EK 4606-85

Office of Legislative Liaison

Routing Slip

TO:	ACTION	INFO
1. D/OLL		X
2. DD/OLL		X
3. Admin Officer		
4. Liaison		
5. Legislation		X
6		X
7		
8.		
9.		
10.		
	SUSPENSE	Date

STAT

Action Officer:

Remarks:

STAT

22 NOV 85

Name/Date

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:		ACTION	INFO	DATE	INITIAL
1	DCI		X		
2	DDCI		X		
3	EXDIR		X		
4	D/ICS		X		
5	DDI		X		
6	DDA		X		
7	DDO		X		
8	DDS&T		X		
9	Chm/NIC				
10	GC		X		
11	IG				
12	Compt				
13	D/OLL		X		
14	D/PAO				
15	D/PERS				
16	VC/NIC				
17	C/CI/DO		X		
18	C/SECOM		X		
19	D/Security		X		
20	ES		X		
21	NIO/FDIA		X		
22					
	SUSPENSE		Date		

Remarks

The attached material was used in the 20 Nov. SSCI hearing on counterintelligence. (one of a series of 5 such hearings).

STAT

[redacted]

Executive Secretary

21 Nov 85

Date

3637 (10-81)

HOLD FOR RELEASE

THE ATTACHED MATERIAL IS DESIGNED FOR USE IN CONNECTION WITH THE RELEASE OF THE STUDY OF DoD SECURITY.

THIS IS A TOTAL EMBARGO AND THE MATERIAL MUST BE HELD FOR RELEASE UNTIL THE BRIEFER COMPLETES HIS REMARKS AT THE NEWS BRIEFING EXPECTED TO END AT ABOUT 12:30 P.M., THURSDAY, NOVEMBER 21, 1985.

UNTIL RELEASE, NONE OF THIS MATERIAL MAY BE PARAPHRASED, HINTED AT OR ALLUDED TO IN ANY WAY. THIS MATERIAL MAY NOT BE TRANSMITTED BY THE WIRE SERVICES UNTIL THE EMBARGO IS LIFTED. THIS MATERIAL MUST NOT BE DISCUSSED WITH OR PROVIDED TO OTHERS WHO HAVE NOT ACCEPTED THE PACKAGE ON AN EMBARGOED BASIS. IN ADVANCE OF RELEASE, NO TELEPHONE INQUIRIES ON THIS MATERIAL WILL BE ACCEPTED BY DEFENSE DEPARTMENT PERSONNEL.

HOLD FOR RELEASE

Keeping The Nation's Secrets:

A REPORT TO THE
SECRETARY OF DEFENSE
BY THE COMMISSION TO
REVIEW DOD SECURITY
POLICIES AND PRACTICES

Sanitized Copy Approved for Release 2010/02/23 : CIA-RDP87M01152R000200130004-7

COMMISSIONERS

Richard G. Stilwell, General, U. S. Army (Ret), Chairman

Arthur E. Brown, Lieutenant General, U. S. Army, Director of the Army Staff

John L. Butts, Rear Admiral, U. S. Navy, Director of Naval Intelligence

Jerry L. Calhoun, Acting Assistant Secretary of Defense (Force Management and Personnel)*

Chapman B. Cox, Department of Defense General Counsel

William O. Cregar, Director of Security, E. I. duPont deNemours & Co.

Robert W. Helm, Assistant Secretary of Defense (Comptroller)

Fred C. Ikle, Under Secretary of Defense (Policy)

Robert L. J. Long, Admiral, US Navy (Ret)

William E. Odom, Lieutenant General, U. S. Army, Director, National Security Agency

Winston D. Powers, Lieutenant General, U. S. Air Force, Director, Defense Communications Agency

Robert D. Springer, Lieutenant General, U. S. Air Force, Inspector General of the Air Force**

James P. Wade, Assistant Secretary of Defense (Acquisition and Logistics)

James A. Williams, Lieutenant General, U. S. Army, Director, Defense Intelligence Agency

*Lawrence J. Korb, Assistant Secretary of Defense (Force Management and Personnel), served on the Commission until August 31, 1985

**Monroe W. Hatch, Lieutenant General, U. S. Air Force, Inspector General of the Air Force, served on the Commission until July 15, 1985

COMMISSION STAFF

L. Britt Snider, Staff Director*

Richard F. Williams, Assistant Staff Director

Professional Staff Members

David H. Bier, U. S. Navy

Doyal L. Edwards, U. S. Air Force

William M. Hix, Colonel, U. S. Army

George L. Jackson, Captain, U. S. Navy

Harold H. Nicklas, Jr., Colonel, U. S. Army

Administrative Staff

Martha Nadine Smith, Secretary, U. S. Army

Irene D. Larrow, Staff Assistant, U. S. Navy

Noel E. Sills, Staff Sergeant, U. S. Air Force,

Consultant

Charles A. Krohn

*William R. Fedor, Staff Director
(June 26 - September 29, 1985)

TABLE OF CONTENTS

INTRODUCTION

On June 25, 1985, Secretary of Defense Caspar W. Weinberger established the Department of Defense Security Review Commission in the wake of the arrests of three retired and one active duty Navy member on charges of espionage. The Commission was directed to "conduct a review and evaluation of DoD security policies and procedures" and "identify any systemic vulnerabilities or weaknesses in DoD security programs, including an analysis of lessons learned from incidents which have occurred recently, and make recommendations for change, as appropriate."

The Commission began its work by reviewing extant policy, programs, and procedures in the security area. It also reviewed the recommendations of other bodies which have recently urged changes to DoD security policies and procedures, notably the Subcommittee on Permanent Investigations of the Senate Government Affairs Committee, and the DoD Industrial Security Review Committee (the "Harper Committee"). The Commission specifically addressed each of the problems raised by the reports of both bodies where DoD itself had not already taken action on their recommendations. Previous DoD reports in this area were also reviewed and analyzed, as were a number of audit, inspection, and survey reports of various DoD components.

The Commission also solicited recommendations for improvement from DoD components, other departments and agencies in the Executive Branch, congressional staffs, defense contractors, and private citizens and organizations. Testimony before the Commission was presented by 31 witnesses (see Appendix A for identification). In all, more than 1,000 recommendations were received and considered.

The Commission held 17 separate formal sessions commencing on June 26, 1985 and lasting through November 6, 1985. In addition to these formal sessions, Commission members conducted separate interviews with selected corporate officials whose companies held classified defense contracts and received written views from 23 others, in order to obtain greater industry participation. (See Appendicies B and C for identification.) Informal discussions were also held with a number of other individuals who held views on the conduct of DoD's security programs.

The Commission was briefed in detail regarding past and pending espionage prosecutions, and many of the Commission's recommendations are directed at vulnerabilities apparent from the misconduct proved or alleged in these cases. However, inasmuch as the Commission wished to avoid any action that could jeopardize any pending prosecution, this report does not refer to them, or to actions alleged to have been committed by any defendant, as the basis for specific recommendations.

The Commission's report focuses upon the protection of classified information. While fully aware of the importance of protecting unclassified but sensitive information--a monumental "security" problem in its own right--the Commission did not interpret its charter as requiring an analysis in this area. However, it urges more expeditious implementation of the authority given the Secretary of Defense to withhold from public disclosure unclassified technical data which is subject to export controls.

The Commission's recommendations relate primarily to countering the human intelligence threat as contrasted with the threat posed by collection through technical means. Although fully aware of the vulnerability of communications networks and automated information systems to compromise by technical means, the Commission did not assess the current capability to prevent such collections. The Commission took note that inter-agency mechanisms have recently been established at the national level to develop effective technical solutions in this very complex and increasingly important area. For its part, the Commission endorses the need for accelerated research to support this effort.

The report does not address, and, unless specifically stated, does not affect, policies and procedures for the protection of Sensitive Compartmented Information (SCI), which are under the purview of the Director of Central Intelligence (DCI).

The report provides only a general description of DoD security programs because it would require volumes to detail the myriad of policy and procedure in this broad and complex area. However, the report does treat the major policies and procedures and attempts to identify shortcomings and vulnerabilities that are amenable to practical solution. Those solutions are set forth in the report, but without analysis of the competing alternatives that were considered.

This is not to say that other alternatives were not considered; they were. Based upon the evidence before it, the Commission arrived at a unanimous position with respect to those recommendations which would be effective, given the nature of the problem, and those which would be feasible, given existing law, policy, and operational impact.

EXECUTIVE SUMMARY

Each year thousands of classified programs and projects are carried out by the Department of Defense, through its components and its contractual base, in a wide variety of operational and geographical settings. These activities generate millions of items of classified information, ultimately disseminated to almost four million individuals who require such information to perform their assigned tasks. This classified information is not only in the form of documents. An enormous inventory of classified equipment, both end items and components, must be safeguarded; and, increasingly, classified data is being processed, transmitted and stored electronically, posing serious new problems of protection.

Arrayed against this vast and immensely important target are the intelligence services of the Soviet Union, its surrogates and other countries with interests hostile to the United States and its allies. In combination, those services conduct massive and highly organized collection operations to acquire all information, classified and unclassified, of military value. Although a variety of means, both human and technical, are employed, human collection constitutes the more significant threat within the continental United States today.

Protecting a nation's defense secrets from compromise is an age-old challenge. However, the stakes for the United States have never been higher. Given the extraordinary importance of advanced technology to our nation's military capabilities, its loss to a potential adversary--by espionage, theft or other unauthorized disclosure--can be crucial to the military balance. So, too, can compromise of operational plans or battle tactics. Thus to the extent that classified information can be kept from the hands of those who may oppose us, the qualitative edge of United States military forces is preserved and their combat effectiveness assured.

The Department of Defense has countered the threat posed by hostile intelligence services by establishing a comprehensive set of policies and procedures designed to prevent unauthorized persons from gaining access to classified information. Some of these policies implement national directives; others were promulgated by the authority of the Secretary of Defense.

The need to protect classified information is taken as an absolute imperative in principle. In reality, however, policies fashioned to protect classified information are tempered by budgetary constraints, operational necessities and the basic rights of individuals. Moreover, some security practices continue in effect even though demonstrably unproductive.

Policymaking in the security area is centralized, but implementation is properly left to DoD components who provide instructions to thousands of commanders and supervisors around the world. In the final analysis, safeguarding classified information comes down to proper supervision and the individual's responsibility to apply the rules.

GENERAL ASSESSMENT

In general, the DoD security program has been reasonably effective. When considering the potential for compromise, known DoD losses have been relatively few. Some losses, however, have proved gravely damaging. While no system of security can provide foolproof protection, it can make espionage more difficult to undertake and more difficult to accomplish without detection; and it should minimize the compromise of classified information whatever the cause. In these respects, DoD's current program falls short of providing as much assurance as it might.

The reason, in part, is technical. There are insufficient technical means available to securely process, transmit and store classified information in electronic form. But important as this might be, the far greater challenge is people--those who create and handle classified information, those who disseminate it, and those who oversee its protection. While the overwhelming majority carry out such functions responsibly, there are some who fail to do so. And the current security system falls short in limiting the opportunities for errors of omission or commission; in providing the means to identify those who transgress; and in dealing appropriately with the transgressors.

This, then, was the focus of the Commission's inquiry: how can the DoD security system be improved to ensure that only trustworthy persons are permitted within it; that they abide by the rules; that those who choose to violate the rules are detected; and those who are detected are dealt with justly but firmly.

KEY FINDINGS AND RECOMMENDATIONS:

The report contains numerous recommendations to improve the security of classified information within DoD. Highlighted below are the Commission's key findings and summaries of major recommendations.

FINDING: Requests for security clearance must be reduced and controlled. DoD components and contractors request security clearances for many individuals who do not need continuing access to classified information. Unjustifiable requests overburden the investigative process and pose an unneeded security vulnerability. Although some reductions have already been achieved, better means of control are essential.

RECOMMENDATIONS:

-- Create a TOP SECRET billet control system, similar to that in use for Sensitive Compartmented Information (SCI) access, to ensure that TOP SECRET clearances go with a position, rather than an individual.

-- Require contractors to provide specific justification for requests for security clearances; and prohibit requests solely for movement within a controlled area whenever exposure to classified information can be prevented.

-- Authorize, subject to strict control, one-time, short-duration access to specific information at the next higher level of classification to meet operational exigencies.

FINDING: The quality and frequency of background investigations must be improved. The investigative basis for award of a SECRET clearance is a personal history statement and a National Agency Check which provides extremely limited knowledge of the subject. DoD conducts background investigations for TOP SECRET clearances. It conducts five-year reinvestigations only for TOP SECRET clearances and SCI accesses, and is far behind schedule in meeting this requirement.

RECOMMENDATIONS:

-- Expansion of the investigative scope for a SECRET clearance to include a credit check of the subject and written inquiries to past and present employer(s).

