996 and again in 1998, the Security Policy Board advised DSS not to adopt policies that ran counter to the federal investigative standards. The

[5]The Board consists of senior representatives from the following 10 federal agencies, departments, and other organizations: the Central Intelligence Agency; the National Security Council; the Office of Management and Budget; the Joint Chiefs of Staff; the Departments of Commerce, Defense, Energy, Justice, and State; and a non-defense agency rotated on an annual basis (now served by the Department of Transportation). It is responsible for developing directives for U.S. security policies, procedures, and practices.

[6]The National Performance Review was a task force headed by Vice President Albert Gore, Jr., in 1993 aimed at reinventing government to make it less expensive and more efficient.

Board noted that DOD was a full partner in developing the new standards and that the planned actions would undermine the objectives of achieving reciprocity in investigations among the federal government's agencies, cause a serious deterioration in the quality of investigative work, and increase security risk. It stated that if DSS wanted to change the standards, it should bring such requests to the Board, which was specifically established for that purpose. In spite of this advice, DSS adopted the relaxed investigative guidance. The new DSS Director, appointed in June 1999, has acknowledged the need to bring DSS standards in line with the federal standards, and he has directed a review toward this end. He also has expressed his intention to improve cooperation with the Security Policy Board.

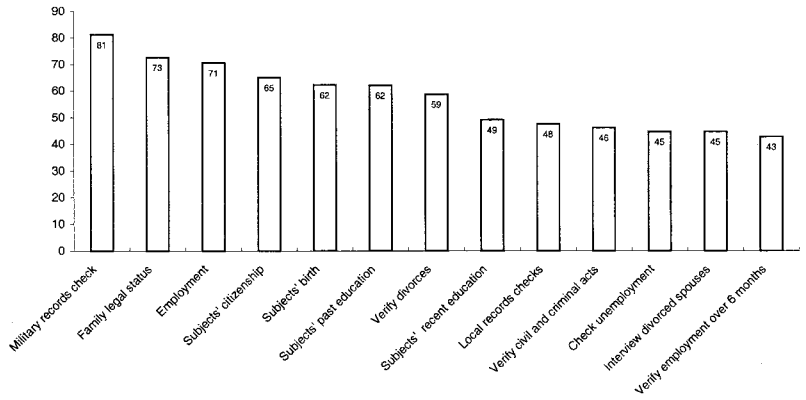
DSS Eliminated Important Quality Control Mechanisms and Did Not Provide Adequate Training

In 1996, DSS eliminated two quality control mechanisms that were critical to ensuring the quality of the investigative work—supervisory review of completed investigations and its quality assurance branch. Previously, field supervisors routinely reviewed all completed investigations before they were forwarded to DSS headquarters and submitted to the adjudication facilities for clearance decisions. The quality assurance branch conducted weekly reviews of a sample of completed investigations and published a newsletter on common investigative problems. Both programs were eliminated under DSS's reinvention efforts.

Investigative quality has also been diminished by inadequate training on the federal standards for both the investigative and case analysts staffs. During the past 3 years, DSS provided almost no formal training on the standards, and DOD dismantled the major training organization that provided the training. As a result, from 43 percent to more than 80 percent of the investigators we surveyed stated that they were inadequately trained on the various federal standards. Figure 3 shows the areas where the investigators most frequently cited training gaps.

Figure 3: Percent of Investigators Without Recent Training on Investigative Requirements

Percent of investigators



Source: GAO survey of 1,009 DSS investigators who provided information on their training.

Poorly Planned Automation Efforts Have Consumed Millions of Dollars and Delayed Case Processing

DSS did not properly plan for the implementation of a new system designed to automate its personnel security investigation case processing. As a result, (1) DSS has not been able to process its investigations; (2) the volume of investigations sent to field offices and the adjudication facilities has decreased sharply; and (3) according to DSS officials, DOD may have to add $100 million to $300 million more to the $100 million already spent on its automation efforts to have a workable system. The automation problems have exacerbated DSS's efforts to cope with the large backlog of overdue investigations.

Our survey of investigators shows the dramatic impact the automation problems have had on their workload. Before the system was implemented in October 1998, 58 percent of the investigators said they had too much work. Since the system was implemented, the situation has reversed: Now, 60 percent of the investigators said they had too little work. A similar decrease in workload has occurred at the adjudication facilities. The volume of investigative cases for four facilities included in our review dropped between 37 percent and 67 percent following the implementation of the new automated system.

Inadequate Oversight Is Underlying Cause of DSS Problems

The problems we found in the completeness and timeliness of DSS investigations and in its automation efforts were due to inadequate oversight by the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence). For at least 4 years, DSS has operated with little scrutiny of its programs by the Assistant Secretary, who is responsible for DSS oversight. Sound management practices call for such oversight. DOD officials stated that once DSS initiated its reinvention efforts, it was allowed to operate, for the most part, at its own discretion.

DOD Is Implementing GAO's Recommendations

Because of the significant weaknesses in DOD's personnel security investigation program and the program's importance to national security, we made numerous recommendations to the Secretary of Defense. We identified the program as containing material internal control weaknesses and recommended that the Secretary report this to the President and the Congress in accordance with the Federal Managers' Financial Integrity Act. We recommended that the Secretary develop a strategic plan and performance measures for the program. We also called for the Secretary to (1) direct that oversight of DSS be increased, (2) provide the necessary funding and prioritization to effectively deal with the large backlog of overdue investigations, (3) improve the mechanisms for implementing investigative policy changes consistent with federal procedures, (4) establish effective investigative quality control mechanisms and a training infrastructure, (5) take near- and long-term actions to correct the case automation problems, and (6) direct the adjudication facilities to grant clearances only when all essential investigative work has been done. With respect to this last recommendation, the Ranking Minority Member, House Committee on Armed Services, has recently asked us to review DOD's adjudication policies and procedures, including those used to grant and deny clearances for DOD contractors.

DOD agreed that the deficiencies we found represent a potential risk to the personnel security program and the protection of classified

information. DOD concurred with all our recommendations to improve its personnel security investigation program and to fully implement all recommendations. In response to our recommendations, DOD is in the process of taking a series of actions to correct program weaknesses. To its credit, DOD did not wait for us to issue our final report before it began taking corrective actions. Although most of DOD's actions are in their early stages, they appear to be responsive to our recommendations and are positive steps toward addressing the weaknesses we found.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared remarks. I would be happy to answer any questions you may have.

(702035)

Mr. TERRY. Thank you very much.

Mr. Shays is the real chairman of this subcommittee. Would you please start?

Mr. SHAYS [presiding]. I will be happy to start. I ask unanimous consent that all members of this subcommittee be permitted to place any opening statement in the record, and that the record remain open for 3 days for that purpose. Without objection, so ordered.

I further ask unanimous consent that all witnesses be permitted to include their written statements in the record, and without objection, so ordered.

I have a number of questions that the staff has written out that I want to go through because I really want to cover those in some sequence. First, let me ask you, re- investigations occur how often?

Ms. SCHUSTER. It depends on the level of the clearance. For a top secret clearance, which was the focus of our investigation, it is every 5 years. For a secret clearance, which is the next level down, that is currently now 10 years. For a confidential clearance, which is one step below that, it is every 15 years.

Mr. SHAYS. The number was approximately 2 million people with any of these three, the top, the secret, and the confidential. What would be the breakdown of the top secret? Do you know that? I could ask the next panel if you do not have that.

Ms. SCHUSTER. Yes. We have 500,000 top secret, 1.8 million secret, and 100,000 confidential. That is a total of 2.4 million. These are rough numbers.

Mr. SHAYS. I understand. Did you evaluate the logic of every 5 years? Did you look at that and say, could it be 6? Could it be 7?

Ms. SCHUSTER. No. We did not include that in our review. The only things that were in our review were top secret clearances. So, that is what we focused on. Those are the people who handle the most sensitive information. So, we focused our efforts on just the top secret ones.

Mr. SHAYS. Has it always been 5 years? Has that just been kind of what we do?

Ms. SCHUSTER. Top secret has been every 5 years for a long time. The new time limits on confidential and secret are relatively new. I think that was 1997. Those requirements are in the force now. DOD had been doing the secret clearances every 15 years. Now, they will be doing them every 10 years. They had not been doing the re- investigations on the confidential clearances until the new requirement came into being.

Mr. SHAYS. In the 530 cases that you reviewed for top secret clearance, you basically said 92 percent of the 530 investigation cases were deficient and that they did not contain information in at least one of the nine required investigative areas. Then you said 77 percent of the investigations were sufficient in meeting Federal standards in two or more areas.

Was there any one of those nine areas that was mostly ignored?

Ms. SCHUSTER. Yes. There were some that were more prominent than others. The one that was most frequently omitted was establishing residency, going out to the neighborhoods and making sure that the person really lived at the address that he did, verifying birth and citizenship, checking birth records.

Mr. SHAYS. I do not understand. If I would logically make an assumption, I will be the devil's advocate here, that if they had been investigated once, that was determined. It is like if they were born in the United States, what is the point of checking 5 years later that they were born in the United States.

Ms. SCHUSTER. Right. You are making a distinction between the initial investigation and the periodic re- investigations. For the periodic investigations, they do not have to go back and verify certain things that were already verified the first time. They just have to cover the period since the initial one.

Mr. SHAYS. There is logic to it that way.

Ms. SCHUSTER. Absolutely.

Mr. SHAYS. You also said 16 percent not pursued when something like a drinking problem or a financial problem. I basically thought the whole point of doing these re- evaluations was to identify a problem area. I mean, to me that is the most shocking thing that you have told me today.

Ms. SCHUSTER. I would agree with that, yes. I believe that there is really not too much of an excuse for not following up when you come up with derogatory information. The guidelines do call for going beyond just getting the basic information. When there is derogatory information that seems significant, it should be pursued under the guidelines.

Mr. SHAYS. It reminds me of a cartoon I saw in a newspaper years ago and it showed an investigator and he was looking for a bank thief. He got into this house, and he opened the closet, and all of this money came cascading down on top of him. He said, nothing here but money, and then went on to the next thing. So, that you would clearly identify.

How has the mismanagement of the agency contributed to the weakness found in your review of the Personnel Security Investigation Program?

Ms. SCHUSTER. I think the management problems that have come to light have been very well-documented, including testimonies as recent as last week, I believe, when the Secretary of Defense acknowledged that there were a lot of problems there. We found the weaknesses in several areas. The first area was relaxing the standards below the Federal standards, and also allowing perhaps too much latitude with their investigators as to how far and how deeply they went into the investigative areas.

The second area was doing away with some of the quality control mechanisms they had on those investigations. They did away with the Quality Assurance Branch, and supervisory review, for instance. In the training area, they just really were not giving very much training to the investigators.

Because there were new investigative standards, there was a need for such training. They also did away with the Security Institute, which was training not only DSS investigators, but investigators throughout the Government.

Mr. SHAYS. Did this happen during the Clinton administration or did this happen before the Clinton administration?

Ms. SCHUSTER. This occurred primarily between March 1996 and very early 1999, but primarily between 1996 and 1998.

Mr. SHAYS. Frankly, I find this pretty astounding. I was thinking if I was asked to come in, as General Cunningham has come in, to remedy this, I mean, to think that you would eliminate the training of your employees who go out, as one example of what you mentioned, to me just frankly boggles the mind.

What would attribute to that? Did we in Congress just give lots less money? I mean, what ultimately happened that made that occur?

Ms. SCHUSTER. What appears to have occurred is that leading up to 1996, there were several groups that were bringing up problems with the Personnel Security Program across the board. They were saying it was taking too long to do the investigations, and that the whole process was fragmented and needed to be streamlined. So, the Joint Security Commission, and the Defense Reform Initiative, the Quadrennial Defense Review, all of those bodies were saying that something needed to be streamlined and done to try to improve that whole personnel security process.

So, at that particular time, the Director decided to take up the mantle and try to do something to streamline the procedures, and got approval to become a re-invention laboratory and streamlined some of the procedures.

Mr. SHAYS. In the beginning of this, I was trying to think. Well, you know, once you have gone through a clearance, I think of myself. I am not really going to change that much. So, I think once they have done a clearance, why would we keep doing it every 5 years? That is why we have these hearings. The answer is quite evident here.

What I had realized is that the value of the re- investigation is that as people are in the system, they gain more authority. They have really an opportunity to see things that are far more precious, and important, and sensitive. So, the logic, it seems to me, is that the re- investigation is two things. Then I want you to comment. It is really your statement. So, thank you for it. It is an excellent statement.

You have a more important job and you are seeing more sensitive information. Also, you can fall on hard times. You can have a financial problem. You can start to have a drinking problem, both of which would, potentially, to tremendous compromise. So, I am pretty comfortable with why we want to re-investigate.

Ms. SCHUSTER. I am in full agreement with what you have said, yes. As a matter of fact, many of the people who are experts in this arena have emphasized that periodic re-investigations are probably more important than even the initial investigations. So, you are absolutely right.

Mr. SHAYS. I think I will just yield back my time, and if other Members want to ask questions.

Mr. TERRY. Yes. I have got a couple of mop-up questions, if you do not mind. I appreciate it. The field that you investigated from the 530 cases, I apologize for maybe asking questions that are already involved in your statement. I assume those 530 were random.

Ms. SCHUSTER. Yes.

Mr. TERRY. They were not particularly pulled out of a field that was waiting to be investigated.

Ms. SCHUSTER. Right. If I could just explain our methodology.

Mr. TERRY. I would appreciate that, yes.

Ms. SCHUSTER. We took all of the cases that were sent four of the adjudication facilities, in January and February 1999. Those four adjudication facilities were the Army, Navy, Air Force, and the National Security Administration. We included all of the cases that went there for adjudication, which means they were going to decide whether to approve or deny a clearance at the top secret level.

We took a statistical sample of those cases. I think there were 1,698. We took 530 of those.

Mr. TERRY. That is a pretty good percentage.

Ms. SCHUSTER. The size got us to certain tolerance levels. To be able to project results to that universe of cases that were there. Now, those four adjudication facilities were selected because they represent 73 percent of all the cases that are adjudicated in the defense area. So, it does indicate, I think, that our findings are representative of a systemic problem. So, that is how we selected those.

Mr. TERRY. The phrase "systemic," shall we assume that it was equally weighted from the four adjudication centers or was it one that was predominantly the problem while one was doing an excellent job?

Ms. SCHUSTER. What we found was that all had problems. The lowest one was 88 percent in the Army. That statistic that I gave you about 92 percent had one thing. It was 88 percent in the Army, 91 percent in the Navy, 94 percent at the National Security Agency, and 95 percent in the Air Force. So, all of them were pretty deficient.

Mr. TERRY. Well, that is incredibly depressing.

Ms. SCHUSTER. I did not come here to depress you.

Mr. TERRY. No, but it is disturbing. It really is, especially the 16 percent with derogatory information that lacked any follow-through and followup. It really speaks volumes. You have done an excellent job, I think, in your report about learning where the problems lay; identifying that there is in fact a problem that we need to address. Now, let us look toward the solutions.

You mentioned that General Cunningham has already started addressing them. That became obviously the shorter part of your report and presentation here today, but I think that is where we need to focus on now, since you have done an excellent job of identifying the problems.

Let us focus now on the solutions. What has he been able to implement to-date? Where can we help out? Where have been the obstacles that you have been able to identify toward doing a better job?

Ms. SCHUSTER. Let me first compliment General Cunningham. He has really taken the bull by the horns and has taken actions on every single item that we recommended in our report. GAO is not used to the agency coming back and agreeing with us 100 percent. But in this particular case, the Department did agree with all of our recommendations.

Some of the things that he has done on the management front: we asked for a strategic plan, and for performance measures to try to measure how much progress they are trying to make to meet

their goals. He has developed a strategic plan. They are working on it and a performance plan to set milestones for trying to correct some of the problems there.

They are designating this investigation program, as a material weakness to the Department of Defense under the Federal Managers Financial Integrity Act. He has brought the standards back in line with the Federal Standards so that the investigators will be following the same standards that other investigators throughout the Government are following, and has created a new manual for them to follow, and will be providing them training.

He has re-established the Quality Control Unit within DSS. These staff will be periodically tested on the standards to try to maintain the quality of the investigations. In terms of the backlog, this is a real difficult problem for them to solve. I understand that what they have done is to go back and try to re-evaluate the backlog to see whether in fact all of the people that were in the backlog really in fact needed an update.

Some people, for instance, retired. Some people were separated. Some people were no longer working in classified areas. So, they are trying to get a better fix on exactly the extent of the backlog. Because there were quotas established on how many could be sent to DSS for investigation, there is sort of a pent-up demand. The statistical data base was not really very good at capturing the total universe of this backlog.

They are taking several actions. One in particular, I think, is very promising. They are working on an algorithm that will try to identify those cases that are most likely to result in a denial of a clearance, based on their past experience. That will allow them, if they can get this to work, to identify those cases that are most risky to the Government and be able to process those in a priority manner.

Mr. TERRY. Let me interrupt. What do they need to make that work so that we do not run into the same problem that you identified in your testimony as spending $100 million on automation that has not worked?

Ms. SCHUSTER. Right. Well, that is a fair question. I do not know the answer to that question because we have not really gotten into the details of how they are developing that algorithm. The idea is certainly a good one. They also are contracting out for some of the backlog. They have put some Reservists on active duty to temporarily work on the backlog. They have OPM working on some of the civilian investigations. They are thinking about also having a contract that would do some end-to-end investigations from the very start to the very end with contractors who would be focusing on some of the cleaner cases, the ones that do not seem to be as risky. They would contract those out.

So, they are doing a lot of things on that front. As you alluded to, they have a lot of problems with the Automated Case Control Management System. That, to my mind, is the biggest challenge that they face. That automated system just was not planned properly. It was not implemented properly. The people who were trying to procure that system and manage it really were not totally qualified to do that.

They did not have the background in a major acquisition program. They did not have the information technology expertise to really do that. I think all of these weaknesses have been acknowledged. So, they are at a juncture now where they have got to decide whether they are going to try to patch up the system, or if they are going to just give up on it and try to replace it. That is going to be a major decision for them to make.

Regarding past evaluations, there was a DOD red team that came in, and evaluated what they should do with that system, and what went wrong with the system, and what they would recommend. A TRW contractor evaluation also looked at it from a technical standpoint.

Both of those groups pointed out numerous problems with the way the thing was put together, the lack of documentation, the lack of checks and controls, just what you would expect of an automated system, to the point that the TRW investigation did not feel like it was salvageable.

Mr. TERRY. I was curious if any of the people from the outside that have reviewed this made any suggestions. You are saying TRW has made a suggestion that you walk away from it. I assume that there are probably people on the inside, for want of a better word. When you invest $100 million and a lot of reputation, that is probably emotionally hard to walk away from, but that is what TRW is recommending?

Ms. SCHUSTER. That is what they recommended in their evaluation. Now, I understand that there is another evaluation going on right now. I am not sure who is conducting that. But that evaluation is supposed to come up with a recommendation to the Secretary, I think it is May 1st of this year, who would make the decision: Are we going to try to fix this system or are we going to consider an alternative?

One point that should be brought out is that if they do go with a new system, that would fall under the Clinger-Cohen Act, which would mean that they would have to look at things like: Is this an inherently Governmental function? Does it have to be done by the Government? Should it be governmental or could it be privatized?

Are there other alternatives out there, such as OPM's system that might be an alternative? Is a new system by the Government needed and should one be procured? So, all of those decisions. Make this sort of tough. It will take awhile to work through that, if the decision would be made to go with a new system.

Mr. TERRY. But they are moving toward that direction. So, that is movement and that is appreciated.

Ms. SCHUSTER. They are at least considering all of the alternatives now, and a decision is going to be made apparently the first of May.

Mr. TERRY. All right. Thank you very much.

Mr. SHAYS. Mr. Mica.

Mr. MICA. Thank you. Just a couple of questions, if I may. Tell me about the numbers of personnel that we are dealing with, with DSS. How many full-time equivalent employees?

Ms. SCHUSTER. The employees that we are talking about that do investigations are 11,075, roughly, at the time of our review, and 112 case analysts who also work in this area. The total number of

DSS employees is 2,500 or thereabouts. I could get the exact numbers for you for the record, if you would like.

Mr. MICA. Well, wait a second. Now, 2,500?

Ms. SCHUSTER. Total DSS employees.

Mr. MICA. That is total DSS. The 11,000 are those conducting the investigations?

Ms. SCHUSTER. I am sorry, 1,175. I misspoke.

Mr. MICA. OK. They conduct how many background investigations?

Ms. SCHUSTER. They conduct about 150,000 investigations. That would include secret, confidential, and top secret. I would like to check that number and get back to you on that exact number.

Mr. MICA. I would like to know the figures on that.

[The information referred to follows:]

Personnel Security Investigation Workload

Investigations in thousands

	Fiscal Year							
	1991	1992	1993	1994	1995	1996	1997	1998
Investigations opened	227	271	214	208	212	126	190	126
Change from FY1991		+19%	-6%	-8%	-7%	-44%	-16%	-44%
Investigations opened per investigator	137	173	149	157	172	113	163	101
Change from FY1991		+27%	+9%	+15%	+26%	-18%	+19%	-26%
Investigations closed	232	264	217	206	204	158	172	142
Change from FY1991		+14%	-6%	-11%	-12%	-32%	-26%	-39%
Investigations closed per investigator	140	169	152	156	166	141	148	114
Change from FY1991		+21%	+8%	+11%	+18%	+1%	+5%	-19%

Source: Defense Security Service and GAO analysis of DSS data.

Mr. MICA. Then I am curious, OK, then they do a rash of other sort of renewable?

Ms. SCHUSTER. Right. There are other kinds of investigations.

Mr. MICA. Maybe you could give us a breakdown of figures on that.

Ms. SCHUSTER. OK.

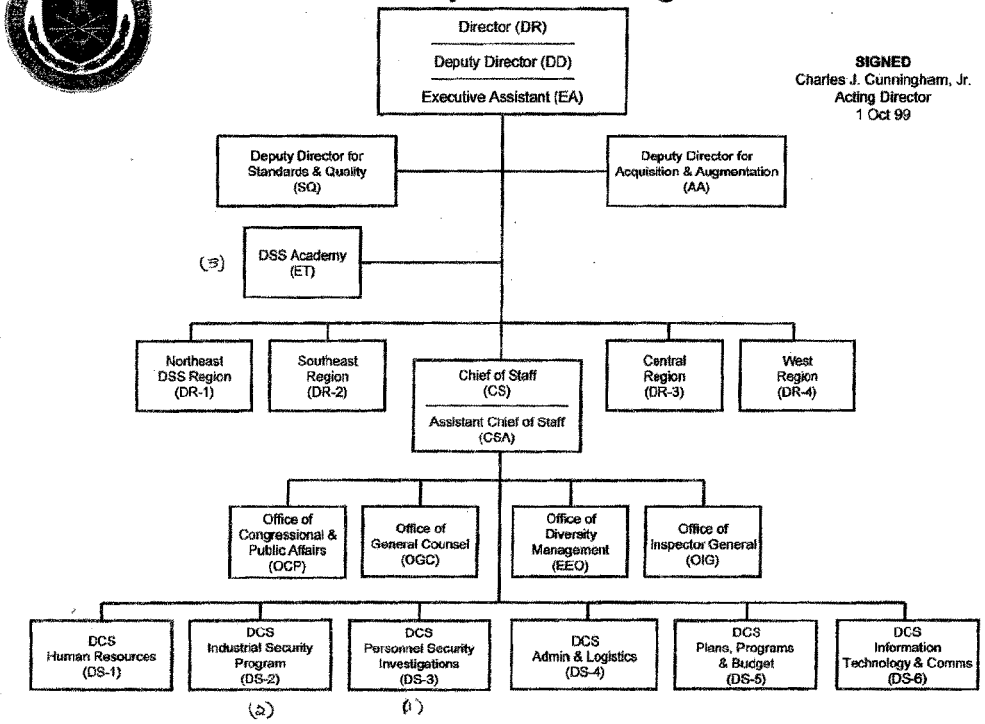
[The information referred to follows:]

BUDGET FOR INVESTIGATIONS AND OTHER MISSIONS OF THE DEFENSE SECURITY SERVICE

The Defense Security Service (DSS) has three core missions: (1) conducting personnel security investigations for DOD military, civilian, and contractor personnel; (2) administration of the National Industrial Security Program; and (3) providing security education, training, and awareness for security professionals in DOD, 21 other non-DOD federal agencies, and contractor communities. These three functions are noted on the following organization chart. About $270 million (84 percent) of DSS's fiscal year 2000 budget is for the personnel security investigations. Regarding the other core missions: DSS budgeted in fiscal year 2000, $20 million for the National Industrial Security Program, $5 million for security education and training, and $16 million for miscellaneous administrative costs (including the Inspector General, legal support, and other administrative support for DSS headquarters offices).

Regarding the personnel security program, DSS reported that it conducts 600,000 personnel security investigations each year. More specifically, DSS said that is conducted 663,818 personnel security investigations in fiscal year 1999, 55,219 of which were for Defense contractors. DSS was unable to provide the specific number of personnel security investigations for military personnel, DOD civilians, and other authorized non-DOD agency personnel that are included in the total number of 663,818 investigations.

Defense Security Service Organization



SIGNED
Charles J. Cunningham, Jr.
Acting Director
1 Oct 99

03/10/00 FRI 13:23 FAX
001

Mr. MICA. The budget was $320 million. Is that right?

Ms. SCHUSTER. It was $320 for fiscal year 2000.

Mr. MICA. 2000.

Ms. SCHUSTER. Right.

Mr. MICA. Now, did that include any of the—how much of that is personnel? Was any of that capital $100,000?

Ms. SCHUSTER. No.

Mr. MICA. Was that already spent?

Ms. SCHUSTER. Yes. I think that $100 million is what has already been spent to-date. Then they have estimates of what additional funds might be needed to try to fix things.

Mr. MICA. I am trying to get a handle on what it costs to operate this, as far as personnel. Another big item, you said they contract out work. How much in dollars is contracted out for conducting these activities?

Ms. SCHUSTER. I would have to get those details for you. I do not have those with me today.

Mr. MICA. OK.

[The information referred to follows:]

Defense Security Service Fiscal Year 2000

Contract Costs for Personnel Security	In Millions
Investigation Backlog	$45.4

Source: Defense Security Service

Ms. SCHUSTER. I can say that the investigations are an important part of DSS, but they also have other missions that these 2,500 people conduct. One is the Industrial Security Program. Then they also do security training and education.

Mr. MICA. Do they do this also for contractors, for private contractors?

Ms. SCHUSTER. Right. It is for civilian, military, and contractors.

Mr. MICA. Is there any way for the contractors to reimburse for the cost of that service? Are they billed for that?

Ms. SCHUSTER. I am just not familiar with the way they are paid. I know they are trying to move toward a fee-for-service kind of a thing. It has not gotten off the ground. I think that has been put on hold right now because they have not made much movement toward that fee-for-service.

Mr. MICA. Because people do not want to pay for it. I think that is something we ought to look at. As chairman of Civil Service for 4 years, kicking and screaming of course, we were successful in reducing the Office of Personnel Management from nearly 6,000 to about 3,000.

Of the 3,000 we eliminated, we privatized all of the investigators into an ESOP, Employee Stock Ownership Plan. If you think that was not controversial, Mr. Shays, they did everything to subvert that possibly. But it was actually most successful. Do you know if they contract with our ESOP at all to, yes, I see your shaking of the head. Are they doing a good job? I see another shake of the head. We are getting affirmative shakes of the heads from the audience, just for the record.

I know privatization strikes fear into the heart of anyone on a Federal payroll, but it does work and it is a great example of it. I am not sure what could be privatized, or what portion of this could be done, or how much could be contracted out to the entity already privatized. I think it would be good to look at the number of people, what we are producing.

Who is paying for the services? The Government picking up the tab for private contractors who are doing business with the Government. There ought to be some reimbursement in it. Certainly, the way it is operating now, just the information from your initial study seems that we have to be able to do a better job doing this.

Possibly a little innovation might be in order. $320 million is a pretty big sizable budget. If possible, maybe you could submit for the record and also for me, I would like to see both a flow chart of the organization, and then I would like to see a breakdown of the expenditures. I do not see it. I looked through here and did not see it of how much is in these different categories for personnel, for contracted services, and other expenditures. Maybe we could get a handle on that.

Ms. SCHUSTER. We can provide that for the record. That was not part of the scope of our investigation, but we can certainly get those numbers for you.

[The information referred to follows:]

INSERT 6

Defense Security Service
Cost Breakdown
Fiscal Year 2000

Cost Category		**In millions**
Civilian Pay		$172.6
Contracts:		
Information technology	19.0	
Communications	5.8	
Rent	6.4	
PSI[1]	31.9	
PSI – Backlog	45.4	
Capital acquisition	11.9	120.4
Other (Travel, supplies, equipment, maintenance, fuel)		27.3
Total		$320.3

Source: Defense Security Service

[1] Costs to process current volume of personnel security investigations at a steady state.

Mr. MICA. I noticed in your recommendations, one of the things is prioritizing. That they need some better system of prioritization. I would imagine some of those would be of the utmost urgency and highest level of security clearance, which would have to be done in a certain fashion by a very secure personnel to start with. Then as it filters on down, maybe some change in procedures in the way that is done. I guess that is a part of your recommendation.

Ms. SCHUSTER. Yes. Our recommendation was that they try to work on that backlog as a priority matter. What they have done is they have found several different means to try to catch up with that backlog. Then they are also working on this algorithm that is going to try to identify those cases that, from their past experience, tells them that they might be most likely to be denied a clearance.

They have an automated personnel questionnaire that flags certain items. Based on their past experience, if there is derogatory information on certain elements, it tells them that the likelihood this clearance might be denied is higher than another. So, that is what they are working on internally to try to find a means of prioritizing the workload. That seems like a good idea.

Mr. MICA. The other final question that deals with $100 million spent on the unsuccessful computerization.

Ms. SCHUSTER. What they did was they took the long questionnaire that probably all of us have filled out and they automated that into an electronic form. The whole idea was that everything would be paperless.

Mr. MICA. Right.

Ms. SCHUSTER. Throuigh this Case Control Management System, they would be assigning the cases to the investigators.

Mr. MICA. What basically went wrong? I mean, was it something in the specifications that the agency provided, or was it something that the vendor did not produce?

Ms. SCHUSTER. Just about everything that you can imagine that could go wrong did go wrong, I think.

Mr. MICA. Was the vendor held liable or did we pay the whole thing?

Ms. SCHUSTER. I am not so sure it was the vendor's fault although maybe some of it was the vendor's fault. But the basic underlying factors are that it really was not planned very well as an acquisition program. The people were not very well qualified in either IT or acquisition management.

A lot of the basic planning steps that you would go through for a major procurement program, such as determining your requirements, and drawing up a plan, and developing a testing plan, those basis just were incompletely followed. So, when they got to the point where they wanted to implement this, the electronic questionnaire was only being used about 50 percent of the time. Because it was designed as a totally automated paperless system, and you still had paper, then you were trying to keep two systems going; one with paper and one without paper.

It just caused all sorts of delays because they could not get the cases to the investigators fast enough. So, that really did contribute to the backlog that we are seeing today.

Mr. MICA. Thank you, Mr. Chairman.

Mr. TERRY [presiding]. Mr. Shays.

Mr. SHAYS. Thank you. As I fully grasp what you are saying, and I am not fully there yet, it is astounding. I do not know how DSS could be in worst shape, or how they could have done a worst job, given the backlog. I want to ask a few more questions. Their budget was $74 million and then it went to $84 million?

Ms. SCHUSTER. For the whole agency?

Mr. SHAYS. Yes.

Ms. SCHUSTER. $340 million.

Mr. SHAYS. Where am I getting this $74 million?

Ms. SCHUSTER. $320 million for fiscal year 2000 was their budget.

Mr. SHAYS. OK. It must be just one part. Was that the contractors?

Ms. SCHUSTER. Total budget.

Mr. SHAYS. We had an AIA member company survey. They tried to estimate what its impact, what the backlog was on the companies. These are some of the companies. Boeing had 570 employees that were zero to 90 days. I want to take the 90 days beyond; 1,161 employees. They believe it cost them $52.1 million.

Honeywell, 31 employees. They think it cost them $1 million. Northrup-Grummend, 735 employees. They believe it cost them $27 million. Lockheed-Martin. Now, they divided in technical services 58 employees, 4.8; LMTAS, I do not know if they call it LMTAS or what, but 529; employees, $28.4 million. Skunk Works, 540 employees, $26.6 million.

United Defense, 145 employees and they did not give a cost in that one. Aero Jet General, 40 employees, $4 million. General Dynamics Information Systems 8 employees. They did not give us a cost. Where we have the cost $143 million, which is basically almost half of what the budget is. Now, I make an assumption, and maybe you can answer this, that the cost that these companies incurred ultimately gets passed on in terms of the cost of the project to the Government.

Ms. SCHUSTER. I would assume that is correct, that is the information you are bringing to light. While I do not know those figures, I do know that during the course of when this backlog was building up, there was some association of these contractors—I forget the name of it—that complained to DSS about this and emphasized that it was costing them a lot of money to have these delays.

Mr. SHAYS. But just 3,247 employee backlog, the private sector of these companies has basically determined it cost $143 million. We are talking about potentially hundreds of thousands. So, it is the kind of thing I begin to wonder about the $600 toilet seat. We do know it cost the Government money. We do know that somehow we have not factored that in.

Ms. SCHUSTER. Right.

Mr. SHAYS. That is a strong argument to provide the resources necessary to DSS to get the job done. To the extent Congress has not done it, and it may be that we privatize more. My understanding is that when we hear from DSS that they are basically going to tell us that they have a 50 percent assistance from the private sector, ultimately when they get their number down from contractors, those employees disappear.

I am basically wondering this question. They had a tremendous backlog so they were to find ways to streamline. It strikes me that the streamlining not only did not streamline, it did the exact opposite. It created even more backlog and it provided a less acceptable quality of result, such as ignoring a large percent, was that 16 percent, of indications you should look at something. That was ignored. Am I correct here? Reinventing got the backlog larger and it compromised the system. I am not looking for a big answer.

Ms. SCHUSTER. OK. There were several reasons that led to this backlog. The first thing is back in 1995, the Assistant Secretary of Defense put quotas on the number that could be sent forward. So, you got sort of a pent-up demand that is now a part of that backlog that was not submitted. Then we had new requirements that were instituted during this period for re-investigations on secret and confidential clearances. Those had not been requirements before. So, this added to the periodic backlog.

Mr. SHAYS. So, when you said the 5 has been there for years, the 10 and the 15 were?

Ms. SCHUSTER. New.

Mr. SHAYS. OK, fair enough.

Ms. SCHUSTER. Right. Also this automated system that we were talking about just did not work. So, the caseload was not going through there like they really wanted to. That contributed to the backlog. Then DSS, also point to a couple of other factors. One is that they feel that there are more people requesting clearances.

Their customers are requesting more clearances because of information technology jobs that may require clearances and a couple of other factors. One was that there was a reduction in the number of investigators that they had. So, all of those factors collectively contributed to that problem. The re-invention part certainly had an impact on the quality of the investigation.

Mr. SHAYS. I did not want a long answer, but I needed it because you needed to clarify that there were a whole lot of factors.

Ms. SCHUSTER. A lot of factors.

Mr. SHAYS. I know we have a vote, but I just want to just get into this last area. If you go into a company and you try to determine, well, they got bad and so on. You really want to face up to really how bad it is. This is so bad that you could almost be tempted to say, well, it could not be worse. But it could be worse in one respect. It could be that we have a larger backlog.

When you go into a company and they say, well, you know, our total IOUs are $10 million and then you look further and you find it is $20 million, that is a shock. Can you tell me with 100 percent confidence that the backlog is not larger than we think it is?

Ms. SCHUSTER. No. I cannot tell you what the size of the backlog is. I would really question whether they have an exact fix on it.

Mr. SHAYS. OK. Let me ask you, how was the backlog determined?

Ms. SCHUSTER. Each customer that comes to DSS with a need for an investigation has a fix on the number of clearances that they need investigated. But these inputs are not put into a data base that is reliable enough to the extent that you really know the totality of it. So, all they know is what is coming in to DSS to be investigated.

Mr. SHAYS. So, you do not know, in a sense, your liabilities?

Ms. SCHUSTER. I would guess that they are probably just estimating the backlog, but you will have to ask General Cunningham exactly how they are estimating that.

Mr. SHAYS. So, potentially it could be double or it could be half of what it is. We at least know that it is this number, but it could be worse.

Ms. SCHUSTER. It could be worse. It could be better. I do not think they really know.

Mr. SHAYS. How could it be better? We have a number of actual people, do we not?

Ms. SCHUSTER. Well, what General Cunningham has said is they have been trying to look at that backlog with more scrutiny and determine whether all of those people that are in the backlog really need to be investigated, because some may have retired, been separated, et cetera.

Mr. SHAYS. OK, fair enough. You are telling me I should have some question about the number.

Ms. SCHUSTER. Yes.

Mr. SHAYS. That it is an estimate.

Ms. SCHUSTER. I agree.

Mr. SHAYS. And it could go in either direction. So, we have to determine whether it was a conservative or a liberal estimate. In other words, you get the point. One last and final question. There were 11 recommendations. Is that right?

Ms. SCHUSTER. I think there were 14.

Mr. SHAYS. So, they agreed to 11.

Ms. SCHUSTER. I think they agreed to all of them.

Mr. SHAYS. Twelve.

Ms. SCHUSTER. Twelve.

Mr. SHAYS. In fact, in every one that I see in the letter they wrote on October 13th, uncharacteristically but thankfully, they are succinct. They give you a recommendation and then they say "concur." In ever instance, it is "concur."

Was there any additional recommendation that they did not concur? Was there any area where you had disagreement or can I basically accept the fact that all of your recommendations they concurred with and now the issue is how do you remedy it? In fact, you suggest how to remedy it.

Ms. SCHUSTER. Yes.

Mr. SHAYS. They are following your guidelines in many cases.

Ms. SCHUSTER. Right. From their official response, we can conclude, at this point, that they are doing something about all of those recommendations, and that they do agree with them.

Mr. SHAYS. And that is a very positive thing. So, the bottom line for me, though, is I should take a second look at the number. The committee should take a second look at how is the number determined and is it reliable, the backlog.

Ms. SCHUSTER. Right. I am sure General Cunningham can address that.

Mr. SHAYS. OK. Mr. Chairman, thank you. I am finished.

Mr. TERRY. Thank you, Mr. Chairman. We will be in recess until——

Mr. SHAYS. I think we have a couple of votes.

Mr. TERRY. Then we will talk to the Generals.

Mr. SHAYS. It will probably be at least a half hour. So, I would say 20 minutes.

Mr. TERRY. We will take a 20-minute recess.

[Recess.]

Mr. TERRY. Yes.

Mr. SHAYS [presiding]. I call our second panel, our two witnesses, General Charles Cunningham, Director of Defense Security Service, and General Larry D. Welch, chairman, Joint Security Commission. I appreciate you remaining standing. I will swear you both in. Thank you.

[Witnesses sworn.]

Mr. SHAYS. Thank you very much. It is very nice to have both of you here. I know both of you have testimony. You can have your testimony as long as you find it necessary. I think we will start with you, General Cunningham. I know we will start with you. Thank you.

STATEMENTS OF GENERAL CHARLES CUNNINGHAM, DIRECTOR, DEFENSE SECURITY SERVICE; AND GENERAL LARRY D. WELCH, CHAIRMAN, JOINT SECURITY COMMISSION

Mr. CUNNINGHAM. Thank you very much, Mr. Chairman. I made a statement and I would like to submit that for the record. If it is agreeable with you, sir, I would just like to abbreviate that in the interest of time.

Mr. SHAYS. Sure. That testimony will be in the record.

Mr. CUNNINGHAM. Thank you, sir.

Sir, as the GAO reported, the agency did agree completely with the report. In fact, we have used it as a very, very helpful road map to fix the discrepancies and to go beyond those actions. So, I want to start by thanking the GAO. It is working very well in recovering the agency. I would quickly like to go through why we are in this situation. What are the problems? What are the solutions? Of course, I will not be able to cover all of the problems or all of the solutions, but I want to quickly get through this part.

Mr. SHAYS. Feel free to be quick, but do not speak fast.

Mr. CUNNINGHAM. All right, sir. The situation that we found ourselves in was caused by very much a breakdown in our management effectiveness as reported by the GAO. In fact, a substantive part of the effort made by management, those efforts by management were caused by a work force reduction. It is well-understood that the Defense Security Service was not the only activity in the Department of Defense being reduced in size.

That was happening across the Department. Nevertheless, work force reduction was a major factor in that we reduced almost 40 percent of the work force. Investigative requirements increased as the GAO had testified. In fact, the quotas imposed all led to a buildup in the backlog of periodic re- investigations.

A major factor in this was that in an effort to compensate for the reduction in personnel, information technology in the form of the Case Control Management System was seen as a major way to reconcile the difference in achieving our mission. Nevertheless, the Case Control Management System, as the GAO reported, was managed in such a way that it did not deliver.

You will recall that the Case Control Management System was turned on in October 1998. Immediately it ran into problems. It was barely able to function at all for the first 6 weeks that it was in being. That was a major part of causing the situation we are in because: of the turbulence that it caused beyond just not getting the work done; the turbulence that it caused in the organization.

Thus, the management decided, and I do not agree with it at all, the management decision to relax standards and cease the many of the quality control activities that were ongoing. I would hasten to add that the Security Policy Board also did not agree with that action.

So, the problems, as they were seen inside the agency, were that there was an un-achievable task to be accomplished. The work force became demoralized. Training had been reduced. There was great fear of out-sourcing in the agency. All of that is not gone. There was a growing backlog. That becomes the definition or the metaphor for a larger problem.

The agency, in fact, was trying to work with both the information technology, the electronic personnel security questionnaire and with a paper questionnaire. So that at the time that technology was supposed to be solving the problem, the old method had not gone away. There was the continuing false starts that occurred in the Case Control Management System because that program management was not organized, as reported by the GAO.

Very quickly on solutions. The solutions for DSS have had to derive from a comprehensive change in how the agency operates. Quickly, the agency had to return to standards and quality. Training had to be emphasized. The timeframe that I am in now is the summer of 1999. Resources had to be organized to task. That is done. Training is reestablished in the DSS academy.

Standards are reestablished in the agency, and operating instruction on August 16th achieved that. An investigations manual had to be redone, approved, and fielded in December. Our quality management activity has been reestablished and is staffed. We have returned to basics and sound management practices.

By that, I mean we communicate as openly as possible. We have put our organization in a condition that has a unity of command in it. Everybody now knows their boss. We have reduced the span of control. We are still in the process of this. Be careful how I say that. We are in the process of reducing span of control in the field to where in situations where we had as many as 36 personnel under one first-line supervisor.

In March, that will all be reduced across the board to 11:1. It has been an essential factor in how we bring our people along. Especially, we have now put in something called standardization and evaluation. Standardization and evaluation is an activity whereby new investigators we call them agents after they complete appropriate academic training, which we now give in our academy that has been reestablished, they are given an initial qualification check by a standardization and evaluation examiner.

After that, we have periodic and a periodic examinations or checks of what our agents are doing. We have begun hiring. We are going to increase across the board from about 2,450 people on board now. We will go up over the next year to about 2,600 people.

That will include about 100 more agents, taking us from 1,200 to over 1,300 agents.

Augmentation is a major part of what we are looking at. Before I arrived at the agency, the Deputy Secretary of Defense had ordered that augmentation begin. That was done. The decision was made in May. That augmentation came in the form of getting the help of OPM.

Mr. SHAYS. Let me ask you. Who ordered that?

Mr. CUNNINGHAM. The Deputy Secretary.

Mr. SHAYS. The Deputy Secretary?

Mr. CUNNINGHAM. Excuse me, sir, the Deputy Secretary of Defense. Thank you very much. It is hard to leave the Pentagon. Thank you. The augmentation that we are into now, then, has that first phase that Secretary Hamrey ordered in May, which uses OPM. In addition to that, letter contracts with a company named OMNISEC and a letter contract with a company named MSM. OPM's contractor is USIS. That was the one that Mr. Mica had mentioned earlier.

In addition to that, and this has much higher potential for us, the phase two augmentation will consist of larger contractor support capabilities that we intend to align, as much as possible, with each of the military departments and with industry so that unique requirements can be best met. Those activities begin with the first contract coming on board as early as the end of this month. Four of those contracts we hope to have on board by the beginning of the summer.

Sir, I will stop with that and standby for your questions.

[The prepared statement of Mr. Cunningham follows:]

Statement by

Lt Gen Charles J. Cunningham Jr., USAF (Ret)

Director, Defense Security Service

Before The

House Committee on Government Reform

Subcommittee on National Security, Veterans Affairs, and International Relations

Briefing on Defense Security Service Oversight

January 26, 2000

Mr. Chairman and Members of the Subcommittee, I am Charles J. Cunningham Jr., Lt. General (Retired), United States Air Force (USAF). I am the Director of the Defense Security Service (DSS). I am extremely honored to be here today to provide you with information about the mission and current status of the Defense Security Service and to respond to any questions you may have.

Mr. Chairman, I was appointed the Acting Director of DSS on June 7, 1999, and served in that capacity until I was selected as the Director on November 8, 1999. I will briefly describe for you the three core mission areas of DSS. I will then report on the recovery actions that I have taken in response to the General Accounting Office (GAO) report of October 1999, the Joint Security Commission II Report of August 24, 1999, and my own assessment.

The mission of DSS is an important component of the national security strategy of the United States. DSS is a Department of Defense (DoD) agency that is under the direction, authority and control of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence [C3I]). Our three core mission areas include: (i) the conduct of personnel security investigations (PSIs) for DoD military, civilian and contractor personnel; (ii) administration of the National Industrial Security Program (NISP) on behalf of DoD and 21 other non-DoD federal agencies, known as User Agencies (UA); and (iii) providing security education, training and awareness for security professionals in the DoD, UA and contractor communities. Our PSI mission is

the largest of our three core mission areas and comprises 83.4% of DSS's total budget of approximately $320 million for FY2000.

In accordance with the National Standards established under Executive Order 12968 and the implementing guidance provided by the National Security Council, DSS conducts personnel security investigations on individuals working for DoD who require access to classified and sensitive information. The eight central adjudicative facilities of DoD use these investigations to determine if it is clearly consistent with the interests of national security to:

- Grant an individual access to classified information,
- Determine if access should be continued,
- Determine an individual's eligibility for assignment to sensitive duties, and
- Determine if an individual should be accepted or retained in the U.S. military.

The type of investigation conducted depends on the type of clearance or access the individual requires. An investigation usually includes inquiries of law enforcement files; a financial check; a review of pertinent records; interviews of friends, coworkers, employers, neighbors, and other individuals, as appropriate; and an interview of the individual requiring access or continued access to our nation's sensitive and classified defense information. DSS must obtain and report a view of the individual's entire character so that DoD adjudicators have complete and accurate information on which to make an appropriate security determination.