-- Intensification of behavioral science research to the end of improving the background investigative process and the effectiveness of subject interviews.

-- Reduction of the backlog of reinvestigations for TOP SECRET and SCI accesses to manageable levels within four years and development of a plan for accomplishing periodic reinvestigations of all persons holding SECRET clearances and above by 1995.

FINDING: The Department's most sensitive information must be accorded higher priority in attention and resources. Although the counterintelligence-scope polygraph examination is the one investigative tool which might have prevented -- or earlier detected -- recent acts of espionage, its use in the Department is severely restricted, in time and scope, by the Congress. There are no special eligibility criteria for personnel handling cryptographic materials despite their transcendent importance to an adversary. Only those individuals who have access to nuclear weapons are currently monitored formally for trustworthiness and stability. By definition, Special Access Programs are established to provide extraordinary security protection; in fact, some do not.

RECOMMENDATIONS:

-- Request the Congress to supplant the year-by-year approach to the conduct of counterintelligence-scope polygraph examinations by giving authority for the Secretary to develop a coherent and gradually expanding program, with stringent quality controls and subject to Congressional oversight.

-- Institute a "crypto-access" program for all persons who have continuing access to cryptographic information in large quantities or with highly sensitive applications.

-- Direct appropriate DoD components to institute a reliability program (modeled on, but less structured than, the DoD Personnel Reliability Program) for military and civilian personnel involved in especially sensitive programs or assigned to TOP SECRET positions of high criticality.

-- Direct a review and revalidation of Special Access Programs, promulgation of uniform minimum security standards and the regularization of inspection and oversight of such programs.

FINDING: The adjudication process in which security clearance determinations are rendered must be improved. There is reason for concern about the efficacy of the adjudication process. The denial rate is low throughout DoD but nonetheless varies widely among the military departments and defense industry. Although adjudication is the final step in determining eligibility for access to classified information, such decisions are made on the basis of vague criteria, and many adjudicators are inadequately trained. As a result, it is possible to reach different adjudicative determinations in applying the same guidelines to a given set of investigative findings.

RECOMMENDATIONS:

-- Necessary research and other actions be undertaken to develop more precise and effective adjudicative standards.

-- Development and conduct of standardized mandatory training for all adjudicators.

FINDING: Classified information must be better controlled. There are no uniform controls over SECRET information, or any requirement, apart from records disposition schedules, for unneeded classified documents to be periodically destroyed. There is no overall policy governing access to areas containing sensitive information or search of persons entering or leaving DoD installations.

RECOMMENDATIONS:

-- Institute a uniform degree of accountability for SECRET documents within DoD.

-- Prohibit the retention of classified documents which are not "permanently valuable records of the government" more than five years from the date of origin, unless specifically authorized in accordance with record disposition schedules established by the component head.

-- Establish a general policy, subject to waivers prescribed by component heads, that employees not be permitted to work alone in areas where TOP SECRET or Special Access Program materials are in use or stored.

-- Establish a policy that all briefcases and similar personal belongings are subject to search upon entry and exit from DoD installations to determine if classified information is being removed without authority.

FINDING: Futher initiatives are needed to counter the effectiveness of hostile intelligence activities directed at DoD. Although recent congressional and Executive Branch actions are important, more should be done to limit the size of the hostile intelligence presence within the United States and to constrain its freedom of action. Counterintelligence capabilities should be strengthened and greater efforts made to detect contacts with hostile intelligence services. Security awareness activities need to be substantially increased and their quality improved.

RECOMMENDATIONS:

-- Urge expansion of the national policy of parity in numbers in the diplomatic establishments of the United States and Soviet Union, to include parity in treatment and privileges; extension of this concept to all nations which present a hostile intelligence threat to the United States; and imposition of travel restrictions on non-Soviet Warsaw Pact diplomats accredited to the United Nations.

-- In coordination with the DCI, ensure increased funding for counterintelligence analysis.

-- Require all cleared personnel to report foreign travel as well as contacts with foreign representatives who request defense information.

-- Direct DIS, in conjunction with the FBI and military departments, to undertake immediate efforts to increase the size, effectiveness, and coordination of the security awareness program in industry.

FINDING: The professionalism of security personnel must be enhanced. DoD does not prescribe minimal levels of training for security personnel. In general, training is narrow in scope and coverage, is not mandatory and does not lead to official certification. Some individuals performing security duties do not adequately understand overall security concepts.

RECOMMENDATION:

-- Establish training standards, direct development of basic courses of instruction for the several security disciplines and prescribe requirements for certification.

FINDING: Substantially increased basic research is needed to guide security policy and practice. The Commission's work was hampered by the lack of firm data and meaningful analysis in several aspects of the security equation. There is minimal ongoing research although the potential dividends from a purposeful effort into a wide range of security-related matters are high.

RECOMMENDATIONS:

-- Direct expansion of the Defense Security Institute and task it, inter alia, with overall coordination of significantly increased research and development in essential security-related areas, notably including the personnel investigative process and physical security technology.

-- Provide increased funding of the National Computer Security Center's research and development program.

FINDING: More effective action should be taken against those who violate security rules. While sanctions available to remedy security violations by uniformed military personnel appear adequate, remedies with respect to civilians and contractors are not. Moreover, those remedies which are available could be better utilized.

RECOMMENDATIONS:

-- Continue to advocate enactment of legislation to enhance criminal enforcement remedies against civilian employees and contractors who disclose classified information without authority.

-- Utilize existing legal remedies to withhold payments under DoD contracts to obtain contractor compliance with DoD security requirements.

-- Revoke the DoD facility clearance of contractors who display management indifference to security through repeated security violations or in other ways, even though security deficiencies are remedied.

FINDING: DoD's security posture is critically dependent upon the actions of commanders and supervisors at all levels. Security is everybody's business and, most notably, that of the individual in charge. As with all other responsibilities vested in them, it is incumbent upon commanders and supervisors to underscore the importance of the security function by personal example, by setting forth the rules, by inspecting for compliance and by disciplining those who fall short. Throughout DoD, discharge of this responsibility is uneven. Insufficient attention has been given to the overall purpose of security as it relates to organizational mission, to observation of subordinates' security performance and insuring that basic security principles are adhered to in practice. The key to genuine improvement in DoD's security posture is continuing, pervasive oversight by commanders and supervisors at all levels.

(Relatedly, the Secretary of Defense has already approved an earlier Commission recommendation that supervisors and commanders personally review the performance of their subordinates from a security standpoint as part of recurring performance appraisals and fitness reports.)

RECOMMENDATIONS:

-- Direct all DoD components which handle and store classified information to institute a one-time "top-to-bottom" command inspection at every level of their organizations within six months, to determine compliance with applicable security policies. Recurring inspections performed thereafter should also include examination of compliance with these security requirements.

-- Instruct commanders/supervisors to utilize all appropriate enforcement remedies against security violators.

RESOURCE IMPACT

While the resource impact of its recommendations cannot be determined with precision, the Commission estimates that the cost of implementing them would be relatively modest. If these recommendations are approved, DoD components should be directed to begin accommodating these increased outlays within the normal program/budgeting process.

CONCULUSION

The Commission believes that increased priority must be accorded DoD security efforts to provide reasonable assurance that the nation's secrets are protected. More resources should be allocated to security, even at the expense of other DoD programs. New safeguards must be established and old ones improved, even at some cost to operational efficiency and convenience. This is not to say that some resources cannot be saved, or operational efficiency improved, by eliminating burdensome and unproductive security requirements. Indeed, a number of such changes are recommended. But on the whole, DoD must be willing to pay the price to protect its secrets.

The Commission arrives at this conclusion mindful that security plays a supporting role in the successful accomplishment of DoD's mission. But the success of any classified project or operation will be short-lived at best if, at the same time, the results have been revealed to potential adversaries, who are then enabled to develop countermeasures at a more rapid pace than otherwise. As bureaucratic and mundane as security requirements sometimes appear, they offer the only systematic means available to protect and preserve the defense community's triumphs and advances, over time. Security must be given its fair share of serious attention and its fair share of resources.

OVERVIEW

THE TARGET

The Department of Defense, together with its contractual base, constitutes a target of immense size and importance to the intelligence services of nations with interests inimical to the United States and its Allies. Given the major role of our Armed Forces as an instrument of U.S. foreign policy, DoD is involved in virtually every national security decision; and the myriad classified plans, programs, and actions that derive from those decisions reflect U.S. intentions and capabilities in peace, crises and war. With few exceptions, our fielded weapon systems are the world's most effective; and our laboratories and test facilities have the requisite lead in most militarily-relevant areas of research and applied technology, assuring the qualitative advantage of future weapon systems. A huge intelligence organization supports all these activities.

It follows that most elements of the Department must deal with classified information. Thousands of classified programs and projects are carried out annually throughout the large and complex structures of the three Military Departments, the Office of the Secretary of Defense, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies. The geographic distribution of classified information is also extensive. DoD maintains an official presence--some very large, as in Western Europe and Korea--in 95 countries. Additionally, vast quantities of classified documents, technical data, and equipments are released to Allied and friendly governments and to international organizations under bilateral and multilateral arrangements.

The volume of classified material produced, received, transmitted, and stored within DoD is staggering. DoD reported that some 16 million documents were classified in 1984. The number of classified documents actually maintained in DoD filing systems and those of its contractors is unknown; however, an estimate of 100 million is not unrealistic.

But size alone does not begin to convey the dimensions of the task of protecting classified information. DoD, for example, maintains enormous inventories of classified end items and components, which require different protection than documents. Similarly, the DoD is moving at a bewildering rate from controlling "hard-copy" documents to controlling classified information electronically stored and transmitted by automated data processing systems. Within DoD, there are an estimated 16,000 computers, most of which process information of value to an adversary, and many of which are internetted. And not only government facilities are involved--classified work is presently progressing at over 13,000 cleared defense industrial firms.

Not surprisingly, 90 percent of the personnel in the Executive Branch who hold security clearances are in DoD. 2.6 million uniformed and civilian personnel have some form of clearance (after the 10 percent reduction mandated in June 1985 by the Secretary of Defense). These are augmented by 1.2 million cleared industrial employees. (DoD, incidentially, administers industrial security not only for itself but for 18 other Executive departments and agencies). A substantial number of these cleared personnel--military, civilian and contractor -- are located outside the continental United States.

In short, the challenge of protecting United States defense secrets is of almost immeasurable scope.

THE THREAT

The Soviet Union, its Warsaw Pact and Cuban surrogates, and other countries with interests adverse to the United States, have conducted and will continue to conduct massive and highly organized intelligence gathering operations against DoD personnel, installations, and contractors. Such operations utilize both human and technical collectors targeted against classified and unclassified information of military value.

Unclassified information available to the public is systematically exploited by the intelligence services of these countries, and, by authoritative accounts, comprises the bulk of information being collected. Unclassified information which is not available to the public generally, but which is militarily significant, is also sought through a wide variety of sources. For example, information which is transmitted electronically through the air can be presumed to be within the reach of hostile intelligence. Similarly, it can be presumed that hostile intelligence will exploit every chance to acquire information of military value through industrial sources; through attendance at scientific and technical conferences; or through purchase, direct, or via intermediaries.

Classified military information presents a more lucrative, if more difficult, target. Since such information is not, in theory, made public or transmitted over means which permit exploitation, the avenue to it is usually through persons who have, or may attempt to gain, authorized access. Indeed, there are hundreds of contacts with suspected intelligence agents reported by DoD personnel and contractors every year, evidence of an active and continuing effort at recruitment. Unfortunately, there are numerous examples where DoD employees and contractors have volunteered their services, offering to sell classified information to which they have access. While evidence suggests that such disaffections are rare when compared to the size of the defense community, one person with sufficient access to classified information may be in a position to do incalculable harm to the national security, to include jeopardizing the lives of Americans.

It also merits underscoring that the same level of damage to the national security can be caused by persons who are not in the employ of a foreign power. The transmittal of classified information to unauthorized persons -- whether by indiscretion or wittingly -- places it beyond government controls. One must therefore assume that it may ultimately appear in the data bank of a hostile intelligence service.

None of this is new; indeed, espionage is as old as the relationships between nations, and unauthorized disclosures of defense secrets have plagued governments for centuries. The stakes today, however, are much higher than ever before. Given the extraordinary importance of sophisticated technology to our nation's military capabilities, its loss to a potential adversary--by espionage, theft or unauthorized disclosure--can have a substantial and long-term bearing upon the military balance of power. Similarly, the loss of operational plans or tactics can provide an adversary with precisely the edge needed to defeat United States forces in combat. To the extent, therefore, that classified information can be kept from the hands of those who may oppose us, the effectiveness of United States military forces is preserved and extended for longer periods at lower costs to the defense effort.