Our second mission--administration of the NISP--includes determining a contractor's eligibility from a security standpoint to perform on classified contracts, and providing security oversight, consultation and assistance on security matters to over 11,000 currently cleared contractors. This mission was given to DSS in 1980, eight years after DSS was established as a personnel security investigative agency in 1972.

Rapid advancements in information technology and increased globalization over the last decade have resulted in more diverse and complex foreign threats to our nation's sensitive information and technologies, directly impacting on our responsibilities in administering this program. The continued influx of foreign investors into U.S. companies performing on classified contracts and the rapid expansion of U.S. companies into international markets have created an environment that places greater demands on today's security professionals. Not only must they possess a different set of skills but they must understand the complexities of today's business environment.

Our third mission--to provide security education, training and awareness to security managers and personnel throughout DoD, including industry and other non-DoD federal agencies--is critical to the successful implementation of sound and effective security practices. These security professionals must receive training that enables them to understand and implement effective security practices within their own unique environments and to ensure that all individuals authorized access to classified information understand their individual security responsibilities. It is a daunting task. Under the prior administration of DSS, the Department of Defense Security Institute, previously

chartered with this important mission, was disestablished in 1997. Responsibility was transferred to an internal component of DSS headquarters; however, there was no longer a centralized classroom facility or a formalized educational structure. This situation had an adverse impact on DSS's ability to adequately meet the security education, training and awareness needs of our customers. One of my most urgent recovery actions was to reestablish this mission under a training academy. By July 1999, we had chartered the Defense Security Service Academy to provide an institutional focus for the DSS security education, training and awareness mission. Since that time we have continued to concentrate on reestablishing a quality security education and training infrastructure and reinvigorating our security curriculum to meet the requirements of our external customers in DoD and industry as well as our DSS workforce. I will address this topic in further detail later on in my testimony.

I understand that the concerns of the Subcommittee today are focused on the recent findings of the GAO report of October 1999, entitled "DoD Personnel – Inadequate Personnel Security Investigations Pose National Security Risks," and the August 24, 1999, Report by the Joint Security Commission (JSC) II with respect to DSS. The remainder of my testimony will address the near- and long-term recovery actions we have initiated in response to those findings and our own internal assessment. I will conclude with my thoughts regarding the continuing and future challenges confronting DSS and my assessment with regard to DSS's ability to perform its mission effectively.

Let me first state that the Agency's position is in full agreement with the GAO findings, which are mirrored, in part, in the JSC II report. As the Director of DSS, I have made a continuing commitment to take all actions necessary to correct the noted deficiencies, and I intend to go beyond the GAO recommendations to establish an organization known for its excellence in accomplishing our mission and ensuring the national security of the United States. We have already taken many important steps in correcting these deficiencies, which I will briefly describe for you now.

My appointment as Acting Director at DSS on June 7, 1999, followed the departure of the prior Director just three days earlier and a newspaper article on June 3, 1999, which publicized the serious Periodic Reinvestigations (PR) backlog within DoD, management problems at DSS, and a Case Control Management System (CCMS) that was designed to automate the management of the investigative process but did not work. I had also been informed that the GAO had been scrutinizing DSS's administration of the PSI program for a period of approximately sixteen months and that the investigation was still ongoing but was drawing to a close, with anticipated unfavorable results.

My first priority as Acting Director was to understand the nature and complexity of the problems facing DSS, particularly in the near term, and to quickly resolve those issues requiring immediate attention. From the outset, I was informed that the DoD priorities included: (i) elimination of the PR backlog, (ii) recovery of the CCMS, (iii) revitalization of the national industrial security program as administered by DSS, and (iv) reconstitution of sound and orderly management practices within DSS.

In an attempt to synchronize DSS's recovery actions with preliminary indications of the GAO findings and recommendations, I met with the GAO investigative team in July 1999. They reviewed their findings and recommendations with me. DSS immediately went to work on recovery actions, giving priority to those critical problems that required immediate fixes. The findings and final recommendations of the GAO, as reported to me during July 1999, can be found in the GAO's October 1999 report that describes in some detail the basis and nature of those findings and the challenges we faced.

Based on my initial assessment, the GAO findings, and DoD's priorities, I established the following near-term objectives:

- Motivate and take care of the workforce.
- Understand and overcome current obstacles to executing the mission.
- Fix the problems that existed in processes, technology and performance.
- Plan, program and budget to achieve the corporate goals and objectives.

The people of DSS were my most immediate concern. If we were to move forward in resolving existing and future problems so that we could effectively accomplish our mission, a dedicated, capable, satisfied, and highly motivated workforce was essential. Events of the past few years had taken their toll on the employees of DSS. Morale was at an all-time low due to CCMS problems and a roughly executed major downsizing and restructuring in 1996. Employees were afraid of losing their jobs or dissolution of the Agency. Productivity was at an all-time low, in part, because of problems with the

CCMS, a general loss of confidence in management decisions, and dissatisfaction with operational guidance.

Proper management of the workforce was essential. To that end we began to restructure management of the organization to ensure uniformity and continuity of command. We began at the headquarters level so as to minimize disruption and prevent further loss of productivity at the field level, and then moved down into the lower levels of the organization. The reorganization has now almost been completed with the recent selection of four Regional Directors who are now realigning their organizations to ensure more efficient and effective mission accomplishment. This overall structure is more consistent and in alignment with other DoD organizations: it is easily understood, provides for unity of command, and ensures operational consistency. Additionally, we are moving forward in addressing other human resource issues in order to improve the morale and productivity of the Agency. We have identified professional development and training, regular and meaningful performance reports, incentives and compensation, promotion opportunities, mentoring, diversity management and recruitment of new employees as areas requiring both immediate attention and long-term improvements.

While stabilization and attention to the workforce were essential, we also immediately turned our focus to the deficiencies in our mission areas. The problems in our PSI program, as noted in the GAO report, could not be easily or quickly resolved because of their complexities. However, we began addressing these issues systematically and

tracking their progress. Let me report on the most significant issues and our recovery actions.

Failure to meet federal investigative standards (Recommendation #7 of the GAO report):

The GAO report outlines in some detail the deficiencies in DSS investigations as substantiated by their review of 530 randomly sampled top secret security clearance investigations and reinvestigations completed by DSS in January and February 1999. As reported by the GAO, 92% of these investigations were deficient in one or more of the nine investigative areas. This was a critical finding that required immediate corrective action. We initiated a review of existing DSS internal operating instructions and procedures that revealed numerous instances in which DSS guidance was not compliant with the national investigative and adjudicative standards. On August 16, 1999, pending a rewrite and republication of the DSS Personnel Security Investigations (PSI) Manual, internal guidance was promulgated to all DSS PSI personnel to immediately ensure compliance with the national investigative standards. The PSI Manual has now been republished with appropriate revisions. Additionally, refresher training of field agents on the new PSI Manual is under way.

I would also like to point out that we will be conducting a random sampling of Top Secret and Periodic Reinvestigations conducted during the period of 1996-98 to determine any risk associated with the conduct of those investigations.

Quality control problems (Recommendation #9 of the GAO Report):

DSS has several initiatives under way to improve and ensure the quality of our personnel security clearance investigations and other security products and services. To accomplish this, we have established a Standards and Quality (SQ) function under the authority and direct control of one of our senior executives. Under the umbrella of SQ, a Standards and Evaluation Office will have responsibility for establishing and maintaining standards for technical competency and knowledge of program requirements. On a periodic or aperiodic basis, DSS employees in the investigative or industrial security professions will be evaluated against these standards to ensure their initial and continued competency and professionalism. There will be a documented history of each individual's initial and periodic training and/or remedial training, as necessary. As the results of these evaluations are reviewed, this office will also serve as a conduit for information to the DSS Academy to ensure continuous improvement in training methodologies and core competency curriculum.

I have concurrently established a Quality Management Office (QM). Complementing Standards and Evaluation, the QM mission serves more broadly throughout the Agency by placing the emphasis on quality at the outset of each process, thereby reducing the problems that might otherwise surface in an evaluation of the final product. Working in conjunction with a structured Productivity and Quality Council that represents the various elements of this Agency, the QM effort will apply sound management practices to the identification of constraints to productivity and quality. Where appropriate and

necessary, alternatives and changes will be adopted and put into place. The system will be adjusted to eradicate impediments to quality production.

Training issues (lack of training for investigative and case analyst staffs) (GAO recommendation #10):

Earlier in my testimony I spoke briefly about our new DSS Academy. Since July we have focused our efforts on building a quality education and training infrastructure and reinvigorating our security curriculum for our external customers in DoD, industry and for the security professionals within the DSS workforce. We have identified and contracted for 32,000 square feet of space to house all Academy operations. These spaces are adjacent to our main operations facility in Linthicum, MD, and will be collocated with our newly established Standards and Quality organization that also includes our Operations Research Office and our Counterintelligence Office. We expect great positive synergy from this organizational alignment, which allows for day-to-day interaction and cross-feed of the knowledge that will underpin DSS operations. Buildout of the Academy facility is currently under way with expected occupancy beginning in February of this year. We are taking this opportunity to initiate a solid communications infrastructure to assure that the Academy will have the opportunity to integrate and leverage the most current of education and training technologies to enhance both the effectiveness and quantity of its education, training and awareness products.

The Academy is also expanding its staff, adding senior subject matter expertise in its key curriculum areas of Personnel, Industrial and Information security as well as the crosscutting areas of counterintelligence and information systems security. Additionally, DSS professional development resources have been integrated with the Academy organization to focus on management of the link between education and training and the development of the DSS security professional. With these resources, the Academy is structuring a developmental curriculum that will be integrated with subject matter training at career progression phase points.

Curriculum development has been the second major Academy thrust, with several major initiatives undertaken beginning in July 1999. The central activity has been the formal review and validation of all courses. Curriculum Stakeholder Panels composed of Academy, DSS, DoD and industry customers have been formed and are evaluating each Academy course offering. We expect to complete course validations for all external course offerings in the spring of this year. There will be an annual review of each course and curriculum area.

Internal to DSS, the Academy has conducted formal training need assessments for the Agency's personnel investigations, industrial security and case analyst career areas as well as for Agency-wide technical training. Based on these analyses, the Academy is revising the basic curriculum for these security professionals; revising and reinvigorating structured mentoring programs for each specialization; and designing continuing education and training programs for each. Pilot courses for each area will be delivered

early to mid-year. This year we will also increase emphasis on the leveraging and integration of technology to support curriculum content and distribution.

Within the coming year, we will also begin to focus on the reestablishment of the security awareness program. This will begin with the hiring of a program manager who will be responsible for building the program with emphasis on traditional security awareness products and on technology-based products to enhance their impact within the security community.

Timeliness Issues and the Case Control Management System (CCMS) (GAO recommendation #11):

DSS has been under severe criticism for the production problems caused primarily by a problematic and inadequately tested Case Control Management System (CCMS). Deployment of CCMS in October 1998 significantly impacted on PSI processing times. The CCMS was designed to be a paperless system when used in conjunction with an Electronic Personnel Security Questionnaire (EPSQ) designed by DSS. However, at the time of deployment, use of the EPSQ was significantly below 50%. This prompted last minute development of systems and processes to handle paper request forms that were not compatible with the system. When workaround systems and processes were hastily designed and deployed without proper testing, it proved to be almost fatal to the system. CCMS was also deployed without a management reporting capability, with inadequate design documentation from the contractors who designed the system, and with no in-

house technical expertise to manage the complex environment and perform the integration activities required for a successful system development and deployment.

During 1999 three separate teams assessed the problems associated with CCMS. Their findings culminated in the decision to turn CCMS operational management over to experienced professionals in the Air Force. In August 1999, a Program Management Office was established under the auspices of the Air Force. That transition has now been completed.

While we have made improvements in case processing times, current case closings remain at slightly less than 1200 a day. We had projected a throughput of 2500 case closings per day by the end of January 2000. Unfortunately, delays in receiving system hardware and resolution of Y2K issues that necessitated deferral of software enhancements/upgrades have precluded us from reaching that objective. We anticipate an increase in system throughput once new system hardware is received, installed and satisfactorily tested; however, we will not see a substantial increase until such time as the integration of both system hardware and software improvements reduce the need for human intervention of various case processing tasks.

By May 1, 2000, in coordination with the Assistant Secretary of Defense (C3I) and Program Analysis and Evaluation (PA&E), I must provide the Deputy Secretary of Defense a plan to enhance or replace CCMS. Additional funding in the amount of $47M has been provided for FYs 99 through 2005. This funding is for stabilization and

enhancement to support system upgrades, thereby increasing system capacity. Additional future funding requirements for CCMS are unknown at this time but are expected to be included in our May 1 plan.

Periodic Reinvestigations (PR) Backlog within DoD and DSS PSI Workload (GAO recommendation #6):

The PR backlog has reached significant proportions. (Based upon a recently revised scrub by the Department, the backlog is estimated to be approximately 505,000.) This backlog, which includes reinvestigations of DoD military and civilian personnel and contractors, is not a recent phenomena; rather it is the result of policies that were previously implemented that established quotas for the Military Components on the number of PRs that could be requested, resulting in a backlog of required reinvestigations since approximately 1995. This policy was an attempt to help DSS reduce its case completion times. Additionally, policy changes affecting the frequency and scope of PRs have contributed to the difficulties we are now experiencing in conducting the required investigations. Customer requirements, driven in part by an upsurge in information technology positions in government and industry, have resulted in an increasing demand for clearances in general.

Even without consideration of the PR backlog, we are experiencing an ever-increasing personnel security investigations workload due to changes in investigative scope for Secret and Confidential clearances, historically declining manpower resources, and increased customer demand for clearances driven by program requirements. The DSS

increased customer demand for clearances driven by program requirements. The DSS budgeted caseload for FY00 is 16% higher than was anticipated in last year's President's Budget (663.8K cases vs. 572.1K). This increase is expected to grow by another 5% in FY01, followed by more modest increases in the outyear projections. Recent implementation of Executive Order 12968, which implemented the new investigative requirements, has resulted in additional field work over what was required by the automated processes of the past.

DSS has established several initiatives to more effectively manage this significant increase in clearance demand while at the same time reducing the inherent risks associated with outdated investigations on individuals already accessing classified information – thus reducing the vulnerability of "insider threat." One of those initiatives is the development of a predictive model to identify those cases that pose a higher risk based on responses to certain questions on the personnel security questionnaire (PSQ). Our studies suggest that scoring based upon responses to this subset of PSQ questions can identify better than 80% of investigations that are likely to result in a revocation/denial within less than 20% of the population. This algorithm will be applied at the front end of our investigative process to ensure that potentially high-risk investigations receive priority processing.

A second initiative consists of a two-phased approach to outsourcing some of our investigative workload. Early in June 1999, we recognized that there was insufficient capacity throughout the DoD and contractor workforce to meet this significant increase in

customer requirements. Phase I of our plan was implemented immediately through the release of two letter contracts to contractor investigation providers in order to augment the DSS workforce in the field. Additionally, we also placed a number of military reservists on active duty as investigators to augment our workforce. Currently, we have over 50 reservists on extended active duty tours. We are proud that we have developed this reserve capability and that we manage it with a staff of only two reserve personnel. DSS has budgeted nearly $4.0M to support reserve activities in FY00. We intend to expand our reserve program by bringing additional reservists onboard as investigators and also to provide targeted expertise in various staff functions such as program management, quality management, and inventory control. In addition, we are in the process of standing up a drilling Reserve Unit at DSS that will consist of reservists permanently assigned to DSS. When fully operational, our drilling Reserve Unit, augmented by individual reservists on extended active duty tours, will provide us with a cost-effective, flexible and highly trained workforce that we can use as necessary to meet changing mission requirements.

Phase II of this augmentation plan is still in the implementation phase and includes a contractual program for a complete "end-to-end" investigation. The advantage to this approach is the ability to completely manage the additional workload outside of the DSS CCMS, thereby minimizing the impact on a system already overstressed. As part of implementation, the risk to national security will be managed through the application of the predictive model, which determines high- and low-risk cases as explained earlier in this testimony. Our plan is to process low-risk cases through the contracted effort while

retaining the high-risk cases within DSS. We anticipate awarding contracts in the February - July 2000 time frame. The same investigative standards and quality requirements will be applied to the contractors as are applied within DSS to ensure a seamless and quality product to our customers. This collaborative effort will result in the building of a competitive industrial base to meet current and future investigative workload surges by our customers. Additionally, in a memorandum dated September 19, 1999, the Assistant Secretary of Defense (C3I), mandated that all investigations for DoD civilian personnel, except for overseas investigations, would be conducted by the Office of Personnel Management beginning October 1, 1999. This arrangement will be reviewed at the end of FY00 and each subsequent fiscal year until the PR backlog is resolved.

We are fully cognizant of the impact of the PR backlog. We are working hard to maximize other efficiencies within the PSI program in order to increase our productivity and systematically address the pending PR backlog.

Establishing a Strategic Plan (GAO recommendation #5):

We are very happy to report that we are fully compliant with the GAO's recommendation to establish a strategic plan in accordance with the Government Performance and Results Act. The DSS FY 2000-2005 Strategic Plan was recently completed and promulgated and is available for the Subcommittee's review upon request. The plan outlines our goals, objectives, mission, vision, and values, and also explains how DSS will maintain a

strategic focus on day-to-day activities. Our performance plan is currently under development and quarterly performance reviews will commence in January 2000.

Revitalization of the Industrial Security Program (JSC II Report -- Recommendation #20):

Over the last decade, rapid technological developments and increased globalization have resulted in more diverse and complex threats to our nation's sensitive information and technologies, significantly impacting upon the complexity and scope of our industrial security mission. Additionally, the increased use of automated information systems (AIS) has changed the knowledge, skills and technical expertise required of our industrial security representatives (ISR) who work with industry to establish and maintain effective security programs to protect classified information. We are facing many challenges with respect to our administration of this program as we strive to provide industrial security services in this more complex environment with fewer ISR personnel, to reestablish a focus on security reviews, and to provide the training that is necessary to upgrade the skills and knowledge required of our security professionals today.

The problems plaguing the PSI program in DSS during the past few years have, to a great extent, resulted in inattention to the industrial security program. A previously designed automated industrial security system that was to provide the data to assist in managing this program could not be fixed due to more pressing problems with the CCMS and, except for certain portions of the system which are still in use today, the system generally became unusable. Advice and assistance visits to contractors were often stressed in lieu

of regularly scheduled facility security reviews and ISR personnel were used to augment the PSI workforce.

Although efforts were already under way to refocus attention on this program when I arrived, there was much work yet to be accomplished. Therefore, in September 1999, I directed a study (i) to develop recommendations for improving our administration of the ISP, and (ii) to determine the feasibility of augmenting our ISR workforce with security resources available from other sources. That study has now been completed and a number of excellent recommendations have resulted that we believe will effectively address some of the challenges facing us with regard to this program. I will briefly address a few of those recommendations now.

Electronic Presence – A New Way of Doing Business

As part of this study, a Concept of Operations was developed for a new automated Industrial Security System that would improve and enlarge upon DSS's presence at contractor facilities. The system would not replace the requirement for on-site security reviews; however, it would allow for those visits to be prioritized based upon potential or reported vulnerabilities and threats to classified information. This proposed system would provide industry and government customers with the ability to *input and access* relevant industrial security information, and provide DSS with the ability to technically access information regarding the security programs of cleared contractors. The system would have "trigger points" that would prompt ISR actions based on input or the

compilation of data from industry or from our government customers. Under this concept, any condition affecting a cleared facility's ability to perform on classified contracts would be reported to DSS electronically and would result in appropriate action by DSS.

As a potential "force multiplier" for DSS, the system would be linked to other relevant government databases, such as the export license databases managed by the Department of State, DoD and the Department of Commerce. This would greatly increase and improve upon the type of information we currently obtain or that is currently unavailable. We will be pursuing funding for this proposed initiative through the Programming, Planning and Budgeting System.

Another important recommendation that I would like to mention includes the proposal to use contractor support to augment ISR resources, particularly in the AIS security area. One of our greatest challenges is attracting and maintaining AIS specialists in this highly competitive environment where information specialists can command much higher salaries within industry. We believe that augmentation of our in-house AIS security specialists with experts from the private sector will significantly improve our capability to provide the necessary security oversight of AIS issues by giving us the security expertise we need in highly specialized and technical areas such as telecommunications, platforms and operating systems.

Although it will take some time for these proposals to materialize, we are moving forward to correct the deficiencies existing in the industrial security program by rewriting our Industrial Security Operating Manual (ISOM) to provide more specific operational guidance and through the hiring of additional industrial security and counterintelligence personnel. This ISOM will be completed in the March-April time frame. We also expect improvements in industrial security program performance during FY2000 as our standards and evaluation and training programs are implemented and as we continue to develop performance goals and measurements for our industrial security program.

We have a capable and experienced cadre of industrial security representatives who, with additional training and professional development, will be better equipped to meet the security demands of our customers. As our reorganization continues down into the field levels of our organization, I am confident that the effectiveness of our industrial security program will improve as sound management and leadership practices are implemented.

Counterintelligence (CI) initiatives:

I would like to speak briefly about the integration of counterintelligence knowledge and threat awareness into our Agency's core mission areas. In 1994, DSS created a CI office to work with our investigative and industrial security professionals for the purpose of imbedding CI principles into the products and services of our core mission areas. This effort significantly enhances the value of DSS PSIs as our investigative workforce can now more readily identify potential espionage indicators as they conduct background

investigations. The CI office also works closely with our ISR workforce in providing threat information to cleared contractors, which increases industry's recognition and reporting of foreign collection attempts and assists them in establishing threat-appropriate security countermeasures to ensure the protection of classified information. CI is also an integral part of our training, education and awareness mission, with our CI personnel serving as adjunct instructors in the DSS Academy's training programs for DoD and industry personnel.

Several procedural and technical improvements that will enhance services provided by our CI office to our security workforce have recently been completed or are in the late stages of completion. For example, major improvements were made in the CI office's automation capabilities, in particular with respect to accessing U.S. CI and Intelligence Community databases in order to provide better threat data to DSS field elements and defense industry faster and more conveniently.

Funding Issues for DSS:

The 1997 Quadrennial Defense Review (QDR) directed DSS to "reengineer business processes . . . by streamlining the security investigative process and *implementing service fees*." Originally, the plan, as submitted to the Office of the Secretary of Defense (Comptroller), (OSD(C)), was to implement Fee for Service (FFS) as a test year in FY99 for the PSI program, with full implementation in FY00. Additionally, FFS for the

Industrial Security Program and the DSS Academy was to be implemented with a test year in FY00 and full implementation in FY01.

During the FY99 test year, operational results provided evidence that DSS programs were not suited for FFS and should potentially be removed from the Defense Working Capital Fund (DWCF). In accordance with this evidence, Program Decision Memorandum (PDM-1), dated August 16, 1999, stated "the Director, DSS, in consultation with USD(C) and ASD(C3I), should reevaluate implementation of full fee-for-service and provide recommendations to the Deputy Secretary of Defense by May 1, 2000."

For FY00, DSS is using the concept of service-level billing to bill its customers for PSI services. Under this concept, DSS bills customers in equal monthly installments. Based on the 1999 PDM-1, DSS will continue service-level billing through FY02, or until a long-term decision is made regarding FFS implementation. However, the ISP program currently remains an appropriated budget that is devolved into the DWCF from which DSS is paid for ISP services. It is important to note that the PR backlog within industry has been funded for FY00 and FY01 at $45.4M and $40M, respectively. In July 1999, DSS began actively soliciting PR submissions from the largest contractor facilities and DSS recently solicited PR submissions from the cleared contractor community at large.