THE DOD RESPONSE: IN RETROSPECT

Responding to the hostile intelligence threat over the years, DoD has established for its components and contractors a comprehensive set of policies and procedures to prevent access to classified information by unauthorized persons. Some of these policies and procedures implement law and national policy; many DoD promulgates on its own authority. In either case, however, DoD typically has determined how classified information will be protected against specific vulnerabilities by adjusting policy and procedure to the resources available, or which can reasonably be obtained, and to the probable impact of such policies and procedures on mission accomplishment. Thus, even though the protection of classified information is, in general, taken as an absolute imperative, how this is accomplished often gives way to practical considerations of budget constraints and operational necessity. Moreover, even after policies and procedures are agreed to, these same considerations affect the level of implementation. Policies and procedures which are not adequately funded fall short of their objective; those which are perceived as interfering unduly with mission accomplishment are often not enforced.

Inadequately implemented policy and procedure do not constitute the entire problem. Some policy and procedure continue to be implemented after they have proved to be ineffective, and, on balance, a waste of resources. Elimination or adjustment of long-time practice, despite demonstrated reason therefor has proven difficult for security policymakers.

While policymaking is centralized at OSD level, implementation is properly left to DoD components who provide instructions to thousands of commanders and supervisors at installations and facilities around the world in a variety of operational settings. Posters in the Pentagon proclaim that "Security is everyone's business," and certainly, in the final analysis, protecting classified information comes down to the responsibility of individual employees to apply the rules and proper supervision.

Despite the complexity of policy and procedure, and the vast population of cleared personnel governed by it, the DoD security program must be regarded as reasonably effective. Considering the potential for compromise, known DoD losses have been, on the whole, relatively few. Some of these, however, have proved gravely damaging. Clearly there is room for improvement. Many people are cleared who do not need access to classified information. Background investigations yield relatively little derogatory information on those being cleared, and under the existing adjudication process, far fewer still are actually denied a clearance. Once cleared, very little reevaluation or reinvestigation actually occurs, and relatively few indications of security problems are surfaced. The principle that a cleared individual is authorized access only to that information he "needs-to-know" is not well enforced. For those contemplating espionage or intent on compromise of classified information for other reasons, the system does not provide s ufficient deterrence. Moreover, the volume of classified information created and stored within DoD, and the less-than-stringent manner in which it is sometimes handled internally, often present opportunities to the would-be culprit that should not otherwise arise. Security regulations are often violated but only serious cases are typically made a matter of report; few of those are investigated, even where a pattern of such conduct is in evidence; and fewer still result in punishment.

PART ONE: POLICY AND PROCEDURES

I. Gaining and Maintaining Access to Classified Information

Persons may gain access to classified information needed to perform official duties after receiving a security clearance. Requests for clearance originate with and are validated by the organization to which the individual is assigned or the defense contractor with which employed. They are submitted together with a personal history statement filled out by the subject, to the Defense Investigative Service (DIS), which carries out appropriate background checks, based upon the level of clearance requested. Normally only TOP SECRET clearances require field investigation; SECRET and CONFIDENTIAL clearances generally require only a check of the records of relevant government agencies. The results of these investigations are returned, in the case of DoD personnel, to the requesting component and, in the case of defense contractors, to the Defense Industrial Security Clearance Office in Columbus, Ohio, for final processing. A decision to award a security clearance takes into account all the factors involved in a particular case, and is made on the basis of an overall, common sense determination that access by the individual concerned is "clearly consistent with the national security", the standard for civilian employees set forth in Executive Order 10450 or, in the case of industrial employees, Executive Order 10865. Once a clearance has been awarded, it remains valid until the requirement for access to classified information is terminated. However, receipt of adverse information regarding an individual may lead to a "readjudication" of his or her clearance. Those who have TOP SECRET clearances or SCI access are required to be reinvestigated every five years although, due to lack of sufficient resources being allocated, DoD lags far behind in meeting the TOP SECRET requirement.

The Commission notes that virtually all of the extant federal policy with respect to gaining and maintaining access to classified information, including the revision of Executive Order 10450, is under review by an interagency working group, chartered under National Security Decision Directive 84, and chaired by the Department of Justice. Unfortunately, this project has been delayed for many months awaiting Administration approval of the working group's proposed course of action. The Commission urges the Secretary to continue to press for National Security Council approval of this interagency group's terms of reference for revamping federal policy in this crucial area.

The following discussion breaks down the process set forth above into component parts, permitting a more focused discussion of the Commission's recommendations with respect to each part.

A. Requests for Security Clearances

There is no effective mechanism in place for adequately screening requests for security clearances to ensure that nominees for a security clearance actually need access to classified information. Components and contractors frequently request security clearances to provide additional assurance regarding the trustworthiness of their employees, even if they have no need for access to classified information. In many cases, persons are nominated for clearances because they were previously cleared and want to maintain such status. There is also a common practice of clearing those who may physically require access to a controlled area, regardless of whether such persons need access to classified information. Similarly, clearances are sometimes requested to avoid the requirement to escort uncleared persons in a classified area, even where such persons need not be exposed to classified information. Further, many contractors nominate employees for security clearances to establish and maintain a "stockpile" of cleared employees to be in a better competitive position to obtain classified work.

These practices are very damaging in two respects. Where TOP SECRET clearances are concerned--which require substantial field investigation and reinvestigations--unjustified requests delay the clearance and reinvestigation of those who legitimately--and sometimes urgently--need access. Such delays necessarily result in lost time in a productive capacity both in DoD components and in industry. Moreover, overburdening field investigators erodes the quality of investigations.

The recent action of the Secretary of Defense to direct an across-the-board 10 percent reduction in the number of existing clearances, and, concomitantly, his instruction to reduce by 10 percent the number of new clearance requests to be made in fiscal year 1986, should provide an immediate, if temporary, control of the process. More permanent means of control are essential and feasible.

The first is to adopt a system of billet control for TOP SECRET similar to that in effect for SCI accesses. Each component would identify those positions within its respective organization which required a TOP SECRET clearance. These would then be validated and maintained by appropriate authority. Only persons coming into such validated positions would be eligible for a TOP SECRET clearance. When they left such positions, the clearance would lapse. Provisions would be made to adjust the number of authorized positions based upon new classified functions or contracts, as validated by appropriate authority.

The second is to remove from the security clearance process those individuals who require access to classified facilities but not to classified information; and to institute other procedures to assess their reliability.

The third is to reaffirm the policy that the continuing need for access to classified information is the condition precedent for requesting a security clearance while, concurrently, authorizing responsible officials to grant one-time access to the next higher level of classification to meet unforeseen contingencies.

RECOMMENDATIONS:

1. Establish a billet control system for TOP SECRET clearances both in DoD components and in industry.

2. Prohibit the practice of requesting security clearances solely to (i) permit access to a controlled area but where there is no exposure to classified information involved or (ii) to permit ease of movement within classified areas, where the individual involved has no need for access to classified information and access realistically can be denied. However, allow heads of DoD components to request appropriate investigations for determining reliability of individuals separate and distinct from the issuance of a security clearance.

3. Require contractors to justify requests for security clearances by specifying the reasons(s) why the clearance is needed, (e.g., contract number, RFP number, or other) rather than simply asserting such a need. Also, require contractors to rejustify every two years the security clearance of any employee who remains in an overseas assignment. Clearances which are not rejustified should expire.

4. Modify the process whereby contractors obtain security clearances in order to bid on classified defense contracts by:

a. Permitting firms which have held facility clearances within the past two years to be expeditiously reinstated provided they are still eligible;

b. Permitting contractor employees who have held security clearances within the past five years to be reinstated administratively provided they have remained in the employ of their company, and no derogatory information concerning such employee is known to the company. However, in the case of a TOP SECRET clearance, a reinvestigation should be required if the last investigation of such individual is more than five years old.

c. Prescribe that contractors' "stockpiling" of clearances for contingency purposes will henceforth constitute a major security deficiency when identified by DIS inspectors.

5. Authorize one-time, short duration access by cleared personnel to the next higher level of classified information necessary to meet operational or contractual exigencies. Within DoD components, such determinations must be at a level not lower than that of flag officer, general courts martial convening authority, or Senior Executive Service. Within industry, such determinations must be

approved by the DoD contracting office, and reported to the DIS regional office with security responsiblity for the contractor concerned. Each such determination shall be recorded and maintained: within DoD by the approval authority; for industry by the cognizant DIS regional office.

B. Eligibility for Security Clearances

Current DoD policy permits immigrant aliens (i.e., foreign nationals admitted into the United States for permanent residence) to receive SECRET security clearances based upon DoD's need to utilize the special expertise possessed by that individual, provided DoD has the ability to establish investigative coverage for the previous 10 years. Currently, native-born and naturalized United States citizens may be cleared at any level; no distinction is made based upon country of origin and no additional residence requirement exists for naturalized citizens (who typically must have maintained residence in the United States for a minimum of five years as a condition of naturalization). Dual citizens are treated as United States citizens. Foreign nationals who are employed by DoD do not receive security clearances, per se, but, with high-level approval, may receive a "Limited Access Authorization", which entitles them to access up to SECRET level information for a specific purpose.

Although there are relatively few cases where these policies are known to have led to penetrations of DoD by hostile agents, they undoubtedly increase that risk. Policies can be tightened without jeopardizing DoD's use of such individuals, with due regard for their rights as recognized under United States law.

RECOMMENDATIONS:

6. Establish policies that provide:

a. Only United States citizens are eligible for standard security clearances and that immigrant aliens and foreign nationals employed by the DoD are eligible only for "Limited Access Authorizations" not exceeding the level of classified information which may be released to the country of current citizenship. Such authorizations shall ordinarily be approved only where 10 years of investigative coverage is feasible; and, where SECRET information is at issue, the subject agrees to a counterintelligence-scope polygraph examination.

b. Recently naturalized United States citizens, whose country of origin is determined by appropriate authority to have interests adverse to the United States, or who choose to retain their previous citizenship, shall ordinarily be eligible for a security clearance only after a five-year period of residence within the United States after becoming a citizen; otherwise, a minimum of 10 years of investigative coverage must be possible.

c. Exceptions to these requirements shall be permitted for compelling national security reasons.

C. Initial Investigations

Largely due to requirements originating from the DCI (for SCI access) and the Office of Personnel Management (OPM) (for civilian employees of DoD), DIS conducts three different types of background investigation for TOP SECRET clearance. A SECRET clearance is granted on the basis of only a National Agency Check (NAC); a CONFIDENTIAL clearance is similarly based upon a NAC.

Unless the existence of potentially derogatory information is indicated by the subject on his personal history statement, the sum total of investigation performed by DIS for a SECRET clearance consists of a check of FBI criminal records and a check of the Defense Central Index of Investigations, which would indicate any previous investigations by DoD elements. Thus, unless the subject himself suggested the existence of possible derogatory information, the NAC would likely turn up only evidence of criminal involvement with the federal system. Although the Department has long recognized the inadequacy of a NAC, particularly when most classified information is at the SECRET level, the numbers of such clearances in existence--over three million--and the numbers granted each year--over 900,000--are so huge that adding field investigations of any significant scope could require as much as a quadrupling of DIS investigative resources. Thus, expansion of the investigations required for SECRET clearances have been heretofore regarded as infeasible.

On the average, the background investigation for TOP SECRET currently takes 90 days. A NAC, required for a SECRET clearance, presently averages 60 days. If the case turns up derogatory information that must be further developed, or if it involves investigative leads abroad or that are otherwise difficult to accomplish, the processing time may be considerably extended. Individuals who are awaiting completion of their security checks may not have access to classified information. Interim clearances may be awarded, however, based upon case-by-case justification, allowing interim access to TOP SECRET information based upon the submission of a "clean" personal history statement and a NAC, and interim access to SECRET based upon submission of a personal history statement, without having to await completion of the field investigation. If derogatory information should turn up in the course of the field investigation, the interim clearance is immediately withdrawn pending resolution of the case. Although precise figures are not available, it is clear that the costs to DoD, in terms of lost production capability that result from employees and contractors awaiting for background investigations to be completed, are substantial.

Given the relatively small number of cases in which derogatory information is developed by the initial investigation where the personal history statement indicates no adverse information, the Commission believes the Department would incur small risk in providing interim access to information classified at the SECRET level for a period of several weeks, based upon the submission of a "clean" personal history statement. Adoption of this procedure DoD-wide would enable both DoD components and contractors to utilize their employees in cleared positions at a much earlier stage, avoiding considerable costs in terms of lost productivity.

Normally, DIS investigators doing background investigations receive excellent cooperation both from official and private sources of information. There has been a long-standing problem, however, with several state and local jurisdictions that refuse to provide DIS with certain criminal history information concerning the subjects of background investigations. Frequently these problems arise from state or local law, or the interpretations of such law made by local authorities, precluding the release of criminal history data which did not result in convictions, or precluding release for other than law enforcement purposes, even though the subject himself has consented to the release of such data. Where this problem exists, DoD is forced to determine the clearance without benefit of potentially significant criminal history data.

The Intelligence Authorization bill for FY 1986, as reported from the conference committee, contained a provision which provides DoD, OPM, and CIA investigators access to state and local criminal history records notwithstanding state or local laws to the contrary. If enacted, this measure should provide DoD with the legal authority needed to access such data.

RECOMMENDATIONS:

7. Obtain the consent of the DCI and OPM for a single-scope background investigation for both TOP SECRET and SCI access, to ensure the same type of investigation is done on all categories of DoD personnel, including contractors, who have access to TOP SECRET information. Until the NSC prescribes a different scope applicable to the entire Executive Branch, such investigations should cover a time frame and be composed of only those elements which have been demonstrated to be effective in determining the bona fides of the subject or produce significant derogatory information.

8. Immediately expand the investigatory requirements for SECRET clearance to include a NAC, credit check, and written inquiries to present and past employers. Assess the desirability and feasibility of requiring the subjects of investigations for SECRET clearances to themselves provide greater evidence of their identity and bona fides as part of the pre-investigative process.

9. Apply the procedures now used for granting interim SECRET clearances based upon a case-by-case justification to the processing of all such clearances.

10. Press efforts to obtain statutory authority to obtain criminal history data from state and local jurisdictions, as proposed in the pending Intelligence Authorization bill for FY 86. With such authority, DIS should resolve any problems it may have obtaining access to relevant criminal history data with the state and local jurisdications concerned.

D. Adjudication

The results of background investigations requested by DoD components are returned to central adjudication points* within each DoD component for processing in accordance with DoD Regulation 5200.2-R, the basic DoD personnel security regulation. The investigative reports on contractor employees which contain significant derogatory information are sent to the Defense Industrial Security Clearance Review (DISCR) Office where they are adjudicated in accordance with DoD Directive 5220.6. Both DoD Regulation 5200.2-R and DOD Directive 5200.6 contain adjudicative guidelines for those charged with making clearance determinations. The adjudicative criteria in DoD Directive 5200.6 have recently been revised to mirror those in DoD Regulation 5200.2-R, with the exception of the criteria relating to criminal misconduct. Under the industrial criteria, a person who is convicted of a felony, or admits to conduct which would constitute a felony under state or local law, cannot be granted a security clearance unless a waiver is approved by the Under Secretary of Defense for Policy for compelling national security reasons. Under the guidelines applying to military and civilian personnel, such conduct is considered a factor, but not in itself determinant of the clearance decision.

Experience has demonstrated that the adjudication criteria in both regulations are stated so generally that it is possible for different adjudicators to arrive at different determinations after applying the same guidelines to a given set of investigative results.

DoD requires no formal training for persons performing adjudicative functions. Indeed, no such training is conducted beyond an occasional seminar. The application of adjudication guidelines thus becomes largely a matter of on-the-job training. Moreover, the grade levels of adjudicators appear uniformly low, considering the degree of judgment and skill required. (See discussions on "Training" and "Career Development" below.)

---

* The Navy, which has had a decentralized adjudication system for military personnel, is in the process of centralizing that activity.

All of these factors tend to produce inconsistent, uneven results in terms of adjudications. While no precise analysis of the extent of this problem was available to the Commission, there is little confidence that the adjudication process in many DoD components guarantees the same results based upon a given set of investigative findings. The imprecision of adjudicative standards partially explains why relatively few clearances are denied on the basis of the initial investigation. In the absence of definite standards, adjudicators, using their own "overall common sense" yardstick, may be inclined to conclude that access by the subject is "not clearly inconsistent" with the national security, regardless of the investigative findings involved. In fact, with respect to DoD components, only 2.5 percent of the initial clearance determinations resulted in denials in 1984. With respect to contractors, only 0.2 percent of the cases resulted in denials.

Clearly, there is a pressing need to improve the adjudication process, the ultimate step in determining an individual's trustworthiness for access to classified information. The key requirement is the enunciation of more precise criteria and, particularly, better definition of behavior which is per se not consistent with the national security. This is a fertile area for research, as there is scant empirical data available on which to base sound standards. One approach to this task might be to analyze the "Statements of Reasons" issued by the Defense Industrial Security Clearance Review Office to justify the denials of industrial clearances. Such an analysis should begin to produce more concrete, better defined criteria for denials, which have also been subjected to legal review.

RECOMMENDATIONS:

11. Revise the criteria which govern the adjudication of security clearances to provide far more specificity than is currently the case, to the end of more uniform and consistent security clearance determinations. (See also Recommendation 59, under "Training", and Recommendation 58, under "Research", below.)

12. Consolidate the adjudication functions for civilian employees of the Office of the Secretary of Defense, and all defense agencies except the Defense Intelligence Agency and the National Security Agency, who are cleared at the collateral level, under the Director, Washington Headquarters Services (WHS). Enforce the current requirement that the Military Departments are responsible for the adjudication of the clearances for military personnel assigned to other elements of DoD.

E. Periodic Reinvestigations

Recent espionage cases have involved persons with security clearances who were recruited by or offered their services to hostile intelligence services. The Department has an obvious need to ensure that persons who are being initially

cleared have not been recruited and are not vulnerable to recruitment by hostile intelligence. As a practical matter, however, the greater and more probable threat to DoD security is the individual who is recruited after he has been cleared. Nevertheless, DoD has devoted relatively small investigative resources to reinvestigations.

Since 1983*, the Department has required reinvestigations at five-year intervals of persons holding TOP SECRET clearances and SCI accesses. These are comprehensive investigations, but have so far resulted in very few terminations. Moreover, DIS is far behind schedule in completing these reinvestigations.

Since 1983, DIS has conducted roughly 27,000 such investigations a year. But given there are approximately 700,000 persons in the affected categories, it would be impossible to eliminate the backlog if the same level of effort continues. Fortunately, the Congress has approved an additional 25 million dollars for DIS in Fiscal Year 1986 to be applied to the existing backlog of periodic reinvestigations. If this level of effort remains constant, DIS expects to be back on schedule in five years.

No periodic reinvestigations are required for SECRET or CONFIDENTIAL clearances, and, given the volume of such clearances now in existence (3.3 million SECRET, and 400,000 CONFIDENTIAL), an across-the-board requirement to conduct reinvestigations for SECRET clearances will not be feasible without a substantial increase in DIS investigative resources. However, it should be feasible to conduct some reinvestigations in the SECRET category where the subject has access to information of unusual sensitivity.

RECOMMENDATIONS:

13. Accord periodic reinvestigations significantly increased priority:

a. Mandate that the backlog of reinvestigations due on persons holding TOP SECRET clearances and SCI access be reduced to manageable levels within four years.

b. In the interim, authorize the heads of DoD components to request periodic reinvestigations on a case-by-case basis of persons holding SECRET clearances who, nonetheless, are exposed to very sensitive information.

c. Establish a goal of conducting periodic reinvestigations of all persons holding SECRET clearances and above by 1995.

---

*DoD had in the past conducted periodic reinvestigations of very limited scope for SCI access. In 1981, a moratorium was placed on these investigations in order to deal with the enormous backlog of requests for initial investigation.

F. Use of the Polygraph as a Condition of Continuing Access

Polygraph examinations have been used in DoD for many years for a variety of purposes. Prior to 1985, however, the polygraph was not used within DoD as a condition of continuing access to classified information except at the NSA, and, since 1981, in a sensitive Air Force project.

While there were no legal restrictions on DoD use of the polygraph for this specific purpose before 1984, and it had been required for applicants for employment at both CIA and NSA for many years, DoD had refrained from using a broad lifestyle polygraph examination to supplement its personnel security program largely out of concern for the privacy of, and fairness to, employees already on the rolls. In 1982, however, the Department proposed a modest expansion of the use of polygraph examinations, limited to questions of a counterintelligence (rather than personal) nature, and set forth a variety of procedural safeguards to ensure that its employees were treated equitably and with a minimum of personal intrusion. The objective was to authorize DoD components to use such examinations, under the ground rules established, as a condition of access to specially designated programs of high sensitivity.

This proposal, although endorsed by DoD components, was not implemented at the time because of Congressional concerns regarding expanded use of the polygraph. After a number of hearings and consultations, however, the Department reached general agreement with the relevant Congressional committees for a test of this concept in fiscal year 1985, limited to 3,500 counterintelligence-scope examinations. Authority to conduct such a test was included in the FY 1985 Defense Authorization Act.

Although the initial test had not been completed, the Armed Services Committees agreed, in conference action on the FY 1986 Defense Authorization Bill, to extend the test program at the same 3,500-examination level for FY 1986 and increase it to 7,000 for FY 1987.

Based upon this action, DoD has directed the Army to serve as Executive Agent for polygraph training, and expand its training facility to accommodate 108 students annually, the increased output estimated to be required to carry out the 7,000 examinations authorized in FY 1987. DoD components were encouraged to analyze their requirements and ensure they are satisfied.

While these actions are going forward, it is clear that the limited, year-to-year authorization, apparently favored by the Armed Services Committees, is impeding the planning and successful execution of the expansion of the DoD training facility, and, accordingly, the program as a whole. It is simply not feasible feasible to concert long-term arrangements and attract highcaliber personnel to commit to them, based upon an uncertain, year-to-year authority.

The Commission is convinced that the counter-intelligence-scope polygraph is the primary technique currently available to the Department which offers any realistic promise of detecting penetrations of its classified programs by hostile intelligence services. Moreover, even the possibility of having to take such examinations will provide a powerful deterrent to those who might otherwise consider espionage. Accordingly, the Commission urges that a substantial, albeit gradual, expansion of the Department's program should be undertaken.

Obviously, because of the very limited capability DoD now possesses to conduct polygraph examinations, its limited ability to train new examiners in the near-term, and its determination to maintain the stringent quality controls that characterize this program, DoD will be constrained to relatively small numbers of examinations for some time to come. It makes sense, therefore, to utilize them on a systematic basis only for specially-designated TOP SECRET and Special Access Programs as the Congress has approved. It would also be desirable, however, for persons cleared at the SECRET and TOP SECRET levels to face the possibility of a randomly administered polygraph examination at some time during their respective careers. Similarly, there may be programs classified at the SECRET level which themselves are of peculiar sensitivity to justify requiring such examinations of all participants. Under the formulation contained in the FY 1986 Defense Authorization Act, a limited polygraph examination within such categories would be barred.

RECOMMENDATIONS:

14. The Department should request the Armed Services Committees of the Congress to supplant the current year-to-year approach, which limits both the numbers and categories of personnel who might be asked to take counterintelligence-scope polygraph examinations, with continuing discretionary authority lodged in the Secretary to make such determinations, subject to Congressional oversight.

G. Establishing Special Controls Governing Access to Cryptographic Materials

Prior to 1975, the Department had special designations for persons who had access to, or were custodians of, cryptographic materials and equipment. Persons whose duties required such access were formally authorized access and required to sign briefing statements acknowledging their special responsibilities to protect this type of information. The program was discontinued in 1975, on the grounds that the administrative burden of the comprehensive program, which at that time included hundreds of thousands of DoD employees, did not justify the rather small benefits that were perceived.

It is clear, nonetheless, that cryptographic information continues to have crucial significance inasmuch as its compromise to hostile intelligence services can, in turn, lead to the compromise of any classified information being transmitted over secure voice or secure data channels.

The Commission, thus, unanimously favors the reinstitution of special controls to govern access by DoD employees and contractors whose duties involve continuous, long-term access to classified cryptographic information in large quantities or with highly sensitive applications. Only U.S. citizens would be eligible for access, and they must, among other things, agree at the time access is given to take a counterintelligence-scope polygraph examination if asked to do so during their period of access. A "crypto-access" program with more focused coverage than before, which also provides greater deterrence, would fully justify the administrative burdens entailed.

RECOMMENDATION:

15. Institute without delay a new "crypto-access" program.

H. Continuing Command/Supervisory Evaluations

Commanders and supervisors at all levels of DoD and defense industry are charged by regulations with reporting to appropriate investigative authorities adverse information which could have a bearing upon subordinates' worthiness to retain a security clearance. Based upon the experience both of DIS and the military investigative agencies, relatively little such information is actually reported. For example, only about four percent of cleared defense contractors have reported such data. In part, this is due to the reluctance of commanders/supervisors to report matters, especially of a personal nature, which could affect their subordinates' reputations or have a deleterious effort on morale. Another reason is that many commanders/supervisors are not sensitive to the significance of their subordinates' conduct from a security point of view. With respect to industry in particular, where the loss of a security clearance could mean the loss of a job, many employers are reluctant to report adverse information to the government for fear of prompting lawsuits by the affected employee. Finally, as a practical matter, contractors typically exercise very little supervision over cleared employees assigned in overseas locations.