CONCLUSIONS:

Mr. Chairman, I would like to state that DSS is moving forward in a difficult environment. The scope and complexities of the problems that we are facing require careful and deliberate action. We are moving forward with a sense of urgency in a balanced and structured manner.

The employees of DSS understand the importance of our mission to national security and they stand ready, willing, and able to accomplish our mission. One of the hallmarks of this agency is our cadre of hardworking, dedicated, professional and experienced employees who have often made great personal sacrifices to work against overwhelming adversities. With continuing training, professional development and implementation of sound management practices, I am confident that we will have a security organization with unparalleled expertise.

The Year 2000 can and will be a year in which DSS focuses intensely on productivity. Everyone in DSS will think and work in terms of providing the products and services dictated by our mission. Given the care that we have taken to lay the foundation for success, we will have continuous improvement. Under PMO management and with anticipated hardware and software improvements, I also expect full recovery of the CCMS

I am increasingly encouraged by the people of DSS who understand that PSI productivity is measured most clearly in the form of *quality and timely* Reports for Adjudication (RFA) provided to the DoD Central Adjudicative Facilities. One of our people recently said to me, "I think we are getting the idea that it simply isn't a matter of moving the job onto the next step in the process; it is really all about the finished product--the quality and timeliness of the RFA." To me, that statement says a great deal about the understanding our people have with respect to our problems and future requirements. And, there are comparable examples all across DSS of appreciating the true meaning of productivity.

I feel very privileged to be the Director of DSS. With additional time, I am confident that the fruits of our recent efforts will materialize. I can assure you that we are moving in the right direction to improve our productivity and that the quality of our investigations--and all of our security products and service--will not be compromised.

Mr. Chairman, this concludes my testimony on the state of DSS. I thank you for the opportunity to discuss the recovery actions that DSS has recently taken and continues to implement. I am confident that these changes will result in the full recovery of DSS. I pledge to you that DSS will rise to this challenge.

Mr. SHAYS. OK, thank you. I am going to ask you question now. I do not want you to answer it, even if you want to answer it, right yet, because I want you to think about it. I am going to ask you how confident you are in the backlog. I want you to know that I am going to be writing a letter of request to GAO that they verify the backlog number. That we not work with guesstimates.

So, I want you, and frankly this could be a help to you because if the backlog is greater and you set out an agenda based on the backlog, you are dead before you start. Then somebody else will be taking your place saying the mismanagement that preceded them.

So, General Welch, thank you. You are on.

Mr. WELCH. Thank you, Mr. Shays. The Joint Security Commission Report II is in the public record. That is really our report for the record. I do not have an opening statement. Let me take 1 minute and remind you of what the Joint Security Commission was about.

Mr. SHAYS. Yes. I know nothing about the Security Commission. So, you feel free to really educate me.

Mr. WELCH. The first Joint Security Commission, one, was asked by the Department of Defense and the DCI for a set of recommendations to address what was seen as an incoherent and perhaps sometimes chaotic set of security guidelines. There was seen a need for much more coherent and security guidelines, both to increase effectiveness and to reduce cost.

We reported out in 1994 with a set of recommendations. It eventually led to a Presidential Decision Directive to implement the key recommendations of the Joint Security Commission. The Joint Security Commission II convened 5 years later at the request, again, of the Department of Defense and the DCI. It was asked specifically to give a grade on how the Government was doing implementing the direction of the PPD and the recommendations of the first Joint Security Commission.

The primary focus, or one of the primary foci of the Joint Security Commission I, was personnel security. Standards were inadequate and execution was inadequate. Once again, one of the primary recommendations of the Joint Security Commission II was that we had agreed to investigative and adjudicative standards, but they were not being followed by all of the Department. So, that was the background for the Joint Security Commission.

Mr. SHAYS. Anything else you would like to say?

Mr. WELCH. No. That is it.

[The prepared statement of Mr. Welch follows:]

Report

by the

Joint Security Commission II

24 August 1999

Report of the Joint Security Commission II

August 24, 1999

TABLE OF CONTENTS

INTRODUCTION **1**
PART I: MEETING THE GOALS OF PDD-29 ..... **2**
Progress in Policy and Implementation **2**
Areas Where New Policies Are Developed, Promulgated, Partially Implemented 2
Areas of Progress in Developing Policies 2
Areas of Limited Progress 3
Future Challenges 3
Key Underpinnings of an Effective Security System **3**
Reliable and Trustworthy People 4
Education, Training and Awareness, and Accountability 8
Cross-Cutting Issues **9**
Security Policy Board Structure and Process 9
Restructuring the Security Policy Board 11
The Concept of Risk Management 12
Understanding the Threat 13
Understanding the Cost 14
Security Policy Board Staff Position Funding 15
The Extranet for Security Professionals 15
Industrial Security **16**
Overseeing Compliance–A Need Overlooked **17**
PART II: SECURING INFORMATION SYSTEMS **18**
Organizing INFOSEC in the Government **18**
Defense in Depth **20**
The Threat from the Inside 22
Training the Information Technology Professional **23**
CONCLUSION **25**
ANNEXES
Annex A - Summary of Joint Security Commission II Recommendations **A-1**
Annex B - List of JSC-II Commissioners and Support Staff **B-1**
Annex C - Status of Joint Security Commission I Recommendations **C-1**

INTRODUCTION

Almost six years ago, the Secretary of Defense and the Director of Central Intelligence established the first Joint Security Commission, based on their belief that the Nation's security systems were slow to move beyond the Cold War, were inefficient, had built-in inequities, and cost more than they should. In February 1994, the Commission proposed a set of policies, practices, and procedures for a forward-looking, rational, fair, and cost-efficient security system. The Commission proposed the creation of the Security Policy Board to oversee development and implementation of security policy. The current Deputy Secretary of Defense and Director of Central Intelligence directed that the Joint Security Commission reconvene for two purposes:

- To assess progress toward the goals recommended in the original report of the Joint Security Commission and directed in PDD-29, as well as the continued relevance of those goals.
- To examine emerging security issues that may require increased emphasis as the security environment becomes increasingly dominated by electronic data systems, networks, and communications systems, and as business and technology become increasingly global.

Our report treats these two purposes in turn. Part I assesses the current state of progress towards the goals directed in PDD-29. Part II focuses on the increasingly vital business of the security of electronic information and information systems. We found a massive amount of effort underway in Information Systems Security (INFOSEC). We also found that the effort is in need of a clear enunciation of principles, goals, and definition of authorities and responsibilities. Two underrepresented but vital attributes of interconnected networks are the ability to provide essential services when under attack or when experiencing product or system failures, and having design features that provide for rapid recovery and restoration of full services after suffering a loss of capability.

INFOSEC is highly fluid and poses unique challenges, but requires security disciplines much like those that have long characterized good security practice. Personnel Security practice is intended to establish and maintain a reasonable threshold for trustworthiness through investigation and adjudication as a prerequisite to granting and maintaining access to classified information. At the same time, there is clear recognition that, because people change, the investigation and adjudication process can only assess identifiable past behavior and cannot ensure that only trustworthy people gain access or that trustworthy people will remain trustworthy. Hence, there is a need for various forms of monitoring within the system. Facilities Security establishes workspaces that are isolated from potential threats to some reasonable level, but security practices must also, through various forms of monitoring, protect against subsequent penetrations. Similarly, the first level of defense for INFOSEC is to create access controls to minimize unauthorized access to information and information systems. But, as in the case of Personnel Security and Facilities Security, access control cannot ensure that only authorized and trustworthy people gain access. Hence, security also demands capabilities to monitor activity within controlled access systems. It also demands quality people, and here INFOSEC presents one of its biggest challenges, for a pressing need exists to create a cadre of highly technical network security specialists who can continue to meet the security challenges created by the increasing reliance on information systems.

PART I: MEETING THE GOALS OF PDD-29

Progress in Policy and Implementation

The Security Policy Board structure has helped achieve significant progress in accomplishing the objectives described in PDD-29. The following sections discuss important issues where there have been varying degrees of progress. The sections cover important and difficult issues where:

- New policies have been developed, promulgated, and implemented through much of the Government;
- There has been important progress in developing policies but where work remains to promulgate new policies; and
- There has been much attention but only limited progress towards agreement on policies.

Areas Where New Policies Are Developed, Promulgated, and Partially Implemented

Developed and approved within the Security Policy Board process, approved by the President, and promulgated by the NSC, uniform adjudicative guidelines and investigative standards form the basis for reciprocity of both investigations and adjudicative decisions for classified access across the Government. With these standards and guidelines in place, there is no longer a legitimate reason to reinvestigate or readjudicate when a person moves from one agency's security purview to another. This policy saves time and resources and helps ensure fair and equitable treatment. These guidelines reflect hard-won compromises, incorporating tradeoffs between ideal security and the fiscal facts of life. Of particular importance is their recognition that, with extensive decompartmentation of once highly classified information, and with more and more sensitive material now available at the SECRET level, the SECRET-cleared population requires greater security attention than before. The regime they impose for SECRET access derives from this recognition. Still, there are important issues regarding the appropriateness of some of the standards that will need to be resolved. There are also important issues regarding the adequacy of any concept that focuses exclusively on protecting classified information. In the modern operational environment, it may be impractical or impossible to bring information critical to the mission under the safeguards provided by classification. These issues are discussed further in the "Key Underpinnings" section in this report.

There are other noteworthy accomplishments. The facilities security community, for example, working within the framework provided by the Board, has effectively achieved facilities reciprocity by issuing common standards that address relevant issues.

Areas of Progress in Developing Policies

The special access community, long regarded as a repository of arbitrary security practices, has made substantial progress toward more effective security by eliminating duplication and other venerable but questionable customs, by working toward much greater reciprocity of access eligibility decisions, and by standardizing security requirements across programs to a considerable extent. DoD's *Overprint to the National Industrial Security Program Operating Manual Supplement* has replaced multiple service-specific Special Access Program security manuals with a single set of rules; this is particularly valuable in industry, where

facilities housing multiple programs need no longer work to multiple sets of overlapping yet conflicting guidance.

The Security Policy Board forwarded the Safeguarding Directive required by EO 12958 to the National Security Council in December 1997; approval did not come until August 1999, more than a year and a half later. Yet the Safeguarding Directive is a key element of the national security program, updating uniform procedures for the handling, storage, transmission and destruction of classified information as a result of the replacement of EO 12356 by EO 12958, and establishing baseline definitions for designation of Special Access Programs (SAPs). In early 1998, the Forum approved and forwarded to the Board the financial consent form required by EO 12968; final Board approval came only a year later, and NSC action is still pending. These two examples suggest that closure is an issue that the Board must more aggressively address.

Areas of Limited Progress

The Board has not succeeded in addressing information systems security (INFOSEC), having been unable to create the intended INFOSEC committee, nor has it established a mechanism for oversight as PDD-29 provides. We discuss information systems security in Part II of this Report.

Future Challenges

Meanwhile, the security environment continues to be dynamic. Since 1994, the traditional boundaries of what we have regarded as security business have expanded to account for relevant changes in the security environment. Industry is increasingly global, and so are military activities as coalition operations are now the norm. The Internet has established rapid, worldwide connectivity, which means not only that Americans, including those in the most sensitive positions, have access to the world, but that the world has access to them. The era when the Government built its secure systems to its own specifications for its own people has given way to one in which outsourcing and use of commercial-off-the-shelf systems have become the business strategy of choice. These and similar changes offer new security challenges.

Key Underpinnings of an Effective Security System

Whatever the specific problem being considered—physical security, the classical task of protecting classified information, protecting computer and network systems, or protecting all classes of critical mission information—there are two basic underpinnings of an effective security system:

- Reliable and trustworthy people, and
- Training, education, security awareness, monitoring, and accountability of people and activities within the cleared system.

The following sections address these.

Reliable and Trustworthy People

Ensuring that all our people with access to classified information, to other mission critical information, and to information systems control and administration are and will remain reliable and trustworthy remains beyond the range of reasonable expectation. The achievable goal is for a system that maintains a reasonable and affordable standard for vetting people for reliability and trustworthiness. There has been continuing discussion about the rigor of the entry-level clearance process, with some citing the fact that the spies who damaged U.S. security interests were people who had such clearances. The Commission found that to be a circular argument; since we define spies as people who violate their trust by divulging classified information to unauthorized people, the spies under discussion will come from the population of cleared individuals.

Investigation and reinvestigation cannot carry the full burden of ensuring reliability and trustworthiness. Instead, the initial investigation provides assurance that a person has not already demonstrated behavior that could cause a security concern; it is predictive to the extent that past and future behaviors are related and to the extent that investigative practices are able to uncover relevant past behavior. Reinvestigation is an important, formal check to help uncover changes in behavior that have occurred after the initial clearance. It is, to some extent, analogous to a periodic physical. But just as a physical is only a part of a good health program, reinvestigation is only a part of continuing personnel security. Neither investigation nor reinvestigation relieves supervisors and seniors of the responsibility and accountability for being attuned to the continued security health of their people, and for identifying problems and working to solve them outside the routine reinvestigation cycle.

Some have suggested that the investigation standards should be tied to the individual's current access level. While that is, to some extent, a current practice, attempting to formally adjust the level of interest in the reliability and trustworthiness of individuals to their current level of access would, at best, be administratively very difficult. At worst, it would signal giving up on the idea of a standard that establishes confidence in all but a dangerous few who will dishonor their commitment to protect security information.

Controversy should not be about the importance of the goal, but about the utility of approaches to checking for reliability and trustworthiness. For example, there are three issues regarding background checks that continue to generate debate, each of which impacts cost and risk assessments. The three areas are neighborhood checks, telephone interviews, and financial data reporting. At present there is little analytical basis for judging the cost effectiveness of these measures. However, many security professionals strongly support them. Without analytical data on risk, there is little choice but to stay with long-standing practices in spite of doubts in parts of the community about their utility.

There are other important unknowns that need to be resolved to ensure that the process is expending resources on valid approaches to assessing reliability and trustworthiness. Data mining to detect anomalies that could indicate someone thought to be reliable and trustworthy is engaging in unauthorized activity is one example of a technique that may hold promise for reducing the amount of fieldwork. However, it could also have the opposite effect of generating leads that warrant further investigation. To make intelligent decisions about the future substance of personnel security, there is a critical need for authoritative research to determine the value of various practices.

The type of research envisioned is an interagency, multi-year effort, separately funded, conducted by research professionals under the direction of the Security Policy Board. The Commission notes efforts already underway, including the ongoing work to consolidate and coordinate personnel security research under Board auspices, recent funding initiatives in the Defense and Intelligence Communities, and a test of the cost and value of financial disclosure.

Modest resources are needed to conduct this needed research to determine whether extant security policies, standards, and criteria are adequate to support the operational security and mission assurance needs of departments and agencies in a threat-based and cost-effective manner. To help avoid duplication and waste, the commission suggests a discretionary budget line for the SPB to be used as bridge and seed money to fund projects executed by a designated department or agency.

Recommendation #1: The Co-Chairs of the Security Policy Board, leveraging efforts already contemplated or underway, should commission and fund a research effort to determine the efficacy of personnel security policies and to resolve issues about their effectiveness. The Co-Chairs should monitor this effort, ensure the proper assessment of its results, and use those results to develop appropriate policies.

The Security Research Center (SRC), formerly PERSEREC, no longer reports directly to OASD C^3I, but to the Defense Security Service (DSS). Because personnel security research must involve the whole process, not investigations alone, the SRC needs to report, not to the investigative agency, but to the policy element, which is OASD C^3I. Evaluating the results of research through the Security Policy Board structure can be expected to lead to new policies, and to their implementation. However, except in extraordinary circumstances where the benefits to be gained are immediate and substantial, the temptation for individual agencies to depart from agreed-to standards is detrimental both to standards and to interagency reciprocity. Likewise, the DoD Polygraph Institute (DoDPI) now reports to DSS. DoDPI must function as the Government's single polygraph institute, yet its organizational placement and even its name weigh against this. Like SRC, DoDPI should report to OASD C^3I; its name should be changed to the National Polygraph Institute to reflect more accurately its actual function.

Recommendation #2: DoD should reassign SRC to OASD C^3I; moreover, DoDPI should be redesignated the National Polygraph Institute with the Security Policy Board designated the National Manager and DoD OASD/C^3I the Executive Agent.

All Government agencies have agreed to background investigation and adjudication standards. The standard for reinvestigation is 5 years for TOP SECRET and 10 years for SECRET clearances. Failure to adhere to these standards can jeopardize reciprocity—acceptance of one agency's clearances by another. More important, such a failure signals to the workforce that the leadership does not believe in the security standards. Such an attitude could be highly detrimental to security awareness, monitoring, and accountability.

Further, many security professionals and the Commission believe that reinvestigations are even more important to ensuring reliable and trustworthy people than the initial clearance

investigation, since people who have held clearances longer are more likely to be working with more critical information and systems. Yet there are as many as 700,000 people listed in Department of Defense records as being overdue periodic reinvestigations, and the backlog still growing at the time of this report. CIA is also not meeting the standard for TOP SECRET clearances, but has developed a plan to reach the standard by 2000.

While 5 years and 10 years are arbitrary, the need for a standard that all agencies adhere to is not. Still, it is not feasible for the DoD to quickly dig its way out of the current situation regarding reinvestigations. Even if funding were no issue, it would take several years to provide the needed added investigators and to work through the backlog. Hence, the Commission suggests that DoD set near-term dates to start adhering to the standard as new reinvestigations come due. Further, the Department should screen all those overdue for reinvestigation to determine those who pose the greatest risk based on position and access, working off all those in that category as soon as possible. The Commission thus recognizes two priorities: first, to ensure that the vetting process is on track for all new entries, and, second, to ensure that a rational, risk-management approach is applied to reducing and ultimately eliminating the backlog. It is unlikely that DSS will have the capability to deal with this requirement. Hence, increased outsourcing may be needed. Regardless, the commitment of senior leadership and appropriate resourcing can solve this problem, as the example of the National Reconnaissance Office—which actually exceeds reinvestigation standards—proves.

At present, there is no limit on the duration of an interim clearance. DoD should set a limit of 180 days, requiring that the needed background checks and adjudication processes are completed within that period.

Recommendations #3 and 4:

- ***The Department of Defense should begin first to fully enforce the standards for reinvestigations and then, within 90 days, should screen all overdue for reinvestigation to identify those whose positions and access suggest the highest risk, and should provide the resources to complete those reinvestigations promptly; the Central Intelligence Agency should expeditiously execute its plan to eliminate its backlog by 2000.***
- ***DoD and CIA should set a limit of 180 days for new interim clearances, requiring that the needed background checks and adjudication process be completed within that period. In addition, they should screen all existing Interim clearances and promptly close out those where positions and access suggest the highest risk.***

For a number of years following the completion of the work of the Joint Security Commission in 1994, we saw little progress in addressing common standards for Special Access Programs (SAPs). In the past eighteen months, however, there has been an energetic and effective effort to apply the principles from PDD-29 to these programs. The engine for this progress has been the SPB-sponsored Special Access Program Security Standards Working Group (SAPSSWG).

While recent progress is encouraging, a continued focus will be required to complete this work. Significant issues remain, including full implementation of SAPSSWG-approved

personnel security reciprocity policies for SAPs and the elusive but desirable goal of reciprocity between the SAP and SCI communities. Fielding a SAP access database is essential to both efforts. Such a database, subject to appropriate security controls, would provide the single source for information regarding SAP eligibility determinations necessary for effective reciprocity. Its continued lack has stymied implementation of the genuine advances made in SAP policy.

Recommendations #5 and 6:

- ***The Security Policy Board should maintain a high priority on applying common standards to Special Access Programs and require that any needed policy recommendations go from the SPB to the NSC within 180 days.***
- ***DoD should immediately provide adequate funding and field a SAP access database, with appropriate security controls, to facilitate effective reciprocity.***

Reliability and trustworthiness are not requirements solely for those needing access to classified information, but apply as well to those in positions that are sensitive for reasons other than classified access. The question arises whether compartmenting security and employment suitability continues to make sense, or whether new policy should require a single program that assesses reliability and trustworthiness for both. Separate, though overlapping, Executive Orders—10450 and 12968—currently apply. There is a need to reexamine screening of personnel, both federal employees and contractors, whether for appointment to the federal, military, or foreign services, or for access to classified information or other sensitive information or facilities. Such a reexamination would recognize that harm to the nation can come from not only the improper actions of people who have access to classified information, but also from those of people with access to unclassified yet sensitive information, to computer systems, and to the critical infrastructures upon which our society depends.

Recommendation #7: The Board should propose to the NSC a new Executive Order that takes a comprehensive approach to addressing the suitability, reliability, and trustworthiness of persons employed in sensitive duties on work for the Federal Government. This would include individuals working in any capacity, and based upon the sensitivity of the duties, regardless of access to classified information. A proposal from the Security Policy Board for such an order is consistent with its stated mission in PDD-29.

Personnel security policies and practices must account for the fallibility of people and the inability to predict future behavior. Past behavior and present conditions, can *shape* what a person will do in the future but do not always *determine* it. Good personnel security, therefore, goes beyond the finding and sorting out of facts—the essence of investigation and adjudication—and moves toward creating a security-aware environment. In such an environment senior officials demonstrate a commitment to security; and from this flows the accountability of line managers. It enhances both security protections and security awareness by appropriate supplemental means; for example, some agencies may consider more frequent

counterintelligence polygraph examinations for people in particularly sensitive positions. Such an environment increases integrity by eliminating pointless opportunities to violate it. For example, it establishes straightforward, system-administered need-to-know regimes for classified material stored in electronic systems and eliminates unnecessary use of portable media. Clearly, ensuring the reliability and trustworthiness of the cleared workforce requires more than investigation, no matter how critical an element investigation is. It requires vigilance, awareness of people and their problems, and application of necessary if sometimes restrictive and intrusive security measures in a way that makes clear they exist to benefit those who must comply with them rather than to suggest that everyone is a suspect in some as yet undefined crime.

Education, Training and Awareness, and Accountability

The time from the Commission's last report to the present has been turbulent for the security-training field. Organizational downsizing and the reallocation of funding have adversely affected virtually every agency in the Executive Branch. Disbanding the Department of Defense Security Institute, which provided quality training for both DoD and non-DoD security professionals, has proven particularly damaging. Agencies that had depended on others for training have not only found their training budgets dramatically reduced, but have been challenged to find other Government courses able to accept external students, even with the remaining funds for training. Yet effective security awareness programs are essential for maintaining a workforce that is sensitive to security issues and that understands the relationship between security and the success of their own work. GSA, OPM, CIA, and DoD need to take immediate steps to re-vitalize their security training apparatus. Furthermore, because the need for training and awareness resources is significant, and because critical requirements can materialize outside the normal budgeting cycle's ability to react, a need exists for a ready source of bridge and seed money to initiate projects that a designated department or agency would then execute. Such monies could be best provided through a discretionary budget line through the SPB.

Security awareness is the responsibility of each supervisor and each individual with access to classified information or other mission critical information or systems. There is no substitute for a high level of such awareness at all levels and for accountability in line management. Counterintelligence and line management responsibility for security must go hand-in-hand: there can be no effective counterintelligence if left to a few professionals without the commitment of line managers who deal with their people every day.

Even so, a professional security force will continue to be essential to an effective program of security education, training, and awareness. It is important that this profession be considered a key part of the management and operational chain. Security, especially information systems security, has become an integral aspect of the national critical infrastructure. A robust national security training program is an important element of risk management. No one agency should bear the burden of supporting all of the Federal Government, but one or more agencies can lead with resources and attention to ensure that adequate security training will be available. The Department of Energy's Nonproliferation and National Security Institute provides one example of a coherent approach to security training that might serve either as a basis of or a model for a federal security training center. Future success in developing a national training program depends on obtaining adequate funding and support from the federal community. The

Commission supports continued efforts toward creating a national training program for security professionals.