To encourage such reporting by industry, DoD clarified its policy in 1983 to state that it does not expect the reporting of rumor or innuendo regarding the private lives of cleared industry employees. Still, it does expect to receive reports of information which are matters of official record or of problems which have required professional treatment. Relatedly, cleared contractors do not now review that portion of an employee's personal

history statement (i.e., "the privacy portion") that contains personal data (e.g., certain criminal history data, use of drugs) unless the employee consents to such review. As a consequence, information concerning the employee's background which may be known by the company and which would supplement or contradict that provided by the employee on the form is not being collected from the employer at the time the clearance is requested. The rationale for this policy is that DoD will obtain more information from contractor employees if they can be assured their employer will not have access; and, secondly, to prevent the employer from using such information for other purposes which could adversely and unfairly affect the employee, (e.g., terminate his employment, reduce promotion chances).

The Commission believes the lack of commanders' and supervisors' involvement in the security process is cause for concern because the command/supervisory system offers the most likely means of identifying security problems, including indicators of espionage, among cleared personnel. In virtually every recent espionage case, there has been evidence of conduct known to the commander/supervisor which, if recognized and reported, might have had a bearing on the continued access of the individual concerned and could have resulted in detection of his espionage actitivies.

The Commission has already recommended, and the Deputy Secretary of Defense has approved, two actions to treat this problem. The first requires annual military and civilian performance and fitness reports be revised to incorporate a requirement for the commander or supervisor to comment upon the subordinates' discharge of security responsibilities. The second requires commanders and supervisors to review all personal history statements submitted by subordinates with TOP SECRET clearances for purpose of initiating the required 5-year reinvestigations. If the commander/supervisor is aware of additional information concerning the employee which may have security significance, he will be required to provide such information at the time the reinvestigation is requested. A copy of the Deputy Secretary's actions is included at Appendix D.

An additional and important means of involving commanders and supervisors in DoD components would be to institute a program modelled after the DoD Personnel Reliability Program (PRP) which is designed to ensure that persons with access to nuclear weapons remain trustworthy and stable while performing such duties and which has proved its effectiveness over the years. Under this program, the commander/supervisor is required to make an initial evaluation of the individual and certify that, after review of the individual's pertinent records, he is fit for his anticipated duties. Periodic evaluation of participating personnel

focuses upon indicators of possible unsuitability for continued duties. The same concept could be applied to a wide range of classified programs, although, given the resources required, it would likely have to be limited to specifically designated programs of particular sensitivity.

RECOMMENDATIONS:

16. Require cleared contractor facilities to adopt procedures designating one or more individuals to act as agent(s) of the government, who shall be responsible for reviewing and comparing all information provided by applicants for security clearances on their personal history statements with other information known to the company, to ensure such information is accurate and complete; moreover, procedures should specify that any applicant may indicate on the form that he has information which he has not included but wishes to discuss with a government investigator. Prohibit any use or dissemination of such data within the cleared contractor other than for this specific purpose.

17. Direct appropriate DoD components to institute a "reliability" program for military and civilian personnel involved in especially sensitive programs or assigned to TOP SECRET positions of high criticality. It should embrace elements of, but be less structured than, the DoD Personnel Reliability Program (PRP).

I. Acquiring Information from Additional Sources

There are no formal channels in DoD for individuals to report information of security significance except through their command or organizational channels. Similarly, employees in defense industry are advised to report information of security significance to their security officer or supervisor. This tends to discourage reporting of pertinent information since the typical employee is reluctant to "inform" on his fellow employees, and, in most cases, is unable to gauge whether the information is significant enough to justify the unpleasant consequences which may follow.

One means of stimulating such reports would be to obtain Congressional authority to reward persons who provide information leading to an arrest for espionage, or the identification of hostile intelligence agents. There is legal precedent for this type of approach to obtaining information on terrorists, tax evaders, and other types of criminal behavior. Rewards may encourage more reporting of significant information by employees who now convince themselves that information in their possession is too "insignificant" to warrant getting involved.

Also, DoD has no formal, systematic means of obtaining relevant information concerning cleared personnel from law enforcement or regulatory agencies of federal, state, and local government. DoD should have a means of learning of misconduct

which is already a matter of public record, whether or not it is also reported by the commander or supervisor. Similarly, other information with potential security significance is available within the federal government (e.g., loan defaults, stock ownership by foreign interests, tax liens), but DIS routinely does not seek or obtain access.

RECOMMENDATIONS:

18. DoD components and industry should establish appropriate alternative means whereby information with potentially serious security significance can be reported other than through command or organizational channels, e.g., drop boxes, post cards, or designated telephones. In this latter case, the "hotline" established by the DoD Inspector General to receive reports of fraud, waste, and abuse, could be used to receive such reports of an unclassified nature, which would then be transmitted to the appropriate military counterintelligence element or the DIS for follow-up as may be warranted.

19. DoD should seek legislative authority to establish a program of monetary rewards for its personnel and contractor employees who provide information leading to the apprehension of persons engaged in espionage, or the identification of a hostile intelligence agent.

20. DoD should seek Department of Justice cooperation in obtaining, public record criminal justice information involving cleared DoD employees and contractors. Similarly, DoD should press for DIS access to other automated data banks of the federal government which contain information of potential security significance concerning cleared employees.

II. Managing and Controlling Classified Information

The majority of DoD's policies and procedures for managing and controlling classified information implement Executive Order 12356, which prescribes policy and procedure for the entire Executive Branch. The Executive Order, among other things, establishes the levels of classified information and delegates the authority to classify information to the heads of departments and agencies, including the Secretaries of Army, Navy, and Air Force, who may further delegate such authority as necessary. The order further provides that information shall be classified if it falls into certain prescribed categories (e.g., "military plans, weapons or operations; vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security") and its unauthorized disclosure could reasonably be expected to damage the national security. Dissemination of such information is limited to those who are determined to be trustworthy, i.e., have a security clearance and a "need-to-know" such information in the performance of official duties. Transmission of such information by either electronic means or by physical relocation must utilize methods which will prevent the disclosure of the information concerned to unauthorized persons. Such information must be stored in approved containers or under other approved conditions, and must be safeguarded to the extent necessary to prevent unauthorized access.

With some exceptions, these safeguarding requirements are essentially the same for DoD components and cleared DoD contractors. The latter are bound by the terms of their contracts to perform classified work and to abide by DoD industrial security regulations.

Executive Order 12356 also permits the heads of departments and agencies to establish "Special Access Programs" to protect "particularly sensitive" classified information; such programs and subject to "systems of accounting" established by agency heads.

Executive Order 12356 does not explicitly treat the transmission of United States classified information to foreign governments, apart from providing that classified information shall not be disseminated outside the Executive Branch unless it is given "equivalent" protection by the recipient. More detailed policy governing the foreign release of classified military information is found in the National Disclosure Policy, promulgated by the President and administered for the Secretaries of Defense and State by the National Disclosure Policy Committee, chaired by a representative of the Secretary of Defense.

A. Classification

There are no verifiable figures as to the amount of classified material produced in DoD and in defense industry each year. DoD reported an estimated 16 million documents classified in 1984, but this estimate is based on a sampling of message traffic from selected automated systems. DoD concedes the actual figure may vary considerably. In any case, it is clear that the volume of classified documents is enormous. Obviously, the Department needs to protect much of what it is doing with classification controls. Nonetheless, too much information appears to be classified and much at higher levels than is warranted. Current policy specifies that the signer of a classified document is responsible for the classification assigned but frequently, out of ignorance or expedience, little scrutiny is given such determinations. Similarly, while challenges to improper classifications are permitted, few take the time to raise questionable classifications with the originator.

The Secretary of Defense and Secretaries of the Military Departments have granted the authority to make "original" classification decisions, (i.e., to decide at the outset whether and at what level a program, project or policy is to be classified) to 2,296 "original classification authorities", including 504 officials with TOP SECRET classification authority and 1,423 with SECRET authority. Over the last 10 years DoD has pared down the number of officials with original classification authority; further reductions can be made. Given the fact that relatively few original classification decisions are actually made each year and these typically govern new programs and projects, such decisions necessarily ought to be made or approved by a limited number of senior-level officials. At present, there appear to be original classification authorities in some DoD components who are not in positions to exercise such control.

All persons who create new classifed documents based upon an original decisions to classify a program, project or policy are bound to carry over the "original" classification decision to the document being created. This process is called "derivative classification", and comprises by far the bulk of classification activity carried out in DoD.

DoD requires that original classification authorities issue classification guides prior to the implementation of a classified program and project, setting forth the levels of classification to be assigned to the overall project and to its component parts. Currently 1,455 such guides are in existence, however, many of these are incomplete and seriously outdated, notwithstanding the DoD requirement that they be reviewed biennially. Generally, classification guides do not cover policy determinations and actions ensuing therefrom.

Cleared DoD contractors do not have "original classification authority" and must apply the classifications given them by the project or program office to the documents they create. This classification guidance is provided in the form of a contract security specification to all classified contracts (DD Form 254), which is intended to provide the contractor with specific classification guidance, including the applicable classification guide, and the identification of the individual to be contacted if questions arise regarding classification. While logical in concept, this system is flawed in practice, being dependent largely upon the thoroughness and diligence of the contracting office to provide the required guidance. Although DIS regional offices have "classification managers" assigned to facilitate the interchange between contractor and program office, they are not in a position to provide such guidance or to motivate the contracting office to become more deeply involved. The contractor, though desiring answers, is often not inclined to bother his DoD benefactor.

In general, shortcomings in the area of classification are primarily a matter of inadequate implementation of existing policy, rather than a matter of deficient policy. (These inadequacies are generally addressed in Recommendation 53, below, under "Command/Supervisor Emphasis.")

The remedy is straightforward: disciplined compliance with the rules.

RECOMMENDATION:

21. Require, rather than simply permit, challenges to classifications believed to be improper.

B. Dissemination of Classified Information

Classified information may be disseminated only to someone with a security clearance at the level of the information concerned who has a "need-to-know" such information in the performance of official duties. TOP SECRET information is strictly accounted for both in DoD and in industry by a system of receipts, serialization, disclosure records, and inventories. Control procedures for SECRET and CONFIDENTIAL information are left to DoD components and, in practice, vary widely. Cleared DoD contractors, however, are required to maintain a chain of accountability for all SECRET documents.

Reproduction of TOP SECRET information under existing policy must be approved by the originator of the information in question. Reproduction of SECRET and CONFIDENTIAL documents is not so restricted, and reproduction controls, if any, are left to components to determine.

Most classified documents produced within DoD are multi-addressee memoranda, messages or publications, whose recipients could number in the hundreds. They are routinely handled by clerical and administrative personnel, as well as the staffs of the named addressees. Often such documents are distributed to recipients who have simply indicated they have an "interest" in the general subject matter covered in this and recurring reports without any critical evaluation of their need-to-know. Similarly, with respect to message traffic, often little confirmation of "need-to-know" is done initially or on a continuing basis. Getting on the list usually guarantees access regardless of actual need.

Classified information is exempted from release to the public under the Freedom of Information Act (FOIA), and, obviously, is not permitted to be released in open congressional testimony, or in articles intended for open publication. While DoD has mechanisms to provide security review of each of these potential channels to prevent improper dissemination, there are occasions when such disclosures occur due to human error or negligence. In 1984, CIA obtained congressional approval to exempt certain categories of its files from review under the FOIA, but DoD has no similar authority for its highly sensitive files. To require that such information be submitted to classification review is ultimately a waste of DoD resources since it cannot be released under any circumstances, and it risks the possibility that through human error it might be inadvertently disclosed.

In a related vein, although Executive Order 12356 provides that departments and agencies may disseminate classified information to persons outside the Executive branch provided such information is given "equivalent protection" by the recipient, DoD elements frequently provide classified information to the Congress without any understanding of how such information will be protected. While all congressional staff members who receive access to classified DoD information are, in theory, cleared by DoD, little attention is given the handling and storage of such information by congressional staffs, who are not, in fact, bound by the safeguarding requirements of Executive Order 12356. The Roth/Nunn subcommittee report cited this deficiency as requiring the attention of the Congress.

RECOMMENDATIONS:

22. Require DoD components to institute a uniform minimum degree of accountability for SECRET documents, which shall provide (1) a means to verify that any such document sent outside a major subordinate element of the DoD component concerned has been received; (2) a record of distribution outside such elements, where such distribution is not otherwise evident from the address line or distribution list; and (3) a method of verifying the destruction of such documents.

23. Direct DoD components and contractors to impose better controls over reproduction equipment used to copy classified information, such as (1) establishing classified reproduction facilities where only designated clerks could reproduce classified materials; (2) instituting key control over reproduction facilities; or (3) requiring two people to be present when classified materials are being reproduced. Additionally, initiate long-term action to develop technical or mechanical controls over unauthorized reproduction built into the equipment itself. (See Recommendation 58, under "Research" below.)