Yet the role of the security professional is to lead and advise the process. Security is a line management responsibility. Effective security demands a cleared workforce that is knowledgeable and motivated. Security awareness programs are an essential element in creating such a workforce. Their revitalization is essential.

Recommendations #8, 9, and 10:

- ***Ongoing efforts to create, coordinate, and implement core national training for both Government and industry security officers should continue. The SPB needs to ensure that such a program is funded and supported, with a goal of implementation within two years.***
- ***The SPB should charter a coordinated, Government-wide security awareness program to be fully implemented within two years.***
- ***A funding line for bridge and seed money should be created to be used for initiating security training and awareness projects, and for security research initiatives, executed by designated departments or agencies.***

Cross-Cutting Issues

Security Policy Board Structure and Process

Key national security leaders perceive that the Security Policy Board process is cumbersome and unwieldy, takes too long to formulate policy, and results in spotty implementation of the policies it does put in place. These perceptions are justified.

We address in detail some important remaining obstacles to faster and more relevant progress in the following pages. However, the overarching issue is that both the daily detailed attention to long-standing security issues and the emerging issues demanding more emphasis and new innovation require the commitment of senior leadership to ensure effective and efficient security policies and practices. Part of that commitment has to be adequate resources directed at the right challenges. At present, the security profession is struggling with a downsized workforce and diminished resources while facing a more complex threat environment. The most obvious consequence of not matching resources to declared policy is the large backlog of overdue periodic reinvestigations already cited. However, there are others; for example,

> In the Department of Defense, security clearance processing is far behind schedule. Consequently, organizations are granting a record number of interim clearances. Furthermore, until recently, DoD SECRET clearances were based on National Agency Checks alone, without the Credit Checks and Local Agency Checks (of local law enforcement records) required by the standard. Since some 22 states do not report data to the National Agency data base, forgoing the Local Agency Check means that an applicant could have committed felonies in multiple states with no adverse information in the records checked.

The Defense Security Service has been unable to conduct security assistance visits to much of the industrial complex supporting the Department's facilities for several years.

Agencies have canceled core security training and awareness programs vital to addressing insider threats.

Information systems security policy remains fragmented at the managerial level, with responsibilities poorly defined and spread over multiple bodies.

The continued organization of threat analysis into specialty areas (such as separate centers for counterterrorism, counterintelligence, infrastructure protection, and so on) makes it difficult for policymakers and security professionals to obtain an accurate and usable picture of the threat to the things they are charged with protecting.

The disconnects between policy and resourced practice in both the Department of Defense and the CIA can be interpreted as signaling that the senior leadership has not been convinced that policy implementation warrants priority resourcing. Discussions with senior leaders in DoD indicate doubt that the policies are as relevant to the modern threat situation as should be the case. There have also been concerns expressed regarding the affordability of the policies, though the funding required is not of the magnitude that would raise an affordability question if senior leaders had confidence in the validity of the policies. In any case, there are obvious disconnects between the policy making apparatus and the resource allocating authorities. Since the intent was for the SPB decision process to reflect the views of these same resource allocation authorities, this raises the question of the effectiveness of the current Security Policy Board structure and process.

The Security Policy Board has been operating for over four years. Figure 1 shows the current structure.[1]

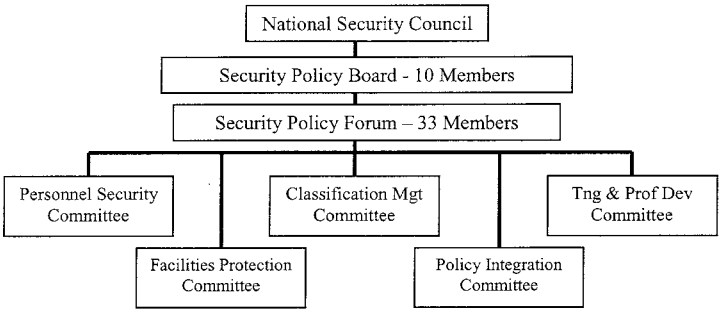


Figure 1: Security Policy Board Structure

Participants in the committees are subject-matter experts from the agencies that have an interest in a particular area. The committee members do the detailed work needed to formulate

[1] The Security Policy Forum is currently considering whether to decommission the Policy Integration Committee.

recommended policies. The Forum is composed of representatives from all the agencies involved in the security structure. The Forum meets as needed to assess the recommendation of the committees. For some issues, the Forum can approve the policy for agency implementation. For others, it passes recommendations up to the Security Policy Board, co-chaired by the Deputy Secretary of Defense and the Director of Central Intelligence and composed of senior representatives from various departments and agencies.

In our review, we found a Security Policy Board structure that is functioning at the committee level much as the original Joint Security Commission had envisioned. Furthermore, an important side benefit has proven to be the forging of positive working relationships across the Government security community, enhancing rapport and cooperation and minimizing distrust among vested interests. The Security Policy Forum has demonstrated value, though it is at this level that the desire to achieve consensus on policy formulation and approval has resulted in a process that is unwieldy, time consuming and frustrating. Hence, with the Forum often unable to resolve issues at its level, too many of them have been seen as requiring Board action. The problems of cumbersome, time-consuming processes, and spotty implementation might vanish if the Board principals exercised their decision authority on the range of issues that tend to produce stalemate in the Forum. Still, it is not surprising that they have not been willing to do this, insisting, instead, that issues brought to the Board be ones appropriate in detail and in scope of action for the level of its participants. The right solution for the Board is to empower and require the Forum to resolve the difficult issues at the right level with or without consensus.

The Security Policy Board structure is not addressing the increasingly important issues associated with greatly expanded electronic network systems or the globalization of business and technology. There is no integrated structure currently in place to address security policies associated with this class of challenges.

Restructuring the Security Policy Board

The Security Policy Forum has been particularly valuable as a means to increase the flow of information and knowledge about security matters and to create buy-in among the members. As already indicated, it has also provided the leadership needed to make important policy changes and to make significant progress towards implementation, but has done so with a high price in the time and energy expended. There needs to be a careful balance between consensus building and decision making.

Because the Forum, envisioned in PDD-29 as a body of Assistant Secretaries, has evolved into a de facto congress of Security Directors, an important management level has been effectively excluded from the security policy process. This void has, in turn, played a role in the difficulty in resolving issues at the Forum level. It has also played a role in the apparent lack of commitment to resourcing the policies. To fill this void, the Commission proposes creation of an Executive Committee, consisting of a few key players at the Assistant Secretary level. This should not be viewed as an additional layer. It is intended, instead, to be the resolution level for most issues. This Executive Committee would establish specific priorities, provide the Forum guidance as necessary, and serve as the primary avenue of communication between the Board and its subordinate structure. Working with the Board staff, the Executive Committee would be responsible for ensuring that policy initiatives, regardless of their source, do not flounder in prolonged debate, but are brought efficiently to resolution. The Forum Co-Chairs, together with the committee chairs, would jointly be responsible to the Executive Committee for day-to-day operations of the policy process.

The Commission believes that both purposes—consensus building and decision making—can be served by continuing the present membership of the Forum while creating the Executive Committee. At the call of the chair(s) of the Executive Committee, additional members with specific interests and equities could be invited to participate for specific issues.

Recommendation #11: The Security Policy Board should appoint an Executive Committee. Its members, at the Assistant Secretary level, would come from the nine agencies with permanent representatives on the Board, and would be empowered by their principals to act for them in all but the most key issues.

Under this concept, the Board would meet only to consider a few key issues. Board members would interact on matters of interest to them primarily through their empowered representative in the Forum or Executive Committee.

Changes in the security environment since 1994 generate a need for a change to composition of the Board and its scope of authority. The revolution in information technology, whose security aspects we discuss below in Part II, coupled with the increasing awareness of the need for infrastructure protection warrant adding the Deputy Administrator, General Services Administration to the Board's permanent membership, and including the Chair of the CIO Council as an observer whenever the Board discusses INFOSEC issues. The Board needs to play an active role in information technology since protecting systems involves *all* security disciplines, and only the Board and its subordinate structure are placed to achieve the necessary fusion.

Recommendations #12 and 13:

- ***The Deputy Administrator, GSA should be added as a permanent member of the Board; the Chair, CIO Council should attend all meetings and be involved in Board activities addressing INFOSEC issues.***
- ***The Board's charter should be modified to clarify its role in INFOSEC and its relationship to the NSTISSC.***

The Concept of Risk Management

The basic concept for a cost effective security system is risk management rather than the unattainable and unaffordable goal of risk avoidance. However, the concept of an effective and affordable system based on risk management assumes an understanding of the threat, the capability to measure the cost, and some means of measuring the risk. At present, there is little reliable analytical data for any of these parameters. Instead, the focus is on the cost of some specific sub-element of security practices without consideration of the impact on other security costs or on risk. Some specific examples are discussed in following sections.

Understanding the Threat

Recognition of the need for a better approach to understanding the threat led to creation of the National Counterintelligence Center (NACIC). The NACIC has made significant strides toward facilitating the flow of information to those cleared individuals who use it daily to form security countermeasures. However, for those seeking an authoritative source of available relevant threat intelligence, the picture is more complex. Diverse areas of concern include espionage, terrorism, threats to critical infrastructures and environmental safety, information/cyber warfare, illicit technology transfer, drug and other international crime organizations, and intellectual property fraud. Multiple infrastructures of intelligence producers, disseminators, and users—spread across agency lines—provide threat products.

This fragmentation has made it significantly more difficult for the security countermeasures community, both Government and industry, to obtain timely and accurate threat data. The most effective way to overcome this fragmentation is through a single organization designated to provide customers from the cleared community with one central location for their threat intelligence needs. The National Counterintelligence Center today has as its area of responsibility the dissemination of foreign counterintelligence information. Given additional resources and responsibility, it could become a community reference center that would provide consolidated threat data or, as a minimum, refer customers to sources of other kinds of threat data relevant to their needs. In conjunction with an expanded NACIC, advancing technology provides other possibilities for disseminating threat information, such as computerized pull-down systems that would provide data when the user needs it.

An expanded NACIC should also be given greater responsibility for providing meaningful threat information to industry partners. Both Government and industry officials have information they do not often share with one another. If the NACIC adopted a more collaborative approach whereby it consulted regularly with industry officials, the few classified threat *briefings* the NACIC now provides could turn into more useful threat *seminars*, providing both Government counterintelligence officials and industry security representatives with better two-way communication. This would allow both parties a far better understanding of the range of current problem sets and how to defend against the threat in a consolidated manner.

In April 1997 an interagency group chartered by the SPB to identify and address the process of threat dissemination issued its coordinated *Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers*, identifying intelligence items relevant to specific security needs. It was intended as a first step in developing an effective, efficient process and dialogue supporting dissemination of threat intelligence information. While it has proven helpful, there is much more potential in the group's work. The National Security Advisor, giving formal recognition that it reflects the needs of the security community, should issue the document. Once this is done, the process and infrastructure necessary for meaningful dissemination of threat data need to be more fully addressed.

Recommendations #14 and 15:

- ***Charter, fund, and staff the NACIC as the single clearinghouse for threat information for the security community.***

– ***The Security Policy Board should formally request the National Security Advisor to issue the*** **Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers.**

Understanding the Cost

As the Commission pointed out in its 1994 report, the cost of security is an elusive target. It remains so today. The Commission believes limited progress has been made, however. In 1994, responding to a House Appropriations Committee tasking, OMB first captured security cost estimates for safeguarding classified information within the Executive Branch. During 1994-95, the Security Policy Board developed a framework for estimating all security costs, not just those associated with the protection of classified information. Beginning in 1995, this framework was adapted to collect security cost estimates for protecting classified in the Executive Branch on an annual basis as required by EO 12958.

However imperfect, the annual cost reporting under EO 12958 is the most broadly applicable, if not the sole measure, of security costs to Government. Additional partial indicators of the costs of security are the special authorizations for FY99 totaling $12.2 billion. Of this amount, $2.8 billion has been authorized for computer security and biological warfare defense, $8 billion for physical security of embassies around the world, and $1.4 billion for critical infrastructure protection. Also, while not a measure of the costs of security, the exigency funding for Y2K is a rare example of spending for other priorities that will incidentally benefit security.

We see several important limitations threatening continuing progress toward accurate security cost accounting. The most important is that few Executive Branch departments and agencies have separate budget line items for security. In many cases, security resources are included in overhead accounts. Additionally, differentiating security costs related to classified and unclassified matters is problematic because security personnel and physical assets typically contribute to both realms simultaneously. OMB recognized that initial reports for the EO 12958 annual collection would be estimates at best, and that the data could not initially be audited. OMB hoped that over time the data would become more credible through repetition and familiarity with the collection parameters and refinement of collection techniques. In fairness, however, we note that there has been no follow-up measurement to ensure applying appropriate rigor to these annual collections or doing them on a department/agency-wide basis. This means that problems of comparability due to widely varying systems, security data standards, and data reliability among agencies limit the accuracy and completeness of current reporting. Furthermore, there is generally no tie-in between agency security budgets and execution of national security policies. A commitment to collect security costs by functional category against the framework developed by the SPB would overcome this shortcoming and would permit establishing, in each agency, separate budget lines for security, which would provide a straightforward and readily understandable answer to questions of security costs.

Fee-for-service has a role to play as a means for clearly delineating costs. However, the attempt to implement it concurrently with the present set of challenges facing the Defense Security Service has proven too difficult. Until DSS can fully achieve base standards and aggregate costs can be determined, fee-for-service should be tabled. Successful implementation

will include a cost accounting system that recognizes security's command function and deemphasizes its administrative role.

Given today's budgeting practices, and varied perspectives on what security means, there is no one simple answer to the question, "How much do we spend on security?" Post-Cold War notions abound that "security costs too much" or that a "peace dividend" should be found by decreasing security resources to match supposedly diminished threats. Such notions are simplistic and misinformed. Whatever its effect on our national security, the loss of the popular notion of a single, all-encompassing threat has only obscured the emergence and proliferation of often less restrained and more virulent security threats. Such novel challenges require vastly different security countermeasures prescriptions, for which the resource implications remain undefined.

Recommendations #16 and 17:

- ***The SPB should mandate collection of all security costs against the security cost framework already developed.***
- ***Agencies should call out security as a separate line item in their annual budgets.***

Security Policy Board Staff Position Funding

The Commission found that assignments to the SPB Staff during the first four years of the Board's existence generally worked well to promote the SPB's mission. Personnel detailed to the Staff brought wide-ranging experience and expert practitioner knowledge to the policy making process. However, the informal nature of the commitment creates turbulence and adversely affects Staff functions. The SPB should be supported with funded staff positions.

Recommendation #18. Provide funded Security Policy Board Staff positions and contractor support where needed.

The Extranet for Security Professionals

Effective security that has reciprocity as a key component requires effective communications among those responsible for administering it. Such communications are important for activities ranging from policy coordination to rapid announcement of changes to day-to-day tasks such as clearance passing and access verification. The Extranet for Security Professionals (ESP), currently experimental, provides a vehicle for such communications. The experiment is proving successful. ESP holds particular potential for resource savings through providing clearance and visit certification throughout Government and industry. Full development and continued operations and maintenance resourcing of the ESP, with attention to providing confidence in its future, should greatly expand its use and ensure the continued availability of what should prove to be an essential tool for more effective security.

Recommendation #19: The SPB should continue to support the ESP, ensuring its continued development, funding, and eventual operational status.

Industrial Security

Including industry observers in the committees and at the Forum has facilitated a dialogue between industry and Government that has proven beneficial to both. Industry is and will remain a critical contributor to national security. As such, it is important that the dialogue continue, but not merely at the policy level. DSS security assistance visits play an important role in ensuring effective security programs, both by serving as a means for identifying problems and potential problems and by conveying to management that the Government continues to place value on security. Yet DSS's ability to conduct these visits has eroded to the point that they have become sporadic: still good in some areas, but nonexistent in others. Industry continues to suffer from excessive backlogs in the clearance process that delays putting people to work. The Government suffers as this slows progress on classified projects and ultimately drives up costs. At the same time, the proposed program calling for industry to convert to the XO7 lock threatens to add additional costs without a commensurate increase in security. The estimated cost to implement the mandate in just five of the many Defense Companies is $24M for retrofit and $92M for lockbar conversion. Given the absence of a credible threat to the security of current containers in the continental US, money that would be spent on XO7 conversion could be better spent to augment the DSS industrial security program and to provide at least some of the wherewithal for expediting the personnel security process for industry.

There has been a notable lack of progress since 1995 in producing usable INFOSEC guidance for the defense industry. Chapter 8 of the NISPOM baseline is mired in disagreement between major players—DoD, CIA, and DoE. This situation creates a vacuum in an area that urgently needs effective, up-to-date security policy. Of particular importance is the issue, as yet unresolved, whether the document should be performance-based or prescriptive. Policy uniformity and consistency of implementation must be elements of all INFOSEC guidance. The continued inability to provide guidance to industry is creating enormous frustration in industry and weakens national security INFOSEC programs. This is an issue deserving and demanding the attention of the senior leadership in information systems security. The NISPOM must become, as it was intended, the single governing document for the industrial security program.

Recommendations #20 and 21:

- ***The Deputy Secretary of Defense should immediately put the Defense Security Service on a footing to revitalize the program of industrial security visits and to provide timely background investigations that meet the agreed-to guidelines.***
- ***The Security Policy Board Co-Chairs should require that the Executive Committee provide the full Security Policy Board an agreed-to baseline Chapter 8 for approval within 180 days.***

Overseeing Compliance—A Need Overlooked

PDD-29 assigns the SPB the responsibility for formulating and coordinating policy. It is, however, silent about mechanisms for oversight of implementation. EO 12958 charters the ISOO, but circumscribes its area of responsibility and does not address resources for it. Other relevant documents, including EO 12968, PDD-63, and OMB Circular A-130, do not provide for national-level oversight.

There is internal agency oversight, and it is essential; however, no effective mechanism is in place today to monitor policy implementation for coherence and consistency, and to ensure that policies are applied equitably and in ways consistent with national goals for standard security policies and interagency reciprocity. Such oversight is not a matter of compliance inspections, but a matter of consultative review at the policy level, designed to ensure that policy is practical, understandable, and addresses real issues, and to identify and resolve implementation issues. The SPB should establish a process for timely reporting of progress towards compliance by all agencies. The SPB is well positioned to assume this national-level oversight role.

Contributing to the general problem of oversight of implementation is the lack of a clearly defined and broadly accepted mechanism for the Security Policy Board to issue its decisions. Once the Board approves a policy, and even when a policy is endorsed in a memorandum from the National Security Advisor, there is no definitive way to institutionalize that policy for the Government as a whole. This shortcoming could be easily overcome by creating a recognized and recognizable series of binding policy documents.

Recommendations #22 and 23:

- ***Clarify the role of the SPB in national level security policy oversight, reemphasizing the SPB as the primary oversight body.***
- ***Establish a recognized mechanism for promulgating SPB decisions.***

PART II: SECURING INFORMATION SYSTEMS

The goal of INFOSEC is to ensure that the National Security Community has reliable and secure networks to originate, store, manipulate, and make information available to those who need it and are authorized to have it. INFOSEC enables readiness. It must do this in a rapidly changing and increasingly more complex technical environment, against threats that are evolving and not well understood, and with a structure of authorities that is still emerging and coalescing. This part of the Commission's report recommends an approach to INFOSEC that, if implemented, will provide a coherent framework for dealing with present and future challenges.

Organizing INFOSEC in the Government

The structure of authorities for INFOSEC in the Government requires clarification and coherence (see Figure 2). An example of the need for increased coherence is found in the Computer Security Act of 1987. It was the first legislation to bind computer and telecommunications resources under a single definition. It also created multiple organizations and divided responsibilities and authorities for information systems security.

The Act emanated, in 1984, from HR-145, a bill intended to nullify National Security Decision Directive (NSDD)-145. NSDD-145 created the National Telecommunications and Information Systems Security Committee (NTISSC) as the *national* authority for information systems security. NTISSC's authority covered both classified and unclassified systems for Government and extended into the private sector. Under NSDD-145, the Secretary of Defense served as the Executive Agent for the Government in national telecommunications and information systems security matters, and the Director of the National Security Agency was the National Manager for such matters. The Chairman of the House Government Operations Committee was opposed to the defense and intelligence community role assigned by NSDD-145, declaring that it violated First Amendment freedoms. HR-145 was enacted into law as PL 100-235, on January 8, 1988. It greatly reduced the role and effectiveness of the NTISSC.

PL 100-235 amended the Brooks Act, which had conferred on OMB responsibility for "fiscal and policy oversight" of the powers assigned to GSA, NIST, and OPM. In matters of information system technology, this authority evolved first, in the Paperwork Reduction Act, into "providing direction and overseeing," and ultimately became, in the Clinger-Cohen Information Technology Management Reform Act, "directing and controlling" the agencies.

The one area of clear agreement is that INFOSEC plays a vital role in national security and in the Critical Infrastructure. Hence, PDD-63 proposed partnering relationships including the Critical Infrastructure Assurance Office (CIAO), the National *Security* Telecommunications and Information Systems Security Committee (NSTISSC), and the US Security Policy Board. CIAO also partners with NIST, OMB, and the Chief Information Officer Council (CIOC) in critical infrastructure matters. The CIOC, authorized by the Clinger-Cohen Act, has established a goal of Government-wide integration, under its auspices, of information technology policy development in coordination with OMB. At a recent briefing to the Computer System Security and Privacy Board, the CIO Security Committee presented a strategic vision of coordinating and integrating existing security groups, assessing and directing ongoing security efforts, and

leveraging existing security group resources. The CIOC is currently collaborating with the CIAO and OMB in formulating a budget for INFOSEC across the Government.

This "everyone is in charge" arrangement means that no one has responsibility for meeting the vital needs for INFOSEC for national security. The OMB, NIST, NSTISSC, and CIOC authorities for INFOSEC are *Government-wide.* At the same time, the SPB is assigned authority and responsibility by PDD-29 and the DCI's authority for DCIDs. Figure 2 attempts to illustrate the fragmentation of authority and function.

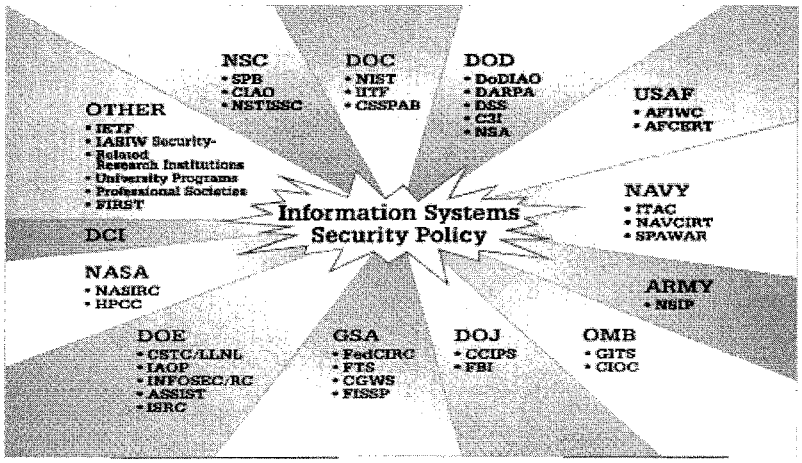


Figure 2: The INFOSEC Policy Structure

There is an urgent need for direction that recognizes the changes in information systems technology over the past decade and the role it plays in national security. The original Computer Security Act was enacted at a time when there was no foreseeing today's global information infrastructure or its importance to national security. Networks were rudimentary and segregated. Implementing directives for the Computer Security Act of 1987, OMB Bulletins 88-16 and 90-06, were suitable for remote batch processing technology. Their later incorporation into the revision of OMB Circular A-130, Appendix 3, leaves us with an urgent need for policies suitable to the modern and constantly changing technological model.