24. Press for legislation similar to that obtained by the CIA in 1984 to exempt certain categories of highly sensitive classified information held by the DoD from processing under the FOIA.

25. Urge the President of the Senate and Speaker of the House of Representatives to adopt, for each House of Congress, rules to provide uniform minimum control over classified information provided by departments and agencies of the Executive Branch. Volunteer to provide DoD resources and assistance to Congress to achieve this goal.

C. Transmission of Classified Information

Classified information must be transmitted in a manner that precludes its disclosure to unauthorized personnel. Classified telephone conversations between cleared persons must be over secure voice equipment. Classified electronic communications between ADP equipments must be transmitted over encrypted, or otherwise protected, circuits. Couriers, commercial carriers, and others who handle and transport classified information or material generally must be cleared to the level of the classified information concerned. There are, unfortunately, shortcomings--some serious--in each of these areas.

Heretofore, there have been serious shortages of secure voice equipment needed to support DoD and its cleared contractors. This has led to "talking around" classified information over unsecured communications channels vulnerable to hostile intelligence intercept. The NSA has initiated a revolutionary effort to make low-cost secure voice equipment available to DoD components, and, on a direct-purchase basis, to cleared contractors. Although this effort is in its initial phases of implementation, it promises a quantum increase in the capability to transmit classified information by secure voice means.

There are also major problems in the area of automated systems security. While DoD and its contractors have grown increasingly dependent on automated systems to process both classified and unclassified information, insufficient attention has been given to building security capabilities into computers and related distribution systems.

Computer security encompasses various internal technical measures as part of the architecture, design, and operation of automated information systems. Devices currently susceptible to unauthorized manipulation include computers, workstations, word processors, and storage transmission and communications systems used to create, process, transfer, and destroy information in electronic form. The technical flaws that render computers vulnerable often exist at the most complex, obscure levels of microelectronics and software engineering. Frequently even skilled engineers and computer scientists do not understand them. The subject is at the leading edge of technology.

The National Computer Security Center (NCSC) has been established at NSA to develop standards for new "trusted" computer systems and to evaluate products for use within DoD. It will be years, however, before all existing DoD systems are adequately analyzed and upgraded or replaced.

Because the federal government accounts for only four percent of the domestic computer market, NCSC strategy from the outset has been to encourage major computer manufacturers to build enhanced security into their standard product lines. Working in cooperation with industry, the NCSC identifies vulnerabilities, develops countermeasures, establishes standards of trust, and promotes government and private sector awareness of the risks and opportunities.

Adequate current funding for computer security research is essential, since the effect of research will not be realized in practice for 10 to 15 years.

Information classified at the SECRET or CONFIDENTIAL level may be appropriately wrapped and sent through registered and first class United States mail channels, respectively, so long as it remains entirely within United States postal control.

Current policy requires that TOP SECRET documents be couriered by a person with appropriate clearance. There is no uniform policy or system, however, for selecting and authorizing such couriers. Most of the TOP SECRET and other very sensitive material which is couriered long distances is handled by the Armed Forces Courier Service (ARFCOS) which operates worldwide under a charter issued by the Joint Chiefs of Staff. Although ARFCOS has, for the most part, been able to carry out its mission in a secure manner, it does not possess the physical facilities, communications means, or secure vehicles necessary to protect effectively the very sensitive classified information in its trust.

Commercial carriers in the United States which transport classified material are required to be cleared at the appropriate level. Through a system of receipts, minimal accountability is maintained from cleared sender to cleared recipient. Although it is patently impossible for DoD personnel to accompany all of the many shipments, checks could be made by DoD elements to determine whether the carrier complies with DoD requirements.

RECOMMENDATIONS:

26. Support and facilitate the efforts of the NSA to provide low-cost, secure voice telephone equipment to components and to cleared contractors.

27. Provide greater funding for the research and development efforts of the National Computer Security Center to improve the security of automated information systems.

28. Direct OJCS to assess the adequacy of ARFCOS facilities, vehicles, aircraft, and distribution elements to protect the highly sensitive information which it transports.

29. Require the DIS, the Military Traffic Management Command, or other appropriate DoD organizations to conduct periodic compliance checks of classified or sensitive shipments in transit.

D. Retention and Storage

Unless a classified document is marked for declassification upon a certain date or event, it will remain classified until declassified by the originating office or higher authority. It may be retained, in theory, only while there remains a "need." In practice, however, there are no real controls in DoD over the retention of classified information apart from the practical one of a place to store it. The required characteristics for such storage containers are detailed in existing policy.

There are statutory and DoD prohibitions regarding the destruction of "permanently valuable records" of the government, but the vast majority of classified documents held by DoD and its contractors do not qualify as such. The bulk of DoD's classified holdings are not "record copies" of classified documents held by the originator; instead, they consist of the multitude of "additional copies" of classified memoranda, messages, and publications that find their way into thousands of safes and filing cabinets.

Under current policy, destruction certificates signed by two witnesses are required for the destruction of TOP SECRET information; for SECRET, one witness is required, unless the requirement for destruction certificates has been waived to meet operational exigencies. As a practical matter, these requirements are not adhered to or enforced in many DoD components.

RECOMMENDATIONS:

30. Prohibit the retention of classified documents which are not "permanently valuable records of the government" more than five years from the date of origin, unless specifically authorized in accordance with record disposition schedules established by the component head.

31. Designate an annual classified information "clean-out" day, where a portion of the work performed in every office with classified information stored would be the destruction of unneeded classified holdings not otherwise required to be retained.

32. Establish a general policy, subject to waivers prescribed by component heads, that employees not be permitted to work alone in areas where TOP SECRET or Special Access Program materials are in use or stored.

E. Special Access Programs

Authority to establish Special Access Programs is contained in Executive Order 12356, "National Security Information." The intent is to ensure that sensitive activities are afforded greater protection than that normally accorded classified information. With few exceptions, such programs involve intelligence, military operations, research and development, and acquisition.

Special Access Programs originating in DoD must be approved by the Secretaries of the Military Departments or, in the case of other DoD components, by the DUSD(P) on behalf of the Secretary of Defense.

Such programs have proliferated in DoD in recent years, apparently out of concern that "normal" security does not sufficiently protect the information at issue. In a few cases, the special security aspects of these programs consist of nothing more than access lists; most, however, involve elaborate security frameworks and requirements, and may involve substantial numbers of persons with access. Most involve defense industry and are typically excluded from the Defense Industrial Security Program by decision of the sponsoring department or DoD agency (hence the term "carve out" contract).

All such programs are required to be reported to the DUSD(P) who maintains the "system of accounting" required by Executive Order 12356. DUSD(P) concedes that not all programs have been reported. Under DoD policy, each of the Military Departments is required to maintain a focal point office for administration of its own Special Access Programs. The DoD Inspector General has also created a special cell of cleared inspectors to conduct audits of such programs.

While the Commission is of the unanimous view that such programs are essential, they clearly present problems from a security viewpoint.

First, although the sole rationale for the creation of Special Access Programs under Executive Order 12356 is to provide enhanced security, there is sometimes too little scrutiny of this determination at the time such programs are created. Unless an objective inquiry of each case is made by the appropriate authorities, the possibility exists that such programs could be established for other than security reasons, e.g., to avoid competitive procurement processes, normal inspections and oversight, or to expedite procurement actions. With or without justification, there is considerable congressional sentiment that security is not the primary cause of the recent increase in Special Access Programs. Congress voiced such concern in its report on the FY 1984 Defense Appropriation Bill.

Second, unless there are security requirements established and adhered to by all such programs which exceed the measures normally applied to classified information, then the purpose of creating such programs in the first place is negated. The Commission has received reports from some contractors that, in fact, some Special Access Programs are afforded less security protection than collateral classified programs. This anomaly results from either failure to utilize the security expertise of the sponsoring agency in the development of the security plan and in inspections, or delegation of responsibility to prime contractors to ensure subcontractors comply with all special security requirements, a procedure not authorized for collateral classified contracts.

Third, it is apparent from reports received by the Commission that there is no uniformity in the extra security measures stipulated by DoD compoments for Special Access Programs. The individually developed security requirements, aggravated by the proliferation of Special Access Programs, place an undue burden on contractors who are participating in a number of such programs.

Fourth, it is also essential that appropriate oversight of the security administration of these programs be accomplished to ensure compliance with those security requirements which are imposed. Refusal to grant special program access to the DoD Inspector General for oversight purposes must be reported to the Congress in accordance with the statutory provisions of the Inspector General Act.

Some progress is being made in each of these areas by a DUSD(P)-chaired Special Access Program Working Group. A draft set of minimum standards to apply to all Special Access Programs, including those with industry involvement, has been under discussion. The need for serious and continuing oversight is acknowledged.

RECOMMENDATIONS:

33. a. The Secretary of Defense direct an immediate and one-time review and revalidation of all existing Special Access Programs and associated "carve out" contracts by the Secretaries of the Military Departments and heads of other DoD components; results to be reported not later than March 31, 1986.

b. The military departments should institute procedures to ensure the conduct of annual security inspection and regularly scheduled audits by the departmental security, contract administration and audit organizations; and submit an annual report, summarizing such inspections and audits, to the Deputy Secretary of Defense.

c. The DUSD(P) should expedite the development and promulgation of minimum security standards for DoD established Special Access Programs including those which involve defense contractors.

d. Appropriate measures should be taken to relieve prime contractors of sole responsibility for subcontractor compliance with Special Access Programs security requirements; and henceforth security inspections of all contractor participation in Special Access Programs be performed twice a year by professional security personnel of the sponsoring component.

e. DIS should establish a core of specially cleared and qualified inspectors for Special Access Programs with associated contracts; and inspection responsibility for these contracts be transferred to or shared with DIS when deemed appropriate by the sponsoring component.

f. Pursuant to his statutory requirements, the DoD Inspector General, in conjunction with the sponsoring department or agency, should conduct oversight audits of Special Access Programs.

F. International Cooperation Involving the Transfer of Classified Information

Transfers of classified military information to foreign governments are governed by the National Disclosure Policy, promulgated by the President, which provides the general criteria and conditions to govern such transfers, and delegates authority for DoD components to transfer certain categories of classified information to certain foreign recipients on their own initiatives. Any contemplated transfer of classified information which exceeds the eligibility levels established under the National Disclosure Policy must be considered and approved on a case-by-case basis by the National Disclosure Policy Committee (NDPC), an interagency body chaired by a representative of the Secretary of Defense.

The NDPC, as a major part of its functions, also conducts periodic surveys of the security framework within recipient countries to ensure that equivalent levels of protection can be and are being provided United States classified information. Based upon the surveys, the eligibility levels of recipient countries are adjusted.

This framework is logical, and works reasonably well in practice. There is, however, room for improvement.

The Commission was made keenly aware of the risk to United States classified information once it leaves United States control, even in the hands of friendly allied countries. Although the United States attempts to assure itself of both the capability and intent of recipient governments to protect United States classified information prior to providing such information, as a practical matter, the United States has little control over such information once in foreign hands, and has little expectation that it will learn of compromises. The problem is particularly critical with respect to co-production arrangements, where losses could entail not only the end-item being produced but also the technical "know-how" necessary to manufacture it in large quantities.

It is also not uncommon for Defense or State Department officials who deal with other governments regularly with respect to arms sales to suggest the United States is willing to sell classified weapons systems prior to obtaining the necessary approval of the responsible military service, and, as required, the NDPC. Such statements have the effect of skewing the NDPC approval process which then must consider the political consequences of failing to follow through on what the other government perceived as a United States commitment.

Finally, the NDPC security survey program is only modestly effective. Too few surveys are carried out, and there is insufficient flexibility in the program to satisfy DoD's most pressing requirements. Even with respect to those surveys which are conducted, many lack the probing, objective analysis required, and, because survey team members (representing NDPC member agencies) return to their normal duties upon completion of the survey, survey reports are often outdated when finally published.

RECOMMENDATIONS:

34. The National Disclosure Policy should be amended to standardize the approach to be followed in approving classified transfers, to include: (1) requiring a determination that the need of the recipient cannot be satisfied by unclassified systems or data; (2) if classified systems systems or data are required, then require selection of a model or type of such

system that minimizes the need to transfer classified information; (3) require phasing in of the most sensitive classified information over time, if feasible; and (4) avoid co-production of military systems which involve the manufacture abroad of the most advanced version of classified components or end-items. While the Commission recognizes that the foreign disclosure process, in practice, generally operates in accordance with these principles, placing them within the National Disclosure Policy should ensure greater adherence.

35. NDPC surveys should be conducted and administered by a permanent, dedicated staff of security professionals assigned to the NDPC capable of producing objective, timely reports. The survey schedule program must also be sufficiently flexible to meet pressing DoD requirements for in-country security assessments.