The vision of the CIO Council to join the fragmented INFOSEC leadership in partnership with OMB will have the proper focus only if it treats the growing global information infrastructure as the model—the *common* carrier of *classified and unclassified* image, data, and voice information through virtual circuits, globally integrated under the control of computers designed and programmed to function as network controllers and switches. This is the holistic reality that must drive the policies, processes, and mechanisms to bring about real world structures and processes that can assure the reliable flow of uncompromised information between, and only between, legitimate senders and intended receivers. The needed holistic

global policy approach leaves no room for fragmentation of authority and responsibility among parochial constituencies.

As an example of the conflict that is inevitable among splintered constituencies, OMB Circular A-130, Appendix 3, Section 4.f. "assigns" the Security Policy Board responsibility for *national security* policy coordination, including policy for the security of information technology used to process *classified* information. However, PDD-29 assigns the responsibility without limiting it to policy for national security or technology used to process *classified* information. This "assignment" perpetuates the fragmentation of responsibility and authority to provide effective protection of mission critical information and information systems regardless of classification.

Recommendation #24: The Deputy Secretary of Defense and Director of Central Intelligence, working with the National Security Advisor and Director of the Office of Management and Budget, should resolve the issue of national authorities for INFOSEC and propose a presidential directive (and legislation if appropriate) to implement their solution.

Defense in Depth

The widely recognized defense-in-depth model for INFOSEC is "detect-protect-respond." However, the Commission found that most of the attention and investment is devoted to the "protect" aspect with reduced attention to "detect" and little attention to "respond." What attention we did find to "respond" tends to be forensic in nature—that is, intended to discover the means used to penetrate the system to strengthen the protection. Yet we must design the security of our systems so that they continue to meet critical needs even—perhaps especially—when under attack.

In contrast to the "detect-protect-respond" model, we strongly support the "resist-recognize-recover" model described by the Computer Emergency Response Team at Carnegie-Mellon. In this context, "resist" means to raise the barriers against attacks to the highest practical, affordable level, but to do so with the understanding that sophisticated attackers are likely to breach barriers that still permit data flow outside some closed system. Further, experience to date is that the greatest damage comes from insiders. Hence it is essential that the information system be designed to control the damage from breaches by external attacks or from malicious or careless insiders. Hence, there is a need to engineer into the system the means of monitoring what is going on within the network—who is in the system, where is information flowing, what is happening to the data in the system, what is happening to the system. This kind of monitoring is essential both to protect the security and integrity of the information and to protect against denial of services that are essential to national security operations. Monitoring, however, is not an end unto itself, but is a tool. Accountability—of the system administrator, of the agency head, and of everyone in between—remains paramount. Technology alone is helpless to solve the INFOSEC problem.

It is equally important in designing secure systems to assume that sophisticated attackers or malicious insiders will find ways to do great harm to the functioning of the system. Hence

rapid recovery capabilities need to be engineered into critical systems—classified or unclassified. With the great strides forward in information system performance and with the rapidly growing dependence on such systems for all kinds of national security operations, it is now essential that all critical system design requirements include specific provisions for engineering in information system monitoring and recovery. These three levels—resist attack, detect anomalies within the system in time to control the damage, and built-in rapid recovery—constitute the needed defense in depth. The solution is a combination of technical methods and security practices and procedures, to include substantive information systems security training, education, and awareness.

Further, with system performance reaching levels that meet or exceed most users' needs, and with the growing awareness of the potential damage from malicious intruders or insiders, there is increasing commercial interest in network defense and an increasing flow of products advertised as contributing to network defense. There is also an increased willingness in the commercial sector to work with the Government to address these critical needs. In particular, there is rapidly growing interest in the finance and banking, telecommunications, energy, and information technology sectors. However, the Commission found no organized approach to partner with the commercial sector or to seek out and evaluate commercial products though an increasingly wide range of such products are in use in various parts of the Government.

One element that has helped enable outsiders to hack systems is their anonymity. The difficulty in identifying the precise source of an attack reduces the range of potential defenses while bestowing on the hacker considerable scope for operation. Removing this anonymity through creation of the electronic equivalent of fingerprints is a technological problem whose solution would prove of significant INFOSEC benefit.

Fundamental to defense in depth is the Government's inherent right to protect its information systems. Defense in depth is to ensure that the national security community can continue to conduct its business. The first responsibility is to protect that which is defended—to minimize damage and to continue to ensure system operation. Catching criminals is important, but never at the expense of protecting the information and the systems that are essential to national security operations.

Recommendations #25, 26, 27, and 28:

- ***The Department of Defense should vigorously pursue defense-in-depth funding, leveraging the growing private interest in such efforts and leading the investment needed to adequately monitor and audit information systems to detect anomalies and respond quickly to control damage.***
- ***The Deputy Secretary of Defense should take immediate steps to mandate an architecture for the Department's critical information systems that includes specific requirements for designed-in monitoring and auditing and provisions for rapid recovery and continued operation in the face of sophisticated attacks or malicious insiders whose purpose is massive compromise of information or denial of service. Such an architecture would leverage current initiatives such as DoD's Public Key Infrastructure Roadmap and work on X.509 certificate policy.***
- ***Available means of raising the barriers to system penetration should be vigorously and rigorously pursued and applied—certifications, tokens, and encryption.***

- ***The Deputy Secretary of Defense should take the lead in establishing a research and development effort that focuses on partnering with commercial interests, exploiting commercial tools, and developing special purpose DoD state-of-the-art tools for recognizing and responding to attacks against information systems.***

The Threat from the Inside

The potential for insider damage deserves special attention. Personnel security practices have long focused on attempting to deal with the dangers posed by the trusted insider who chooses to do harm. The potential for devastating damage is exponentially greater in an information technology environment. Instead of stealing a few documents at a time, the traitor within can now walk away with the contents of an entire system, or write a few lines of code that surreptitiously corrupts critical data or blatantly destroys a network.

Resist-recognize-recover applies equally to the inside threat. The first line of defense against the insider is the classic personnel security model of investigation and monitoring. And, in the case of particularly sensitive programs, the standards for investigation and monitoring are appropriately higher. System administrators, by virtue of the exceptionally important role they play—as positive forces for protection, or negative forces for damage—should receive greatly increased attention. Their special situation warrants more stringent investigations, closer monitoring, limitations on individual authorities, and stringent certification and continuing training.

Specifically, restricting root access to those few who *must* have it to ensure system operation would minimize the most serious vulnerability of a system to the insider. Even then, a two-person process should be considered for such root access. As a matter of principle, no one person should have all the system accesses necessary to shut down or to access an entire system. The two-person rule has long been in use for access to nuclear weapons. Cyber systems have become at least as important to national security as nuclear weapons and the potential for damage to national security rivals that of nuclear weapons.

Recommendations #29 and 30:

- ***The Director of Central Intelligence and the Deputy Secretary of Defense should establish rigorous clearance, monitoring, certification, and continuation training standards for system administrators.***
- ***The Director of Central Intelligence and Deputy Secretary of Defense should reduce the number of people holding root access to their systems to the irreducible minimum, and require that all such accesses follow the two-person rule similar to that used for access to nuclear weapons.***

An added risk of compromise comes from the simultaneous need for frequent upgrades, complex system configuration processes, and the need for rigorous configuration control to ensure that the designed in security provisions can provide the intended level of protection. A single unauthorized modem can compromise an entire system. Today, we find common viruses on the SIPRNET indicating unauthorized introduction of disc-based programs onto computers on

the Internet. Each such unauthorized introduction carries the risk of a compromise to the system. Automatic processes for upgrades and rigorous configuration control are essential elements of information system security.

Recommendation #31: The Deputy Secretary of Defense should require that system design include provisions for automatic upgrade of system security features and rigorous control of applications on critical networks.

The threat from the inside can also reside in products. The Government has no choice but to rely heavily on commercial off-the-shelf products for its information technology needs. However, these products do introduce a degree of risk. Whether a given operating system or other piece of software contains malicious code or an exploitable weakness is difficult if not impossible to determine. We cannot eliminate the risk, but must recognize it and maintain vigilance to the extent possible, exercising the caution consistent with the model of "resist-recognize-recover" already described. As a minimum, working with commercial software developers to ensure disclosure of foreign content in software is desirable, since foreign content is one potential source of security concern. The joint NIST-NSA National Information Assurance Partnership (NIAP) provides a mechanism for addressing security issues in commercial products, but thorough security testing is time-consuming and frustrated by both the rapid changes to existing software and the large number of products entering the market that are the computer industry's norm. Research into advanced tools that can effectively and efficiently evaluate products as they are developed and as they evolve, if successful, would provide the Government a critical tool for increasing the level of security confidence in the products it deploys.

Recommendations #32 and 33:

- ***The Deputy Secretary of Defense should develop a means for ensuring that commercial software developers certify foreign content of all software purchased by the Department of Defense.***
- ***The Deputy Secretary of Defense should further support a research effort, building on the work of the NIAP, that would lead to advanced tools to evaluate commercial computer products to be used by the Government.***

Training the Information Technology Professional

There are too few system administrators and even fewer who are fully qualified. With the increased dependency on information systems, it is increasingly important that those individuals responsible for the operation and maintenance of our information systems be well qualified. Yet, frequently, the job is performed as an additional duty or by individuals without the required background and training. Many, lacking the requisite skills for their tasks, are overwhelmed just keeping their systems up and running. A culture demanding that customer desires for performance take precedence over security creates additional vulnerabilities,

particularly when system administrators are inadequately trained junior people. Poorly trained and overworked systems administrators constitute a security threat, not from maliciousness, but from ignorance. To the operator in the field, it makes little difference whether a critical system failed because of a hostile penetration or because an untrained systems administrator made it vulnerable to a destructive attack.

The Government by itself cannot create the IT professionals it requires, nor by itself provide them with the INFOSEC grounding they need to do their jobs effectively. The Federal Information Technology Service initiative—commonly referred to as "Cybercorps"—which trades undergraduate financial aid for commitment to work for the Federal Government upon graduation, is a prototype for Government-university cooperation, but it remains unfunded. Another alternative would be establishing programs under the auspices of the Corporation for National Service, established by the National and Community Service Act of 1993, in colleges for computer science and information systems security expertise.

Currently, the Government finds it difficult to compete for talented computer experts because the salaries it pays are well below those found in industry. Professionalizing the field by creating its own career service with appropriate grade scales, may be a viable approach to recruit and retain the people it requires.

One way of attracting highly qualified, highly motivated people would be to create a state-of-the art national laboratory that would work leading-edge technologies for the Government. Such a laboratory would create the solutions to unique DoD and Intelligence Community information technology security problems, developing products and approaches to improving security features on a system basis.

Recommendations #34, 35, and 36:

- ***The SPB should formally ask the President to fund and implement a Cybercorps-like program.***
- ***The SPB should create a task force, chaired by OPM and with the support of the CIO Council, to work toward creating a separate career field for INFOSEC professionals, with requisite education, training, and certification requirements and a grade structure that competes favorably with industry for the same talent pool.***
- ***The SPB should formulate to the NSC a recommendation to create a national INFOSEC laboratory that would become the center for creating advanced solutions to unique Government IT security issues and for advancing the state of the art.***

CONCLUSION

In the five years since the original Joint Security Commission issued its report, a great deal has occurred to change the security landscape. The Security Policy Board structure has been instrumental in forging cooperation among disparate agencies where before distrust was normal. Its processes, particularly at the top, are cumbersome; however, it provides the one available structure for ensuring Government-wide solutions to problems that are no longer the exclusive concern of the defense and intelligence communities. The changes recommended in this Report should both retain the benefits provided by the Security Policy Board structure and improve its effectiveness.

Information technology has transformed the Government's ways of doing business (including the business of war), and is transforming the relationship between the public and private sectors. The current structure of authorities for protecting this technology is incoherent and self-defeating. INFOSEC professionals, lacking clear national-level guidance, are struggling with inadequate models. Attention to the question of authorities and recognition of the value to be gained through a resist-recognize-recover model of defense in depth are the minimum starting points necessary to ensure that critical systems will continue to be available to the nation.

Annex A

Summary of Joint Security Commission II Recommendations

Reliable and Trustworthy People

- Recommendation #1: The Co-Chairs of the Security Policy Board, leveraging efforts already contemplated or underway, should commission and fund a research effort to determine the efficacy of personnel security policies and to resolve issues about their effectiveness. The Co-Chairs should monitor this effort, ensure the proper assessment of its results, and use those results to develop appropriate policies.
- Recommendation #2: DoD should reassign SRC to OASD C^3I; moreover, DoDPI should be redesignated the National Polygraph Institute with the Security Policy Board designated the National Manager and DoD OASD/C^3I the Executive Agent.
- Recommendation #3: The Department of Defense should begin first to fully enforce the standards for reinvestigations and then, within 90 days, should screen all overdue for reinvestigation to identify those whose positions and access suggest the highest risk, and should provide the resources to complete those reinvestigations promptly; the Central Intelligence Agency should expeditiously execute its plan to eliminate its backlog by 2000.
- Recommendation #4: DoD and CIA should set a limit of 180 days for new Interim clearances, requiring that the needed background checks and adjudication process be completed within that period. In addition, they should screen all existing Interim clearances and promptly close out those where positions and access suggest the highest risk.
- Recommendation #5: The Security Policy Board should maintain a high priority on applying common standards to Special Access Programs and require that any needed policy recommendations go from the SPB to the NSC within 180 days.
- Recommendation #6: DoD should immediately provide adequate funding and field a SAP access database, with appropriate security controls, to facilitate effective reciprocity.
- Recommendation #7: The Board should propose to the NSC a new Executive Order that takes a comprehensive approach to addressing the suitability, reliability, and trustworthiness of persons employed in sensitive duties on work for the federal government. This would include individuals working in any capacity, and based upon the sensitivity of the duties, regardless of access to classified information. A proposal from the Security Policy Board for such an order is consistent with its stated mission in PDD-29.

Education, Training, and Awareness, and Accountability

- Recommendation #8: Ongoing efforts to create, coordinate, and implement core national training for both government and industry security officers should continue. The SPB needs to ensure that such a program is funded and supported, with a goal of implementation within two years.

- Recommendation #9: The SPB should charter a coordinated, government-wide security awareness program to be fully implemented within two years.
- Recommendation #10: A funding line for bridge and seed money should be created to be used for initiating security training and awareness projects, and for research initiatives, executed by designated departments or agencies.

Restructuring the Security Policy Board

- Recommendation #11: The Security Policy Board should appoint an Executive Committee. Its members, at the Assistant Secretary level, would come from the nine agencies with permanent representatives on the Board, and would be empowered by their principals to act for them in all but the most key issues.
- Recommendation #12: The Deputy Administrator, GSA should be added as a permanent member of the Board; the Chair, CIO Council should attend all meetings and be involved in Board activities addressing INFOSEC issues.
- Recommendation #13: The Board's charter should be modified to clarify its role in INFOSEC and its relationship to the NSTISSC.

Understanding the Threat

- Recommendation #14: Charter, fund, and staff the NACIC as the single clearinghouse for threat information for the security community.
- Recommendation #15: The Security Policy Board should formally request the National Security Advisor to issue the ***Comprehensive Intelligence Production Requirements Statement in Support of Security Countermeasures Consumers***.

Understanding the Cost

- Recommendation #16: The SPB should mandate collection of all security costs against the security cost framework already developed.
- Recommendation #17: Agencies should call out security as a separate line item in their annual budgets.

Security Policy Board Staff Position Funding

- Recommendation #18: Provide funded Security Policy Board Staff positions and contractor support where needed.

The Extranet for Security Professionals

- Recommendation #19: The SPB should continue to support the ESP, ensuring its continued development, funding, and eventual operational status.

Industrial Security

- Recommendation #20: The Deputy Secretary of Defense should immediately put the Defense Security Service on a footing to revitalize the program of industrial security visits and to provide timely background investigations that meet the agreed-to guidelines.
- Recommendation #21: The Security Policy Board Co-Chairs should require that the Executive Committee provide the full Security Policy Board an agreed-to baseline Chapter 8 for approval within 180 days.

Overseeing Compliance - A Need Ocerlooked

- Recommendation #22: Clarify the role of the SPB in national level security policy oversight, reemphasizing the SPB as the primary oversight body.
- Recommendation #23: Establish a recognized mechanism for promulgating SPB decisions.

Organizing INFOSEC in the Government

- Recommendation #24: The Deputy Secretary of Defense and Director of Central Intelligence, working with the National Security Advisor and Director of the Office of Management and Budget, should resolve the issue of national authorities for INFOSEC and propose a presidential directive (and legislation if appropriate) to implement their solution.

Defense in Depth

- Recommendation #25: The Department of Defense should vigorously pursue defense in depth funding, leveraging the growing private interest in such efforts and leading the investment needed to adequately monitor and audit information systems to detect anomalies and respond quickly to control damage.
- Recommendation #26: The Deputy Secretary of Defense should take immediate steps to mandate an architecture for the Department's critical information systems that includes specific requirements for designed-in monitoring and auditing and provisions for rapid recovery and continued operation in the face of sophisticated attacks or malicious insiders whose purpose is massive compromise of information or denial of service. Such an architecture would leverage current initiatives such as DoD's Public Key Infrastructure Roadmap and work on X.509 certificate policy.
- Recommendation #27: Available means of raising the barriers to system penetration should be vigorously and rigorously pursued and applied—certifications, tokens, and encryption.
- Recommendation #28: The Deputy Secretary of Defense should take the lead in establishing a research and development effort that focuses on partnering with commercial interests, exploiting commercial tools, and developing special purpose DoD state-of-the-art tools for recognizing and responding to attacks against information systems.

The Threat from the Inside

- Recommendation #29: The Director of Central Intelligence and the Deputy Secretary of Defense should establish rigorous clearance, monitoring, certification, and continuation training standards for system administrators.
- Recommendation #30: The Director of Central Intelligence and Deputy Secretary of Defense should reduce the number of people holding root access to their systems to the irreducible minimum, and require that all such accesses follow the two-person rule similar to that used for access to nuclear weapons.

- Recommendation #31: The Deputy Secretary of Defense should require that system design include provisions for automatic upgrade of system security features and rigorous control of applications on critical networks.
- Recommendation #32: The Deputy Secretary of Defense should develop a means for ensuring that commercial software developers certify foreign content of all software purchased by the Department of Defense.
- Recommendation #33: The Deputy Secretary of Defense should further support a research effort, building on the work of the NIAP, that would lead to advanced tools to evaluate commercial computer products to be used by the Government

Training the Information Technology Professional

- Recommendation #34: The SPB should formally ask the President to fund and implement a Cybercorps-like program.
- Recommendation #35: The SPB should create a task force, chaired by OPM and with the support of the CIO Council, to work toward creating a separate career field for INFOSEC professionals, with requisite education, training, and certification requirements and a grade structure that competes favorably with industry for the same talent pool.
- Recommendation #36: The SPB should formulate to the NSC a recommendation to create a national INFOSEC laboratory that would become the center for creating advanced solutions to unique Government IT security issues and for advancing the state of the art.

Annex B
List of Joint Security Commission-II
Commissioners and Support Staff

Commissioners	Larry D. Welch, *Chairman*	
	Duane P. Andrews	
	Robert F. Behler	
	Thomas A. Brooks	
	J. Robert Burnett	
	Ann Caracristi	
	Antonia H. Chayes	
	Cynthia P. Conlon	
	James J. Hearn	
	Bernard A. Lamoureux	
	Anthony A. Lapham	
	Frank K. Martin	
	James R. Philblad	
	Dan Ryan	
	Ross E. Schipper	
	Nina J. Stewart	
	Harry A. Volz	
Staff	Dan L. Jacobson, *Executive Director*	Navy
	Edward S. Wilkinson, Jr., *Deputy Executive Director*	CIA
	Wayne Belk	Air Force
	Christopher Bythewood	NSA
	Gary Gower	State
	Gary Harris	CMS
	Doug Hinckley	CIA
	Joseph Holthaus	CIA
	Willard Isaacs	DoD/DSS
	Virginia (Ginna) Kerry	NSTISSC
	Daniel Knauf	NSTISSC
	Ray LaVan	Treasury
	Winiferd (Winnie) Lehman	Energy
	Stephen MacKnight	Navy
	Dan McGarvey	NRO
	William Mussen	DIA
	James Passarelli	Army
	Roger Schwalm	CIA
	Dave Stevens	NSA
	Administrative, Secretarial and Clerical Support:	
	Annette Purcee	CIA
	Phyllis Norling	Navy
	Deborah Jermunson	IDA

Annex C

Summary Status of Joint Security Commission I Recommendations

Rec #	Recommendation	Implementation / Status
JSC_001	One-level classification system with 2 degrees of protection.	Secs 1.3 & 4.2 of EO 12958 issued 20 Apr 1995, retains three levels of classification: Top Secret, Secret, and Confidential.
JSC_002A	Integrate all special access, SCI, covert activities etc. into the new classification system.	EO 12958 issued 20 Apr 1995, did not require the integration of all controlled access activities.
JSC_002B	Combine all special control channels into a single channel with codewords for need-to-know lists.	EO 12958 issued 20 Apr 1995, rejected JSC recommended classification system. However, agencies have made important progress, and continue to seek fewer categories under more integrated special access and compartments, in response to initiatives by the SPB.
JSC_003	Review and validate categories of sensitive information for inclusion under the secret compartmented access control system.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DCIs CAPOC, DOEs SAPOC and DoDs SAPOC review and validate the categories of sensitive information included in SCI programs and NFIP-funded SAPs and Restricted Collateral programs.
JSC_004	Managers shall review information within compartments/ subcompartments and consolidate into the fewest possible compartments.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoD' SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005	Establish uniform risk assessment criteria.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994. and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005B	Conduct independent risk assessments of compartmented access programs.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005C	Across DoD and the IC, review similar compartmented access programs to ensure reciprocity.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_005D	Institute a mechanism to review designation, coordination and integration issues for compartmented access programs and ensure other government elements are advised of such programs affecting their interests.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish the review recommended on a continuing basis.
JSC_006A	Develop a single set of standards for compartmented access.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The NISPOM Supplement cites DCIDs as personnel, physical, and technical security standards for all SCI programs. For SAPs, the DoD issued the NISPOM Supplement Overprint recognizing a common set of security standards for each of three sensitivity levels.
JSC_006B	Provide for waivers down from compartmented access security standards when there is no impact upon	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995, as well as through SPB Issuance 4-97, Reciprocity of Facilities dated 16 Sept 1997.
JSC_007A	All intelligence reporting within compartmented channels be severely restricted to limit the amount of information that could compromise sources/methods or has exceptional political sensitivity.	Policy issues addressed with the Issuance of DCID 1/7 on 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report

Rec #	Recommendation	Implementation / Status
JSC_007B	Intelligence reporting within compartmented channels not related to sources and methods should be released as generally protected information.	Situation improved with the issuance of DCID 1/7 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report
JSC_008A	Establish a separate entity to work with special access program managers and combatant commanders to ensure these commanders are aware of compartmented information pertinent to their responsibilities.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Continued monitoring required.
JSC_008B	Allow combatant commanders to brief staff members with a need-to-know on compartmented access information.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Implementation remains within the management and oversight structures of DoDs SAP Oversight Committee (SAPOC) and the DCIs Controlled Access Program Oversight Committee (CAPOC).
JSC_009A	Rescind the blanket cover status for NRO.	Cover status was rescinded on 25 Apr 1995 by the DNRO.
JSC_009B	Review and limit cover status to covert intelligence or operational missions.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Fully implemented under DoDs SAP Oversight Committee (SAPOC) and SAP Coordination Office (SAPCO) and the DCIs Controlled Access Program Oversight Committee (CAPOC).
JSC_009C	Review existing covert contractual requirements to determine those that may be canceled as soon as advantageous.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Fully implemented under DoDs SAPOC.
JSC_009D	Develop new policies to limit the use of cover.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The CAPOCs annual review of unacknowledged or cover status considers the need for the use of cover.
JSC_010A	The DoD SAPOC should evaluate actual security countermeasures for SAPs and review unacknowledged	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Countermeasures / security provisions were "standardized" with the issuance of NISPOM Supplement "Overprint".
JSC_010B	Assign security oversight responsibilities for controlled access activities to an independent DoD office outside the special program	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. Security oversight for DoD has been assigned to the ASD/C3I.
JSC_011	With the exception of "GOVIND" and "REL TO," eliminate dissemination and control markings.	Implemented through issuance of DCID 1/7 30 Jun 1998. Compliance to be assessed through annual report provided by SPB Staff to the DCI and the DepSecDef on compliance. Staff developing survey tool to support compilation of annual report
JSC_012	Develop government-wide guidance for sharing classified information with coalition partners and the UN.	The International Security Working Group (ISWG), is working to revive the National Disclosure Policy (NDP). DCID 5/6 issued 30 Jun 1998 is the foundation of the government-wide guidance.
JSC_013	Conduct zero-based review to ensure personnel with need-to-know receive access to SAP info.	Implemented through DepSecDef Memorandum, dated 5 Jan 1994 and DCID 3/29, dated 2 Jun 1995. The DoDs SAPOC, DOEs SAPOC and the DCIs CAPOC accomplish this on a continuing basis.
JSC_014	No individual should sign more than two nondisclosure agreements; one for collateral information and one for compartmented information.	A standardized nondisclosure form has been developed, however the recommendation remains open awaiting the proper technology.
JSC_015A	Classifier should attempt to identify a date or event when information can be declassified	Sec 1.6(a) of EO 12958 issued 20 Apr 1995 requires this principle be implemented.

Rec #	Recommendation	Implementation / Status
JSC_015B	Aside from limited exemptions, classified information will be declassified after ten years if no date/event is specified.	Sec 1.6(b) of EO 12958 issued 20 Apr 1995 implements this principle but does provide for eight exemption categories.
JSC_015C	For a narrow category of information the 10 year timeline for automatic declassification may be extended to 25 years.	Sec 1.6(c) of EO 12958 issued 20 Apr 97 requires implementation of this principle. ISOO Directive No. 1 provides further specific guidance. Such extensions are exercised by the Original Classification Authority (OCA).
JSC_015D	Specify that a very narrow category of information will be exempt from the 25 year timeline for automatic declassification.	Sec 3.4(b) of EO 12958 issued 20 Apr 1995 requires implementation of this principle. ISOO Directive No. 1 provides further specific guidance. Such extensions are exercised by the agency head, and reported through the ISOO to the President (for approval/reversal).
JSC_016A	Strong oversight is needed from the security executive committee and at the agency level.	Sections 5.3 and 5.4, EO 12958 issued 20 Apr 1995 require both agency and national-level oversight, with ISOO to monitor and report annually to the President on agency programs, and on overall program status.
JSC_016B	ISOO should be part of security executive committee.	ISOO is a member of the Security Policy Forum created by PDD 29 and chairs the Classification Management Committee.
JSC_016C	Agencies need to strengthen oversight and appoint a classification ombudsman.	EO 12958 issued 20 Apr 1995 did not require an ombudsman, but requires agencies to designate an official responsible to direct and administer a program for compliance with the order, to include an ongoing self-inspection program, rating officials on performance of duties under the order.
JSC_017	Establish process to evaluate sensitive but unclassified information within DoD and the IC.	This recommendation has been influenced by recent events. The PCCIP and PDD-63 have caused the Intelligence and DoD communities as well as the rest of government to address the issue of critical information' the aspects of which share a common range of concerns with SBU.
JSC_018	Establish the DCIs counterintelligence center as one-stop shop for CI & security countermeasures threat	PDD-24 issued 3 May 1994, established the National Counterintelligence Center, which was identified as the primary source for threat information. The NACIC is providing foreign CI threat information.
JSC_019	DCIs CI center create a community-wide CI/SCM database for government and industry use.	On 13 Nov 1997, NACIC established a Threat Information collaboration realm on the Extranet for Security Professionals (ESP). Anyone with ESP privileges has access to this realm. The NACIC is currently in the process of populating this realm with unclassified CI/SCM related information and creating links to existing CI/SCM sites. Funding remains an issue with regard to the automated systems.
JSC_020	Clearances should be requested only for personnel who require access to classified information or technology.	Approved by SPB 24 Apr 1995. EO 12968 issued 7 Aug 1995, requires this be implemented.
JSC_021	Fee-for service mechanisms be instituted to fund security requests.	DoD is in the process of implementing fee-for-service for security clearances. The CIA rejects the concept of fee-for-service.
JSC_022	Formal prescreening of contractors be solely performed by the government or an independent contractor hired for that purpose.	NISPOMSUP (Feb 1995), para 2-205, addresses the recommendation in the "Agent of the Government" concept. The Personnel Security Committee of the SPB recommends that prescreening be a self-evaluating process without direct intervention from a third party.
JSC_023	Staff and contract employees should be formally prescreened for a clearance or access only with their knowledge and consent.	The NISPOMSUP adequately addresses the recommendation for contractors. The same procedures should be extended to government
JSC_024A	NISP Personnel Security Questionnaire (PSQ) form be used throughout DoD and the IC.	The recommendation is complete with the adoption of revised Standard Form (SF) 86 in Sept 1995.

Rec #	Recommendation	Implementation / Status
JSC_024B	Develop a standardized prescreening form.	The Personnel Security Committee has made recommendations regarding prescreening but has been unsuccessful with its development. The SF-86 form, appears to be the most complete form available, yet provides no useful information to the applicant regarding their chances for successfully completing security screening process.
JSC_025	DoD and DCI increase investment in automation to improve efficiency	Effective Feb 1999, the DCII and SII computer databases link DoD and OPM systems. Currently, the SAPSSWG is exploring possible data base solutions, to include the DCII, SII, DoDs Joint Clearance and Access Verification System (JCAVS) and a SAP/SCI data base network.
JSC_026A	Investigative standards for TS clearance/SAP access be an SSBI with a scope of 7 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. Although the standards have been adopted by all government agencies, do to financial constraints some agencies are not meeting the standards.
JSC_026B	Investigative standards for Secret clearance be NACI and credit check.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. DOD implemented 1 Jan 1999.
JSC_027A	Re-investigation for SCA be a SSBI occurring aperiodicaly not less than every 7 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. There is a backlog due to financial constraints at a number of government agencies for re-investigations at both the Secret and Top Secret levels.
JSC_027B	Re-investigation for Secret be a NAC, local agency and credit check conducted on an aperiodic basis not less than once every 10 years.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. DoD implemented the Secret standards in Jan 1999 but has a significant backlog in Secret re-investigations.
JSC_028	All agencies should have Employee Assistance Programs available.	Approved by the U.S. Security Policy Board on 24 Apr 1995. EO 12968 issued 7 Aug 1995 directs that Employee Assistance Programs be established.
JSC_029A	All investigative and adjudicative organizations begin an orchestrated process improvement program.	The TPDC has completed Investigative Training Standards which are under review by the PSC. Course development should be completed in 1999. The TPDC is developing both a community basic adjudicator course and a Senior Adjudicator Seminar. The seminar is scheduled to run four times annually, beginning in 1999. Core training curriculum is scheduled for completion in Aug 1999.
JSC_029B	Develop standard measurable objectives for adjudications, investigations, and appeals.	The U.S. Security Policy Board developed common adjudicative guidelines and investigative standards to satisfy these requirements and are currently developing training courses to conform to them.
JSC_029C	Interim clearances be granted based on favorable review.	Sec 3.3(c) of EO 12968 issued 7 Aug 1995 implements this recommendation, but the investigation must be no more than five years old.
JSC_029D	Standard interim access process.	The President approved "Investigative Standards" on 25 Mar 1997 in accordance with EO 12968. Access will be granted pending a favorable review of the SF-86.
JSC_030	Adopt common adjudicative criteria.	The President approved "Adjudicative Standards" on 25 Mar 1997.
JSC_031	All DoD adjudicative entities (except NSA) be merged.	Currently under review by DoD/IG and ASD/C3I.
JSC_032A	Any individual who as an existing clearance cannot be re-adjudicated.	Approved by the U.S. Security Policy Board 24 Apr 1995. EO 12968 issued 7 Aug 1995 adopted this recommendation.
JSC_032B	The authorities of program managers to limit access determinations should be limited to does the person have the proper clearance and need-to-know.	Approved by the U.S. Security Policy Board 24 Apr 1995. EO 12968 issued 7 Aug 1995 adopted this recommendation.
JSC_033	Agencies should identify who has conditional clearances or waivers through the use of standard codes.	The SII and DCII databases were linked in Feb 1999. Cases flagged with wavers, exception, etc., are omitted. Phase II is addressing how to accommodate these type coded cases. Programming change to effect the DCII for these cases has been submitted to DSS with a target date for completion of Feb 2000.

Rec #	Recommendation	Implementation / Status
JSC_034A	Clearance procedure safeguards be adopted, but not to include trial type procedures for civilian employees.	EO 12968 issued 7 Aug 1995 incorporates multiple procedural safeguards, but not trial-type hearing.
JSC_034B	All DoD employees facing denial or revocation of a clearance by informed they have a right to counsel.	EO 12968 issued 7 Aug 1995 implements the right to counsel concept.
JSC_034C	Any documents on which a proposed denial or revocation of clearance is based should be available to the DoD civilian employee affected, if privileges and national security allows.	EO 12968 issued 7 Aug 1995 implements the right to documents concept.
JSC_034D	DoD civilian employees facing denial or revocation of a clearance be able to appear before the adjudicative	EO 12968 issued 7 Aug 1995 implements the right to personnel appearance concept.
JSC_034E	DoD civilian employees have the right to appeal an adverse decision.	EO 12968 issued 7 Aug 1995 implements the concept of three-member appeal panel.
JSC_035	With respect to security clearances, military personnel should have the same rights as civilian personnel.	EO 12968 issued 7 Aug 1995 implements appeals procedures that are identical for government civilians and military personnel.
JSC_036A	Screening polygraph should be used by those who already use it, but be limited to CI-scope.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036B	Polygraph exams should not serve as a bar to reciprocity.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036C	Strict controls of questions and responses must be maintained to limit polygraph abuses.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_036D	Disqualification should not be based on physiological response alone.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_037	An independent, external mechanism shall be established to address polygraph complaints.	The Personnel Security Committee of the SPB determined that polygraph complaints were best handled by the individual agencies.
JSC_038	Develop standards to ensure consistency in administration, application and quality control of polys.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_039A	The CI scope polygraph will be the standard for all contractor personnel.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_039B	Polygraphs for all contractor personnel working at contractor facilities be conducted under the auspices of a single entity.	Recommendation rejected due to reciprocity of polygraph examinations between polygraph agencies. The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.

Rec #	Recommendation	Implementation / Status
JSC_040	Certify polygraph examiners under the auspices of a single entity.	The Forum on 27 Aug 1998 approved a polygraph MOA, that was signed by 12 of the 13 agencies that conduct polygraph programs. The MOA which addresses the 13 JSC recommendations was signed by an agency official, not lower than Director of Security, that maintains a polygraph program.
JSC_041	Consolidate CIA polygraph school into the DoD polygraph institute.	The CIA school was integrated with the DoD Polygraph Institute in Sept 1995.
JSC_042	Establishment of a robust, centrally funded polygraph research program.	Beginning in FY2000, Intelligence and DoD to sponsor additional Personnel Security research. DoDPI currently has $100K in its yearly budget for polygraph research.
JSC_043	Two-levels of storage protection for all classified material or information.	Recommendation for classified material protection not adopted in EO 12958 issued 20 Apr 1995.
JSC_044	Create a database to record certified Facilities.	The policy for "Reciprocity for Facility Use and Inspection" was approved by President Clinton 16 Sep 1997. Due to the sensitivity of a document that would contain a list of all facilities, the user community opted to develop a list of POCs with knowledge of facilities within their respective organizations. A database of POCs is maintained by the SPB Staff and periodically updated.
JSC_045	No replacement or retrofit of containers and locks currently approved.	This recommendation only affects DoD and the plan for implementation via a prioritization matrix developed within DoD and implemented via DoD 5200.1R was accepted by the SPB.
JSC_046	Routine industrial security re-inspections should be eliminated.	The "National Policy on Reciprocity of Use and Inspection of Facilities" approved by President Clinton limits the frequency of inspections.
JSC_047	Eliminate employment of domestic TEMPEST countermeasures except in response to specific threat data.	NSTISSI 7000 issued 29 Nov 1993 implemented requirements that drastically reduced the use of domestic TEMPEST countermeasures for collateral and SCI and greatly reduced its use for SAPs. All requests must be reviewed by a Certified Tempest Technical Authority.
JSC_048A	Eliminate routine domestic Technical Security Countermeasures (TSCM) inspections in favor of increase emphasis overseas.	The "National Policy for Technical Surveillance Countermeasures" approved by President Clinton on 16 Sep 1997, requires that all programs and inspections be risk base managed and threat driven and that the TSCM be authorized by agency head. The policy is implemented through a series of Procedural Guides and overseen by a working group of program managers.
JSC_048B	The government should fund a coordinated TSCM R&D and training program to support overseas inspections and future technology.	To ensure a continued high level of training, the TSCM training activity has been transferred to the NSA/NCS as the executive agent for TSCM training. Funding to further training and more importantly R&D, remains an issue and a long term strategy is under development.
JSC_049	Develop a Central Clearance Verification database to be made available to government and industry.	The SII and DCII databases were successfully linked in Feb 1999.
JSC_050	Abolish government certification of need to know for contractor visits at the collateral level.	The NISPOM implemented the recommendation, with the exception of non-contract-related visits. These visits require government certification of contractor need-to-know. Approved by the U.S. Security Policy Board on 24 Apr 1995.
JSC_051	Develop a uniform badge system for the government's cleared community.	The Facilities Protection Committee through its Facility Access WG has developed a strategy for a common badge concept and an MOA for the creation of a Configuration Control Board to oversee the strategies development. Work is underway to resolve remaining differences in MOA wording.
JSC_052A	Eliminate requirements to internally track/inventory documents.	Safeguarding Directive Sec VI-Information Controls eliminates administrative control measures which may include internal tracking and inventory and periodic inspections of classified documents, except when technical, physical and personnel control measures are insufficient to deter and detect access by unauthorized person. Safeguarding Directive is at the White House pending approval.

Rec #	Recommendation	Implementation / Status
JSC_052B	Contractors will be authorized routine retention of SECRET classified information.	The NISPOM, Chapter 5, Section 7, para 5-702 allows retention of classified material received or generated under a contract for a period of 2 years after contract completion provided the Government Contracting Activity (GCA) does not advise to the contrary.
JSC_053	Eliminate item-by-item document destruction accountability.	Safeguarding Directive Sec VIII-Destruction, states that classified information is to be destroyed in accordance with procedures and methods prescribed by agency heads. Safeguarding Directive is at the White House pending approval.
JSC_054	Revise document transmittal rules.	Safeguarding Directive Sec VII-Transmission, updates document transmittal rules. Safeguarding Directive is at the White House pending approval.
JSC_055A	Integrate OPSEC into the normal security staff structure & incorporate risk management principles into security training programs.	The OPSEC and Risk Management Training Working Groups under the TPDC have implemented a robust community training program.
JSC_055B	Delete OPSEC requirements from contracts except those in response to specific threat and only when authorized by senior management.	The NISP and the NISPOM have standardized the process.
JSC_055C	NSDD 298 be reviewed, revised or rescinded in accordance with new OPSEC requirements.	A review of NSDD-298 by the TPDC resulted in a recommendation to the Forum that revision of the NSDD was unnecessary.
JSC_056	Develop a coordinated FOCI policy.	The International Security Working Group, under the PIC, reviewed the FOCI policy and found it to be fundamentally sound. However, problems were found regarding consistency of policy awareness and implementation. OUSD(Policy) has incorporated FOCI training and awareness within the Defense Systems Management College's program of instruction.
JSC_057_	Review existing data exchange programs to ensure they are in concert with US national security & economic. goals.	A review was conducted by OUSD(A&T), the DEA proponent. A set of principles for administering DEAs has been established by DoD and disseminated to the services and defense agencies pending staffing of a new DoD directive on DEAs.
JSC_058	Provide comprehensive, coordinated threat analysis and intelligence support to facilitate risk management decisions.	An Intelligence Production Requirements Statement for SCM was agreed to in Apr 1997, and will be forwarded to the NSC for issuance.
JSC_059A	Centralize responsibility for coordinating & overseeing all foreign exchange programs.	Responsibility for DoD foreign exchange programs and issues has been centralized within OUSD(Policy).
JSC_059B	Improve/update national disclosure policy process.	There is general agreement with the language needed to update the national disclosure policy. Final clearance of the new language was requested from the State Department in 1997.
JSC_060A	DoD should expand access to the Foreign Disclosure and Technical Information System (FORDTIS) to command and other consumers.	OUSD(Policy) has expanded access to FORDTIS and continues expansion based upon command and other consumer access requests/needs.
JSC_060B	Ensure CI elements cross-check critical systems and technologies against FORDTIS.	A portion of the OUSD(Policy) international security training and awareness program addresses this issue; however, ultimate utility of FORDTIS database is dependent on consistency and accuracy of "user" (data provider) inputs.
JSC_061	Joint investigative service establish fee for service background investigations.	The concept of a Joint Investigative Service was rejected by DoD. DSS adopted a "fee-for-service" concept in FY 99 for DoD and those DSS supports. Other agencies conducting their own investigations will continue their present practice. CIA rejects the concept of fee-for-service for investigations.

Rec #	Recommendation	Implementation / Status
JSC_062	Joint investigative service to perform industrial security services for DoD and the IC.	The concept of a Joint Investigative Service was rejected by DoD.
JSC_063	Joint investigative service be established and draw resources from existing security organizations.	The concept of a Joint Investigative Service was rejected by DoD.
JSC_064	Consolidate AIS policy formulation under the joint executive security committee, and have it oversee development of a coherent policy for DoD and the IC that also could serve the entire government.	Recommendation not implemented. NSD-42, dated 5 Jul 1990, (as limited by section 10.d), created the NSTISSC, a national level body responsible for issuing national security information systems security policy for the entire Government.
JSC_065	Develop an information systems security investment strategy using 5-10% of infrastructure costs.	Not implemented.
JSC_066A	Give high priority to information systems security research and development programs.	NSD-42, 6.a.(4) and 7.c. authorize the Executive Agent and National Manager to conduct, approve, or endorse research and development of techniques and equipment to secure national security systems. NSA, in conjunction with DARPA, is conducting research and long/short-term development of Information Systems Security solutions.
JSC_066B	Assign NSA as the executive agent for both classified and unclassified infosec R&D.	NSD-42 designates NSA as Executive Agent for national security systems. PL 100-235 designates NIST responsible for unclassified systems with NSA in support role to NIST. National Information Assurance Program (NIAP), a partnership between NSA and NIST.
JSC_067	Assign DISA as the executive agent for providing infosec tools and capabilities.	Not implemented, but will be realized at the FBI's National Infrastructure Protection Center in coordination with GSAs Federal Computer Incident Response Capability, NSAs National Security Incident Response Center, Carnegie-Mellon's Computer Emergency Response Team and DOEs Computer Incident Analysis Center.
JSC_068	Establish an information systems security threat and vulnerability database, available to all DoD, IC, and industry.	NSA makes this information available to DoD, IC, and selected industry through its all-source analysis center.
JSC_069	Appoint DISAs ASSIST program as executive agent for emergency response functions.	Although DISAs ASSIST program was not appointed Executive Agent for emergency response functions, the policy and directive issuances that were intended to make this appointment (NSTISSP 5 and NSTISSD 503) were ultimately used to implement the National Security Incident Response Center (NSIRC) at NSA.
JSC_070	Establish an information systems security professional development program.	Under NSD-42, NSTISSC established the Education, Training and Awareness Issue Group to develop INFOSEC training standards and to assist development of an Information Systems Security Masters Degree Program at James Madison University. Also under NSD-42, NSA assisted NIST in developing INFOSEC training standards for use in protecting unclassified sensitive systems.
JSC_071	Create ad hoc panel to develop common approach and budget framework for defining and tracking. security costs.	A comprehensive framework for capturing estimated costs by security functionality was developed. An abridged version of framework is used to capture annual cost estimates for safeguarding classified information IAW EO 12958. ISOO gathers and reports to the President and Congress the costs to safeguard classified information IAW EO 12958.
JSC_072	Endorse joint government and industry strategy for capturing security costs within a new budget and accounting framework for security.	DoD, as Executive Agent for the NISP, receives annual cost estimates from industry for safeguarding classified information IAW EO 12829. These industry estimates are forwarded to ISOO. However, these estimates are developed on a different framework and algorithm than that used for collecting government security cost estimates IAW EO 12958.

Rec #	Recommendation	Implementation / Status
JSC_073	Develop a long-term resource strategy for security.	Not implemented.
JSC_074	Appoint an executive agent for security Training.	The SP Forum appointed the TPDC as Executive Agent on an interim basis in 1995.
JSC_075	Increase emphasis on developing and funding security education courses for management and up-to-date security awareness programs.	Not Implemented. The community has generally decreased funding and support for both security training and security awareness programs.
JSC_076	Establish a national level security policy committee to provide structure and coherence to security policy, practices and procedures.	The President issued PDD-29 on 16 Sept 1994 which provided the authority and guidance for establishing, supporting and staffing the U.S. Security Policy Board structure.

Mr. SHAYS. OK. Let me just ask you, there was a Commission in 1986. Is this the same Commission that we are talking about now or was that a different Commission?

Mr. WELCH. No, sir. The Commission in 1986, whose name escapes me, was one of the three——

Mr. SHAYS. Stillwell, was that it?

Mr. WELCH. Right. It was one of the three earlier Commissions that lead to increasing concern about the lack of standards, the lack of coherent standards for personnel, and security, and for security in general.

Mr. SHAYS. So, there was in 1986. Was there one earlier or one later? There was one in 1994, right?

Mr. WELCH. There was one in 1986. There was one in about 1988. There was another one in 1992. Then we reported out in 1994.

Mr. SHAYS. Then you were established in 1994?

Mr. WELCH. I am sorry?

Mr. SHAYS. You say you were established in 1994?

Mr. WELCH. The Joint Security Commission I reported out their first report in 1994.

Mr. SHAYS. You reported out your study. You had been in existence for how long.

Mr. WELCH. Then we disbanded. We met for a year and a half. We reported out. It eventually resulted in a Presidential Decision Directive, which then established the Security Policy Board, which was charged with implementing these recommendations. Then 5 years later, we were asked to reconvene, really for two purposes.

One, because it had been 5 years and they wanted to check on how the Government was doing. Second, by that time, there were enough indications of problems with personnel security that we were asked to particularly focus on those issues.

Mr. SHAYS. Well, you are well-aware of what GAO has said. What is your reaction to what they have said?

Mr. WELCH. I agree with what the GAO has said.

Mr. SHAYS. I want you to characterize it. I mean, is it out of concern? Should I be greatly concerned? Should you be greatly concerned? I mean, I want some characterization of—I will just tell you up-front. For me, I read it and I find it so astounding. When I was speaking to someone on the floor before I came back, I said it is so bad, it is so big that you cannot get your arms around it in one way.