III. DETECTING AND COUNTERING HOSTILE INTELLIGENCE ACTIVITIES UNDERTAKEN AGAINST DOD

The FBI has primary responsibility within the United States government for keeping track of the activities of known or suspected hostile intelligence agents within the United States. However, DoD foreign counterintelligence agencies (the Army Intelligence and Security Command, the Naval Investigative Service, and the Air Force Office of Special Investigations) each conduct, in conjunction with the FBI within the United States and in coordination with the CIA abroad, counterintelligence operations and investigations designed to identify and counter hostile intelligence activities taken against their respective services.

DoD components also dedicate substantial resources to security awareness briefing programs among their employees to sensitize them to potential hostile intelligence activities. Their experience has been that the greater the reach of such programs, the more information concerning hostile approaches is reported. In industry, cleared contractors regularly receive "Security Awareness Bulletins" published by DIS; the military services also provide threat briefings to selected contractors, which are supplemented by the FBI's Development of Counterintelligence Awareness (DECA) Program, which again involves briefings to selected defense contractors.

In addition, a variety of measures are currently being implemented on a fragmented basis within DoD which are designed to provide indications of possible espionage activities. These include requirements to report contacts with foreign representatives; to report travel to designated countries, or, in some cases, to any foreign country; the use of sources at sensitive projects to report evidence of hostile intelligence activities or indications of espionage; and the use of physical searches, to determine if classified information is being removed from the premises without authority.

A. Limiting and Controlling the Hostile Intelligence Presence within the United States

DoD information is the primary target of the hostile intelligence presence within the United States. DoD, therefore, has a major stake in what United States actions are taken to reduce (or expand) the size of the hostile intelligence presence, as well as to limit (or expand) its operational environment in the United States. A major step towards achieving reciprocity of treatment for diplomatic personnel was the establishment by statute of the Office of Foreign Missions within the Department of State in 1982. The diplomatic personnel of certain countries are now required to obtain travel accommodations and needed services through the Office of Foreign Missions, which handles such requests in a manner similar to the way in which United States diplomats are treated in the country concerned.

Recently, additional measures have been instituted in both the Legislative and Executive branches which would have the effect of further reducing or controlling the hostile intelligence threat. In the FY 1986 State Department Authorization Bill, for example, two significant provisions impacting the hostile intelligence presence in the United States were added on Congressional committees' initiative. The first would apply to United Nations Secretariat employees who are nationals of a country whose diplomatic personnel are subject to the Office of Foreign controls, those same limitations and conditions, unless the Secretary of State waives such requirements. The second would establish the policy of "substantial equivalence" between the numbers of Soviet diplomatic personnel admitted into the United States, and those United States diplomatic personnel admitted into the Soviet Union, unless the President determines additional Soviet diplomatic personnel may be admitted.

Further restrictions ought to be instituted on the travel of non-Soviet Warsaw Pact nationals assigned to the United Nations secretariat or to the diplomatic missions so accredited. The United States has heretofore refrained from imposing travel restrictions on any non-Soviet Warsaw Pact diplomatic and consular personnel in this country. The rationale has been that our diplomatic personel accredited to East European governments are allowed considerable latitude of movement. A reciprocity principle is sound insofar as it applies to non-Soviet Warsaw Pact diplomatic personnel accredited to the United States Government. Extension of the principle to personnel at the United Nations is quite another matter. They are not accredited to the USG; their duties should be exclusively geared to the business of the UN; but, as a practical matter, they constitute a substantial augmentation of the intelligence collection capabilities based at or directed from their nations' embassies in Washington. The United States has no comparable means of augmenting its diplomatic missions in the non-Soviet Warsaw Pact countries. Should those countries react to travel restrictions on its UN pesonnel by restricting our diplomatic and consular officials, the US would be fully justified in taking similar action against those personnel of the countries concerned that are accredited to our government.

RECOMMENDATION:

36. The Secretary should provide full support to Executive and Legislative branch efforts -- and where necessary initiate action -- to reduce the freedom of action of hostile intelligence operatives within the United States under diplomatic auspices; specifically:

° By expanding the national policy of parity in numbers in the diplomatic establishments of the Soviet Union and the United States accredited to each others' governments, to encompass parity in treatment and privileges.

° By extending this expanded policy of parity to all other nations who present a hostile intelligence threat to the United States.

° By requiring that personnel of the non-Soviet Warsaw Pact missions accredited to the United Nations, as well as personnel of those nations assigned to the United Nations Secretariat, be subjected to the same travel restrictions as to those imposed on Soviet personnel serving in those two capacities.

B. Identifying and Monitoring Hostile Intelligence Agents

The FBI has primary responsibility for identifying and monitoring known or suspected hostile intelligence agents within the United States. Counterintelligence elements of the military services also have trained cadres of counterintelligence specialists who conduct joint counterintelligence operations in the United States with the FBI involving DoD personnel or information. DoD agencies do not, however, routinely support the FBI in terms of monitoring the activities of known or suspected hostile intelligence agents unless such support is specifically related to a joint operation. Potentially, DoD has the capability to provide considerable support to help meet operational exigencies -- not only with agents but also with technical and logistical assets.

RECOMMENDATION:

37. Explore with the FBI and Department of Justice the feasibility of DoD counterintelligence elements playing a wider role in support of FBI responsibilities for monitoring the hostile intelligence presence within the United States during periods of unusually heavy activity.

C. Counterintelligence Operations and Analysis

Policy matters concerning the DoD foreign counterintelligence activitives are coordinated through the Defense Counterintelligence Board, chaired by a representative of DUSD(P). The counterintelligence elements of the military services conduct both offensive and defensive counterintelligence operations and investigations, the details of which are largely classified. They also analyze available information from these operations as well as from other agencies in the counterintelligence community, and provide counterintelligence reports to their respective services (which are also shared with the community). The DIA, while having no operational counterintelligence role, plays a major role in the production of multi-disciplinary counterintelligence analyses for DoD as a whole, and coordinates the production of finished reports by the service agencies.

Although resources for the conduct of counterintelligence operations have increased in recent years, more are needed to fund additional analysis of operations to enhance the capability to utilize "lessons learned" from operational activities. This will provide better understanding of hostile intelligence targeting and modus operandi, as well as improved security to counterintelligence operations.

RECOMMENDATIONS:

38. Ensure, in development of the National Foreign Intelligence Program, there is increased funding for counterintelligence analysis. Relatedly, DIA should establish a Multidisciplinary Counterintelligence Analysis Center as a service of common concern for DoD, funded through the Foreign Counterintelligence Program, which will be responsive to the CI analytic requirements of the Defense Counterintelligence Board and the various DoD components.

39. The Defense Counterintelligence Board should coordinate DIA and service activities to exploit operations; and evaluate technical advances being made by hostile intelligence services.

D. Security Awareness Programs

All DoD components with classified functions have some type of security awareness program, consisting typically of required briefings, briefing statements, audiovisual aids, posters, and publications of all types, describing the hostile intelligence threat. Although such programs are not centrally coordinated in DoD, substantial, if uneven, effort is devoted to them. Moreover, they have proven reasonably effective in sensitizing personnel to possible hostile intelligence approaches. The military services report the number of contacts reported rises in proportion to the number of security awareness briefings which they are able to administer.

Although DoD compoments should continue to be manage and administer their own security awareness programs, DoD should facilitate and coordinate these programs to avoid duplication of effort, and to improve the caliber of briefings and training aids. (See Recommendation 57, below.)

Awareness programs in industry are far smaller and less effective. While the DIS publishes a "Security Awareness Bulletin" sent to all cleared contractors, it is rarely seen beyond the company security office. Similarly, while the military departments and the FBI present threat briefings to selected DoD contractors, these reach only a small portion of the 1.2 million cleared contractor employees, usually being given to security or management officials. There is no overall coordination of security awareness programs within defense industry. The Commission believes that considerable dividends in improved security could be achieved by a relatively small investment to bolster the security consciousness of cleared contractor personnel through an effective security awareness program.

RECOMMENDATION:

40. Direct DIS, in conjunction with the military departments and the FBI, to take action on an urgent basis to increase the size, effectiveness, and coordination of the security awareness program in industry.

E. Reporting Indications of Possible Espionage

There are existing requirements for DoD employees and contractors to report suspected espionage. However, there are few specific or uniform DoD requirements, applicable to all employees and contractors, to report information which could indicate to experienced investigators the possibility of espionage activity and the need for further investigation. To the extent that such information is being reported, the requirements to do so are largely a matter of component regulations, and, in the case of cleared contractors, the requirements of the Industrial Security Manual.

Reports of unofficial or unsanctioned contacts with representatives of foreign governments, particularly where efforts are made to elicit defense related information, could indicate espionage actvities. While most DoD components have some type of requirement to report such contacts, they are not uniform nor are they well enforced. In industry, there is no requirement to report such contacts short of the requirement to report possible evidence of espionage.

Similarly, foreign travel at particular intervals and to particular locations could indicate to experienced investigators possible espionage requiring follow-up. While many DoD components and defense industry have requirements to report travel by cleared personnel to Communist-bloc countries, very few components require reporting of travel to other foreign countries.

Other indicators of possible espionage activities, are not generally required to be reported, although such reports are occasionally made and acted upon. They include such things as unexplained affluence; unexplained absences; attempts to solicit information beyond one's need-to-know; and unexplained, unaccompanied visits to classified areas during non-work hours. In certain particularly sensitive programs, some military counter-intelligence agencies ask a certain person(s) within such program to watch for and report any such indicators directly to the investigative agency. Such sources are not utilized, however, in most DoD components or in industry.

RECOMMENDATIONS:

41. DoD should adopt a uniform requirement for both components and industry employees to report (1) all contacts with foreign nationals who request classified or unclassified defense information, or which suggest a possible effort at recruitment; and (2) all official and unofficial contacts with foreign national of any country determined by appropriate authority to have interests inimical to those of the United States. Reports should be made to commanders or supervisors who will determine whether referral to investigative agencies is warranted.

42. Direct DoD components and cleared contractors to establish appropriate internal procedures requiring cleared employees to report to their security office all personal foreign travel in advance. Records of such travel should be maintained by the office concerned for the last five years. Where travel patterns indicate the need for investigation, the matter will be referred to the appropriate counterintelligence investigative agency. While it is recognized that persons actually engaged in espionage are unlikely to report such travel, a failure to observe this requirement, if detected, could itself suggest the need for further investigation.

43. Authorize the use of passive sources in sensitive, classified projects and programs to watch for and report indicators of possible espionage activities among cleared persons to appropriate authorities.

F. Detecting and Investigating Security Violations

DoD policy requires that security violations (i.e., instances where classified information was, or may have been, compromised) be reported and investigated. Relatively little effort, however, is dedicated by DoD components to detecting such violations through unannounced inspections or searches, neither of which is made mandatory by DoD policy and procedure.

Moreover, where security violations are apparent, they are frequently not reported or investigated, and even less frequently are they referred to professional investigative agencies, even where a pattern of such violations involving the same individual is in evidence. Security violations which appear to be attributable to negligence, misunderstanding, or "exigencies of the situation" can, in fact, be indications of a serious security problem.

RECOMMENDATIONS:

44. Establish a policy that all persons entering or leaving defense activities, including, to the extent practical, its contractors, are subject to inspection of their briefcases and personal effects, to determine if classified material is being removed without authority. DoD components should then establish internal procedures to require some type of inspection program be instituted at the facilities under their control, recognizing the need not to unduly affect the flow of traffic to and from DoD installations and to respect the personal privacy of employees. DoD components should also establish appropriate internal procedures requiring unannounced security inspections to be made of activities where classified work is performed.

45. Require reports to appropriate counterintelligence and investigative authorities concerning any employee who is known to have been responsible for repeated security violations over a period of one year, for appropriate evaluation.

G. Taking Effective Action Against those who Violate the Rules

In order to maximize compliance with the security standards and deter violations, commanders, supervisors, and contractors must effectively employ available criminal, civil, and administrative sanctions against those who engage in espionage, commit security violations, or otherwise compromise classified information. Effective enforcement depends upon both the adequacy of such sanctions as well as the willingness of supervisors to impose them.

Crimes by service members. The FY 1986 Defense Authorization Act amends the Uniform Code of Military Justice (UCMJ) to establish a peacetime military espionage offense and to provide capital punishment for both peacetime and wartime offenses.

With these changes, adequate criminal and administrative remedies will be available to punish a broad spectrum of violations of security rules by military personnel, including the unauthorized disclosure of classified information. The sanctions range from capital punishment for espionage to prison terms for less serious crimes to nonjudicial punishment for minor violations.

Crimes by civilian personnel. Civilian criminal statutes relating to espionage and unauthorized disclosure of classified information do not provide adequate remedies. For several years the Department has supported, in principle, proposed legislation to establish more effective criminal sanctions against unauthorized disclosure of classified information but agreement within the government with respect to the content of such a proposal has not been achieved.