I mean, if you had told me that when they did the reinvestigation the found 2 or 3 percent where they noticed that they should do further research, but when you come up with 16 percent, it is like unbelievable. That is the whole point of the investigation is to identify your problem and then go after it. So, I want you to tell me how you characterize it.

Mr. WELCH. OK. It is bad, and big, and you can get your arms around it.

Mr. SHAYS. You can, c-a-n?

Mr. WELCH. You can. So, let me tell you why I say that. Personnel security is a risk management business. That is the nature of the business. We are making judgments about the trustworthiness and the reliability of human beings. We now have, which we did

not have in the past, a set of standards on which we base those judgments. Understanding that we are always talking about risk management and we are always talking about making judgments.

So, the Government has agreed across all of the agencies of the Government, which is an immensely difficult task, that there is a set of standards that we can apply that will give us reasonable confidence that based on our knowledge of past behavior and current circumstances, we have a satisfactory standard for access to classified material.

So, the standard is in place. The standard is implementable. The standard is quite reasonable. I do not think there is any question that we can achieve those standards. But we did not. Now, you have heard a lot of reasons why we did not achieve the standard, but the solution is very straightforward. The solution is enforce the standards. We have all agreed that those are the right standards.

Mr. SHAYS. Are those standards different than what the report presented in 1994?

Mr. WELCH. The standards are quite different. When we entered the effort that was reported out in 1994, the going-in emphasis was on the cost of this largely incoherent system because there was a lot of county option. Each agency set their own standards. Just to give an anecdote to help understand it, at that time, I had three separate top secret clearances. I had four separate compartmented clearances.

As we were meeting, I happened to, be undergoing three separate background investigations. My neighbors suggested to me that perhaps we should have a neighborhood barbeque and invite all of the investigators at one time. That was what we characterized. As we began to do our work, that 18-months' worth of work, we became very concerned about personnel standards.

Our concern was that in the area of personnel security, some of the agencies had standards that we were so lax that we understood why many agencies would not accept those standards.

Mr. SHAYS. You mean, so some agencies required more than others. So, that is why you had more than one check. Is this kind of like, I used to think that, you know, when you went from red, green, brown, and then black belt, when you reached black belt you were done. Then I learned later on that you had 10 elements to black belt.

Are you saying that we have different elements in our top secret, or are you saying that different agencies just would not accept the review of other agencies because of different standards?

Mr. WELCH. Both. Each agency set their own standards. The Department of Energy had a set of requirements to grant a "Q" clearance, which is the equivalent of a top secret clearance. It is the equivalent of a DOD top secret clearance. The DCI had a different set of requirements for clearances that went by the same name. So, there was no reciprocity, but more important we did not have an agreement on what was an adequate standard.

Mr. SHAYS. That was 1994.

Mr. WELCH. That was 1994.

Mr. SHAYS. So, the focus then was, let us have one review. Let us have common standards among the various departments and agencies.

Mr. WELCH. Yes.

Mr. SHAYS. But you, in no way, were not suggesting that you relax the standards like what took place. I mean, could someone who had been with DSS go back and say listen, we were being motivated by the report that you all submitted? Could they blame your report for a part of the problem?

Mr. WELCH. Well, I suppose anyone can do that.

Mr. SHAYS. Are they?

Mr. WELCH. No. Let me comment on a couple of issues that complicated it a bit. In the end, for the Department of Defense, the standards went up. They went up considerably. This was an interagency effort under the Security Policy Board. So, it took a number of years. I cannot even remember how many, I guess until 1997, for all of these Government agencies to agree on what the standard would be.

That is when we came to the definition of what is required to grant a secret clearance, and what is required to grant a top secret clearance, and what the time period would be for re-investigations. Those standards were more stringent than had previously been practiced by the Department of Defense.

They were perhaps less stringent than someone's standards, although I do not know whose those would have been. So, from a DSS standpoint, the result of that effort was to raise the standards that DSS was expected to follow in their background investigations. Now, that would be demoralizing only if you then did not get the resources to do that.

Mr. SHAYS. But you were also suggesting that they not have to do double and triple reviews.

Mr. WELCH. That is right. That is correct.

Mr. SHAYS. So, there should have been some advantage there.

Mr. WELCH. Our hope was that, that would result in a significant cost savings. But our report did not suggest that we could reduce the cost of personnel security. We suggested you could reduce the cost of physical security and the cost of document security because of the change to electronics.

Mr. SHAYS. You did not suggest lowering the standards. You did not suggest ignoring one of the nine elements. Is that true or not?

Mr. WELCH. Not at all. In fact, our whole emphasis was that we need an agreed-to Government standard, and then you simply must follow the standard. There are two reasons for that. One is you need an agreed-to bar, some standard of judgment based on behavior and circumstances. Second, the real essence of security is security awareness.

Security does not just come from someone jumping over the bar and getting access. Within the organization, everybody in the organization has to be aware of security issues. You cannot have security awareness if the people that you are trying to persuade to have this kind of awareness do not see you adhering to standards.

Mr. SHAYS. Thank you. General Cunningham, before I ask you the question, I said I was going to ask you, I want you to spare me this problem. If you say you have total confidence, then I would want to pursue under what basis you would have total confidence. I would have you try to explain to me, in some detail, how the number was derived.

You may have total confidence. I just want to say that up front. I do not want to find that you have total confidence, but you do not know how they did it and so on. Bottom line question is do you have total confidence? First, what is the backlog?

Mr. CUNNINGHAM. The backlog has been assessed by an integrated product team operating in OSD at 5,005.

Mr. SHAYS. Do you have intricate knowledge of how they determined that? Are you accepting their number based on their expertise?

Mr. CUNNINGHAM. I am accepting their number. However, I do not have total confidence in it.

Mr. SHAYS. Fair enough. So, it is their best estimate as far as you are concerned.

Mr. CUNNINGHAM. Yes, sir.

Mr. SHAYS. What do you think we can do to nail down that number?

Mr. CUNNINGHAM. Sir, the best way to nail down that number is to have very disciplined "scrub and prioritize," scrub in this case, on the part of the military departments, industry, and other smaller entities in the security community. To that end, we, DSS, are working with the military departments to have them embrace the idea and resource the capability to have a central requirements facility on the front end of the process in the same way that there is a central adjudication facility on the back end of the process.

Mr. SHAYS. If I were to ask you for your confidence level that the number would be higher or lower, if you have no sense either way, I do not want you to pick a direction. Do you think it is likely to be underestimated, or overestimated, or do you simply do not know?

Mr. CUNNINGHAM. Sir, while I think it could be overestimated, I think the number is higher.

Mr. TERRY. Will you repeat that?

Mr. CUNNINGHAM. While the number could be lower, I think the number is higher. That is my professional judgment.

Mr. SHAYS. In other words, it could go either way, but if he was a betting man.

Mr. TERRY. It is or it is not, and that is your professional opinion.

Mr. SHAYS. No, no. Since it was my question, what I hear you telling me is that it could go in either direction, but if you were a betting man, it would be higher.

Mr. CUNNINGHAM. Yes, sir. That is it.

Mr. SHAYS. Mr. Terry.

Mr. TERRY. I want your help in coming to a full understanding of an issue. So, I am going to ask you to apply what you are going to perceive as fairly elementary questions, but I have to admit that I am somewhat lost on the role of quotas. As I am perceiving from the some of the testimony and reading the report that some of the backlog, I do not want to say "blame" or "excuse" but the causal relationship of the backlog to these quotas.

Can you explain to me when these quotas were implemented and what they are in their direct relationship toward the backlog?

Mr. CUNNINGHAM. The quotas were implemented about 1994 in an effort to discipline the clearance requests that were coming in,

in an effort to motivate those making their requests to indeed request the clearances they really needed to have. We no longer have those quotas.

Mr. TERRY. Did you do away with those?

Mr. CUNNINGHAM. No. Those were done away with in early 1999, I believe, before my arrival.

Mr. TERRY. But the damage had been done?

Mr. CUNNINGHAM. Quotas were basically saying, out of a certain percentage of the re-investigations, I do not know what the exact quota is. So, maybe 10 percent or the real high priority ones, so we are only going to make you do 10 percent.

Mr. TERRY. Is that a good generalization? Is that a ballpark generalization?

Mr. CUNNINGHAM. Let me tell you what I think I heard you say.

Mr. TERRY. All right.

Mr. CUNNINGHAM. The quotas were put on to try to get the number that were really needed, 10 percent or whatever.

Mr. TERRY. Yes.

Mr. CUNNINGHAM. But it was a large number. It was a reasonable number. However, it also, without intending to do so, created what the GAO was discussing as a pent-up demand. That pent-up demand finally becomes manifest in a backlog when the quotas are dropped.

Mr. TERRY. From my perspective, it looked like the quotas set a minimum bar that everybody strived to meet. Then just like the backlog built up from there and you used the quotas as the excuse to do that. So, I am pleased that the quotas have been dropped. Unfortunately, that puts you in a very tough position to deal with that.

Could you discuss, as my last question, and you did hit on it during your statement, but I would like you to expand on the automation of the caseload and what steps you are taking now to review the current system that I think everyone agrees is not adequate. Where are you in that process of reviewing it? Where do you feel the direction is going?

Mr. CUNNINGHAM. Yes, sir. The Case Control Management System was, as the GAO reported, in need of proper program management. Last summer, we asked for a Program Management Office, and properly trained people to run the program and run the recovery. Our judgment at that time was that it made prudent business sense to continue the system, to continue with the Case Control Management System until we knew that it was recoverable.

There was nothing in any study that said that the system was not recoverable. Our mission is security and this was central to the system. So, it made good sense to continue. When we continued, we committed to get a Program Management Office to indeed have a test capability for the system, which was not in the original architecture; to develop a concept of operations; to identify the priority requirements, support, and concept of operations to do a baseline architecture; and to do a schedule and a budget.

Those things had never been done before. They are now in the process. We will have our first look at those on March 1st. We have our Program Management Office up. It now manages all contractors. The DSS manages none of the contractors. In fact, it has iden-

tified time lines for the recovery of the system, in terms of stabilizing the system by June 1, 2000, improving the system by June 1, 2001. From June 1, 2001 through June 1, 2003, enhancing the system to meet those requirements that cannot now be foreseen.

Mr. TERRY. Thank you. Mr. Chairman, that concludes my questions.

Mr. SHAYS. Thank you very much. I have a number of other questions; some that my staff wants me to get on the record as well. I would like to clarify the budget issue. My sense was that I was being accurate in saying your budget of $74 million went up to $84 million. That the difference of that number of the $300-something is money that goes into a fund that looks at the private sector employees. So, maybe you need to help me sort out your budget a little bit.

Mr. CUNNINGHAM. The budget includes everything that we are doing this year. It is $324 million. The discrete breakout of what each one of those, each part of that composing that $324, I would like to submit that back to you in detail.

Mr. SHAYS. Sure.

My understanding is that basically your Government budgets, $84 million, and then you have a trust fund budget that really is contributed from the employers.

Mr. CUNNINGHAM. Yes, sir. It is a working capital fund.

Mr. SHAYS. Right.

Mr. CUNNINGHAM. It is a financing capability by which the requesting entities that we, say essentially the military departments, identify what level of investigations will they need to have done. Then they put the money in to cover that for the year. They budget in advance. Then they move the money to us with their clearance requests.

Mr. SHAYS. I realize that money is fungible. I mean, it may be the same person that pays ultimately. My sense is that a chunk of your budget is associated or tagged to a private company like Boeing or Honeywell, and that they then pay that cost.

Mr. CUNNINGHAM. Sir, I am not aware of that. I would have to answer you back on that.

Mr. SHAYS. OK.

We will get into that later. It raises some interesting questions that I have. Ultimately, if the private sector is paying some of it, we end up paying for it in the final product we buy. It does raise some interesting questions as it relates to the question I asked earlier. If the AIA member companies' survey has taken Boeing and said they have a backlog of 90 days in November 1999.

This is what it was. And it was 1,161 employees and it cost them $52 million, and when I went through the list, you came up with 3,247 employees costing $143 million. This is a wasted expenditure, as far as they are concerned. It would be an expenditure, if they were done in a timely basis, would not occur. Have you been presented that type of information from anyone?

Mr. CUNNINGHAM. Yes, sir. I have a copy of that correspondence.

Mr. SHAYS. Now, this is where my mind starts to work. I say, you got a backlog of hundreds of thousands, and just 3,247 cost ultimately, I believe the Government, $143 million. I mean, if anybody has a good case for arguing that you get the backlog done and

we invest in it, you do. I hope OMB has been exposed to this. Is this a document I should have comfort that is credible?

Mr. CUNNINGHAM. Sir, I think that the private sector entities who identified that problem are in the best position to state what that is costing us collectively. You are right about that. So, I appreciate the urgency that must go against that kind of a problem.

Mr. SHAYS. Have we, in the private sector, tried to estimate the cost? I mean, in other words, this same logic occurs. I mean, you have someone who is not given clearance. So, you cannot get the job done. You have people waiting in line. The job does not get done. It gets delayed. Well, that happens in the public sector as well.

Mr. CUNNINGHAM. Yes, sir.

Mr. SHAYS. Do we have people in the public sector that have tried to put a cost to this?

Mr. CUNNINGHAM. Not to my knowledge, sir. In fact, you are highlighting what I am seeking on behalf of the agency to have "scrub and prioritize" from everybody.

Mr. SHAYS. Can you tell me how many of the clearance re-investigation checks are the private sector versus the public sector?

Mr. CUNNINGHAM. Yes, sir. In general terms, about 75 percent of our work is in the military departments and otherwise public sector and about 25 percent is in the private sector.

Mr. SHAYS. Thank you. What kind of risk assessment has been developed to determine the danger the backlog poses to national security?

Mr. CUNNINGHAM. Sir, the GAO mentioned the algorithm that we have been working on and we have now completed. I will be most pleased to provide a copy to you and your committee. It is aimed at risk management. Our plan is to go into the total population of the backlog, apply the algorithm, identify which records come up as high risk from the algorithm, which we believe and have had scientific support will predict 89 percent, based on a 6.5 percent sample size, that we use it against the backlog while we are bringing the backlog down.

So that we both work the backlog down and, in the process, go after those that are identifiable as highest risk in the backlog.

Mr. SHAYS. Is that document ultimately going to be a public document or will it be a secured document?

Mr. CUNNINGHAM. Sir, it is a public document. I will be happy to provide it.

Mr. SHAYS. I am going to ask you two benchmark issues. What is your timetable for eliminating the backlog? There is another question that I want to ask. That relates to what timeframe has been established to enhance the Case Control Management System? So, timeframes, benchmarks.

Mr. CUNNINGHAM. Yes, sir. Sir, we believe that——

Mr. SHAYS. And I am going to interrupt you. I am sorry. This is based on the number that has been presented to you as the backlog.

Mr. CUNNINGHAM. Yes, sir. We believe that we can bring the backlog, as we now know it, we can eliminate the backlog by the end of calendar year 01. Sir, that is a hard task, and I will say that right up front, but I believe, as I have come to know the agency

and the ability of private sector contractors who are seeking the work to augment us, that we will be able to do that.

I believe that we can do it in good form in protecting our standards and our quality because we are requiring proper training, certification, applying our standardization and evaluation checking, our quality management, our operations research so we can do the trend analysis that goes along with it, and other activities.

It is important, sir, if I may add, it is important that we are going to use our algorithm to determine which cases should go to those contractors so that cases that we predict we will have problems, we will keep those right in the agency. We intend that all problem cases, issue cases, derogatory information uncovered, that those cases revert back to the DSS.

Mr. SHAYS. Is the integral of success, will you get so many each from this point on or will you see the vast bulk of them done from July 2001 to December 2001? In other words, by the end of this year, what do you anticipate you will have done? Will you have 50 percent of it done?

Mr. CUNNINGHAM. By the end of this year, I think it will be fair for us to expect in the neighborhood of 15 to 20 percent of it. The reason that the rest of it is achievable in the next calendar year is because the contractors will have spun-up. Our timetable for the Case Control Management System, which I have mentioned before, will have taken root.

So, that major constraint will be less so. And because all of the four contractors that we intend to put as major efforts, and they will have the opportunity to bring others in with them, that the way they manage their cases will be managed independently of our Case Control Management System.

So, it will take the agency from complete dependence on this Case Control Management System over onto another capability, all of which will be visible to us so we know that they are being done properly. In other words, we are going to have belts and suspenders.

Mr. SHAYS. I was with you until that last part. In other words, you are going to have what?

Mr. CUNNINGHAM. Well, in this hearing term, "belts and suspenders." You know, we will have it both ways. It is not a trivial point because we had all of our eggs in one basket and we are getting out of that.

Mr. SHAYS. It begs the question of whether you get greater productivity from the private sector or from the public? I realize you have to work with both sides. I understand one reason why we do the private is that we ultimately will have phased down that unusual number. So then you do not want to buildup your bureaucracy. So, it makes sense to farm it out. Does the private sector have some inherent advantages that allow them a greater productivity?

Mr. CUNNINGHAM. Yes, sir. They have agility. They are able to hire and remove people quickly. They are able to locate easily. They are able to spinup fast with a great deal of focus. They are able to marshal resources almost instantaneously, if they decide to go after the business.

Mr. SHAYS. That is a very good answer and one that I would appreciate. One of the things that we have learned on the subcommit-

tees of Government Reform is that in the private sector, three people make a decision. Ultimately, in the public sector it is 11. What that must do for ingenuity, and creativity, and timeliness is mind-boggling.

Mr. CUNNINGHAM. Sir, if I may tag onto that. We will be watching very closely what happens with these private sector contractors. Where there are better methods and applications of IT, we intend to adopt those same things ourselves.

Mr. SHAYS. Now, there are only two benchmarks so far I have heard. So, give me a few more. We are going to want to come back, I mean, whoever is chairman of this committee next year, I would imagine, and someone will pursue this issue. We will want to meet with you to determine that. We frankly would want to meet with you probably later on.

Mr. CUNNINGHAM. Yes, sir. Let me give you a few of those. When we worked with the Program Management Office and the contractors, and we saw the way they went about considering progress on the Case Control Management System, those timeframes I mentioned for the Case Control Management System, we identified the same phasing for the overall recovery of the agency.

We have a target right now for August of this year to be making the number of cases closed per day, on average, to hit that target. It happens to be 2,500 cases a day closed for the DSS. To hit that target in August, and to hit it in a sustainable way, and to hit it in a way that we are continuing to build capability.

To be able to not only take care of the backlog, but also be prepared to be able to do more than that should that arise. We expect that it will arise because of what the security environment is becoming. Therefore, the date to stabilize the agency is September 1st.

It will be manifest in the data of output exceeding input for August in a sustainable way. That we will improve the agency, not just the CCMS, but the whole agency, through June 2001. And that we will enhance our capabilities from June 2001 through June 2003. We are tying them all together, and a very good measurement will be when we hit that target in August.

That is one that I am happy to see the agency held accountable to, and would be more than happy to come back when you say.

Mr. SHAYS. Is that the first key date, as far as you are concerned?

Mr. CUNNINGHAM. Yes, sir. The whole agency right now is marshaling to hit that target in a sustainable way.

Mr. SHAYS. Just a few more questions here. What do you consider to be the most pressing problem confronting DSS? You have got lots of challenges, lots of problems. What would be really the most?

Mr. CUNNINGHAM. I am often asked this by my boss, the ASDC3I, and the answer is——

Mr. SHAYS. Wait a second.

Mr. CUNNINGHAM. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence.

Mr. SHAYS. Thank you.

Mr. CUNNINGHAM. Thank you, sir. Art Money asks me this question a lot. And the answer from the beginning was our people.

Today, the answer is the same. It is our people. This work force has had a tremendously difficult time. To bolster their morale, and we are making progress on this, to ensure they get the right training, proper preparation, proper response from their systems, those are the kinds of things we have to work on, but it all centers on the people.

Mr. SHAYS. You know, I have a few other questions. What I will do is submit them, if we feel it is necessary to followup. I will have the committee to submit it in writing and just have you respond to one or two others. I am happy to have either of you make any comment. Is there a question you wish I had asked you, General Cunningham that you could wax eloquently on?

Mr. CUNNINGHAM. Wax eloquently, sir.

Mr. SHAYS. You do not even have to wax eloquently. Is there a question you were really prepared to answer that you want to answer, or is there a question I should have asked?

Mr. CUNNINGHAM. Yes, sir. You asked the question. The question that is sometimes not asked, but is the right one to ask is, what is your biggest problem?

Mr. SHAYS. Do you want me to ask you what is your second biggest problem is?

Mr. Cunningham. Yes, sir.

What is it?

Mr. CUNNINGHAM. It is the Case Control Management System because it becomes the pacing item for everything else that happens in the agency in investigations.

Mr. SHAYS. Thank you. General Welch, is there a question that you would have liked me to ask or something that you want to say?

Mr. WELCH. Well, I am very happy with your questions.

Mr. SHAYS. That makes me very concerned.

If either of you have a closing comment, we can adjourn.

Mr. CUNNINGHAM. Thank you very much.

Mr. WELCH. Thank you.

Mr. SHAYS. Thank you very much. We appreciate you being here. We appreciate your cooperation and we wish you well.

The hearing is closed.

[Whereupon, at 12:25 p.m., the subcommittee was adjourned.]

[The prepared statement of Hon. Helen Chenoweth-Hage follows:]

Statement of Congressman Helen Chenoweth-Hage
Subcommittee on National Security, Veterans Affairs and International Affairs
Committee on Government Reform
2154 Rayburn House Office Building
February 16, 2000

Thank you, Chairman Shays. I appreciate your holding this hearing on "*Defense Security Service Oversight*". I cannot overstate the importance of this issue. I look forward to listening to the witnesses to better understand how to reform the Personnel Security Clearance Program.

After carefully reading the General Accounting Office's (GAO) Report to House Armed Service Committee Ranking Member Congressman Ike Skelton, I was deeply disturbed to learn about the problems associated with the Defense Security Service's Personnel Security Clearance Program.

Perhaps the GAO's report says it best:

> "92 percent of the 530 investigations were deficient in that they did not contain the information in at least 1 of the 9 investigative areas required by the federal standards for granting clearances, which include confirming the subject's residency, birth and citizenship, and employment records; checking records for prior criminal history, divorces, and financial problems; and interviewing character references;
>
> 77 percent of the investigations were deficient in meeting federal standards in two or more areas; and
>
> 16 percent of the investigations identified issues that the Defense Security Service did not pursue pertaining to individuals' prior criminal history, alcohol and drug use, financial difficulties, and other problems that could be cause to deny a security clearance."
>
> (*DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks*, GAO/NSIAD-00-12, October 1999.)

What disturbs me most is the fact that such a high percentage of investigations by the Defense Security Service were found to be deficient in complying with the investigative standards set by the federal government.

The reason that the government conducts Personnel Security Investigations is related directly to the trust that we place in individual citizens. These citizens are often exposed to information that is potentially damaging to the interests of the United States. By researching the background of individual citizens, the United States is able to judge their responsibility and trustworthiness. Without complete background checks, the ability to judge the responsibility and

trustworthiness of these citizens is greatly hindered.

This is why the Defense Security Service is so critical to maintaining the security of sensitive and classified information. I was genuinely disturbed to discover that a backlog of 700,000 reinvestigation cases are still pending.

However, I am greatly relieved to hear that there are a number of ongoing reforms within the Defense Security Service. I look forward to hearing from GAO and DSS on the important subject of the Personnel Security Clearance process and what progress has been made on developing a strategic plan for the Personnel Security Clearance Program.

Thank you, Mr. Chairman.

○