Other recent developments, however, may result in more effective criminal enforcement against civilian offenders. The first such development is the reinstitution of the death penalty for civilian espionage. A bill for this purpose (S.239) has passed the Senate but not the House. Enactment of S.239 would significantly increase the deterrent effect of existing civilian espionage statutes.

Since 1975, the Department of Justice has vigorously pursued enforcement of the espionage laws and related statutes. An example of this was the recent trial of Samuel Loring Morison, in which the trial judge ruled that the civilian espionage laws can be used to prosecute the unauthorized disclosure of classified information without proof of a specific intent to injure the U.S. or to aid a foreign power. Morison was subsequently convicted. If the conviction is upheld, it will provide additional precedent for the legal principle that deliberate unauthorized disclosure

of classified information constitutes a crime under the espionage statute. Nevertheless, the precedent of the Morison case will not enable the espionage laws to be used to punish unauthorized disclosure of classified information under all circumstances.

The courts have also allowed defendants to be charged with other types of crimes (such as theft of government property and conversion of proprietary information) in cases where classified information has been improperly obtained but where espionage is not an appropriate charge. This is illustrated by a recent prosecution for theft of classified DoD budget documents to enhance a contractor's competitive position.

Civil remedies against civilian offenders. In those cases where the criminal sanctions against civilian offenders are inadequate, civil remedies may provide effective enforcement tools. For example, a suit against the offender for money damages may be possible under certain conditions; or action to recover documents from possession of an unauthorized person may also be undertaken.

Administrative measures regarding DoD personnel. Military and civilian employees of the Department who violate security regulations are subject to a range of administrative actions (in addition to the criminal and civil sanctions mentioned above), to include warning, reprimand, suspension without pay, forfeiture of pay, removal, and discharge. Executive Order 12356, which establishes the security classification system, provides that appropriate sanctions will be administered to those who violate the order.

It is improper to impose suspension or termination of a security clearance as a penalty for security violations. Nevertheless, adjudicative authorities should be permitted to suspend a security clearance in cases where an individual has clearly demonstrated an unwillingness or inability to protect classified information, pending the readjudication of his clearance.

Administrative measures regarding contractors and their employees. The responsibility for taking administrative action against offending contractor employees lies with the contractor. DoD has no legal basis to force the contractor to take such action. In the absence of such actions by the contractors, DoD's only administrative recourse with respect to an offending contractor employee is to seek revocation of the individual's security clearance. Contractors should be required, therefore, to establish and vigorously enforce company sanctions consistent with DoD policy.

With respect to the company itself, DoD may withhold payments under DoD contracts from contractors who fail to comply with the terms of the contract, including security requirements. Although this remedy has not heretofore been utilized in security cases, it is potentially a powerful one.

DoD can also revoke the contractor's facility clearance based upon failure to correct serious security deficiencies. However, since most companies take some type of corrective action, revocation of the facility clearance rarely occurs, even though the company may be cited for repeated serious violations.

RECOMMENDATIONS:

46. Continue to advocate enactment of legislation to enhance criminal enforcement remedies against civilians who improperly disclose classified information.

47. Instruct commanders and supervisors, in consultation with appropriate legal counsel, to utilize all appropriate enforcement remedies -- criminal, civil, and administrative -- against employees who violate the law and security regulations.

48. In the absence of mitigating circumstances, require supervisors and commanders to refer to appropriate adjudicative authorities the security clearance of any person who:

a. Deliberately disclosed classified information to an unauthorized person; or

b. Committed two security violations within a year, one of which resulted in loss or compromise of classified information.

Provide further that adjudicative authorities may suspend such clearance when it appears that other classified information would be jeopardized by continued access of the individual, pending investigation and final adjudication of the clearance.

49. Require defense contractors to establish and enforce company policies which provide for appropriate administrative actions against employees who violate security regulations.

50. Make broader use of the authority under DoD procurement regulations to withhold payments under a classified contract in order to enforce compliance with DoD security requirements.

51. Permit revocation of a contractor's facility clearance for repeated security violations of a serious nature or other conduct which demonstrates a serious lack of security responsibility, regardless of whether actions have been taken to correct specific deficiencies for which the company had previously been cited.

PART TWO: Management and Execution

In addition to reviewing policy and procedure, the Commission addressed shortcomings in the management and administration of counterintelligence and security programs. Policy and procedure are only as effective as the manner in which they are carried out. Indeed, in terms of the entire process, policy formulation--while the indispensable beginning--constitutes only a minute part of the task to be accomplished; the far greater effort--and challenge--is in the implementation and execution.

In general, the Commission found DoD counterintelligence and security programs to be adequately managed by most DoD components. Nevertheless, it discerned major gaps between policy and practice where improvements were urgently needed.

A. Command/Supervisor Emphasis

Commanders and supervisors, from the highest leadership of the Department down to field commanders and officers of small defense contractors, play the key roles in making security policy work. Their roles involve not only issuing orders and instructions, but setting an example as well. Subordinates tend to observe security rules and regulations the way they perceive their commander or supervisor treats them. While it is impossible to measure precisely this intangible but crucial factor, the Department's overall performance in this regard must be considered uneven at best.

Directives clearly tell commanders and supervisors what information should be classified and when it should be downgraded; still, overclassification remains a problem and declassification actions are rare. Directives explicitly prohibit the passing of classified information to those lacking a clearance and a specific need-to-know; yet, all too often classified information is discussed without ascertaining the level of clearance of the persons who are listening, much less determining their "need-to-know". Regulations provide that classified information cannot be taken home to work with, unless stored in an approved safe, but the prohibition is ignored by many for the sake of convenience. Regulations restrict the reproduction of classified material; yet, files bulge with unauthorized and often needless copies. By simply carrying out extant policy, commanders and supervisors can substantially improve the quality of security in the Department.

Yet, some commanders and supervisors show a clear disdain for security, leaving compliance to clerks and secretaries. When security requirements become an impediment, they are ignored either for reasons of personal convenience; or to facilitate job performance; or, perhaps, for political reasons. Whatever the reason, such attitudes have a debilitating impact on subordinates and on the success of the program as a whole. It is difficult for the cleared rank-and-file to take the system seriously when the individual in charge does not comply with the rules.

RECOMMENDATION:

52. The Secretary of Defense should direct all DoD components which handle and store classified information to institute one-time "top-to-bottom" command inspections at every level of their organizations within six months. Such inspections should, at a minimum, ascertain (1) if applicable DoD and component security policies are understood by commanders and supervisors, as well as subordinates; (2) if such policies are, in fact, being complied with; and (3) if they are being enforced. Results of these command inspections should be reported to the next higher level of authority, with DoD components ultimately submitting consolidated reports to the Secretary of Defense within nine months. DoD components should also ensure that recurring inspections are made by their Inspectors General or equivalents in compliance with applicable security policies throughout the department or agency concerned.

B. Organizational Arrangements

The Commission did not consider in depth organizational arrangements below the DoD level. It is apparent, however, that the organizations and offices involved in security policy development and oversight, as well as in security administration, constitute a substantial bureaucracy within DoD. Security policy functions are fragmented in most DoD components. Few have consolidated all aspects of security policy under one official. Moreover, security officers are often "buried" far down in the organization and consequently have little opportunity to bring major problems or meaningful recommendations to top management attention; nor do they possess the authority to conduct effective oversight and deal with deficiencies. Security administration (as opposed to security policy development) is necessarily decentralized, reaching down to the office level. All too often, however, there are no organizational links between security policy offices and security administrators, reducing mutual exchange between them.

With respect to DoD-level organizational arrangements, security policy development within the OSD staff is split between the Deputy Under Secretary of Defense for Policy (DUSD(P)) and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). These offices share oversight responsibility with the DoD Inspector General and the DoD General Counsel. Within DUSD(P), the Directorate for Counterintelligence and Security Policy, staffed by 25 professionals, has primary staff responsibility for policy development and oversight of the areas of information security; personnel security; physical security; industrial security; Special Access Programs; the disclosure of classified information to foreign governments; management of the Foreign Disclosure and Technical Information (FORDTIS) system; operations security; and counterintelligence operations, investigations, and production. As a result of a

recent OSD staff reorganization, responsibility for policy development and oversight in the areas of communications security and automated information systems security was transferred to the Deputy Assistant Secretary of Defense for Command, Control and Communications (DASD(C3)), staffed in these areas by four professionals. Presumably, this decision was motivated, in part, by the designation of the ASD(C3I) as Chairman, of the National Telecommunication and Information Systems Security Committee (NTISSC), which formulates national policy in these areas from which DoD policies and procedures derive.

It is clear, however, that all security disciplines have as their fundamental purpose the protection of classified information and must be applied in a fully balanced and coordinated way. Actions taken in one area, for example, personnel security, have a direct bearing upon actions taken in other areas, e.g., automated systems security. Where security policy functions are fragmented, the chances of reaching inconsistent and wasteful results are increased. Pertinently, the Departments of State and Energy have recently seen fit to establish consolidated professional security organizations at the Assistant Secretary and Deputy Assistant Secretary level, respectively.

While there are numerous interdepartmental boards and committees in the area of counterintelligence and security established by DoD issuances, there is no high-level advisory board which covers the entire security area with a direct reporting channel to the Secretary of Defense. Recommendations for changes to existing policy and procedure are thus moved through normal staff channels from DUSD(P) or ASD(C3I) to the Secretary.

A number of functions vital to the success of the DoD security program which logically should be performed at DoD level are not being accomplished for lack of sufficient OSD staff. Indeed, the staff of the Secretary of Defense for security policy development and oversight is substantially undermanned. One or two professional staff are typically assigned responsibility for huge DoD programs, e.g., two each for personnel security and industrial security; one each for Special Access Programs and use of the polygraph. Most stay fully occupied handling incoming actions; there is little time for policy development or oversight, theoretically their principal functions.

For example, neither DUSD(P) nor ASD(C3I) coordinates research and development activities in the security area. A single action officer located in the Office of the Under Secretary of Defense (Research and Engineering) coordinates research limited to physical security hardware. In general, the military departments and, occasionally, defense agencies initiate such work on their own without DoD-wide evaluation or application. The scope of this research effort is far too narrow (see the discussion of "Research" below).

A second area with virtually no staff involvement is the collection of statistical data needed for management purposes. The Commission was struck by the lack of statistical data available upon which management decisions concerning a number of critical counterintelligence and security programs should logically be based.

A third area where there is no OSD involvement is the coordination of security training activities. The result is that there are numerous gaps and much redundancy in the existing system (see the discussion of "Training" below). Relatedly, in the area of security awareness, there is no OSD oversight to ensure that DoD programs achieve overall coverage or that they are supported by high-caliber briefings and audiovisual aids.

There is also very little OSD involvement in improving career development patterns for personnel with responsibilities in the security area. The DoD components are left to establish and structure their own programs, with mixed results. (See the discussion of "Career Development" below.)

Finally, there is no central clearinghouse for information and publications in the security area. No office is charged with the systematic collection and distribution of reports or research. Work done by one component gets to OSD or to other DoD components who may have a use for it only by happenstance. The system would benefit if a clearinghouse program were in effect.

The functions set forth above are crucial to the overall security program. The discharge thereof will require personnel resources not now available to the OSD staffs concerned. Those functions involving policy direction and oversight -- and properly the responsibility of the DUSD(P) -- can be accommodated by modest staff augmentation. Discharge of the other functions will require more personnel resources and need not, in any case, be placed within the OSD staff. In the Commission's view, the most practical solution would be to assign these responsibilities to an expanded Defense Security Institute (DSI). That institute is now part of DIS and its mission is limited to training DoD personnel and contractors in various aspects of security, as well as publishing security awareness materials for industry. Under the Commission's concept, the Defense Security Institute would remain assigned to DIS but would be responsive to the policy direction of the DUSD(P).

RECOMMENDATIONS:

53. The Secretary of Defense should re-examine extant OSD staff functions in light of the desirability of placing related security policy responsibilities in a single staff element.

54. Unless countervailing management considerations obtain, the senior official(s) responsible for counterintelligence and security policy matters within OSD and DoD components should have a direct reporting channel to the head of the department or agency.

55. The Secretary should establish a Security Advisory Board to advise him periodically with respect to the security posture of the DoD.

56. The Secretary should authorize modest augmentation of the OSD staff to insure effective policy direction and oversight.

57. The Secretary should designate the Defense Security Institute as the principal support activity for DoD security programs; authorize its expansion; and place it under the aegis of the DUSD(P) for policy direction.

C. Research

Although billions of dollars are spent annually for security, relatively little goes to research activities. Moreover, significant aspects of security policy and practice should properly be based upon research. Yet, such research is neither ongoing nor planned.

For example, there logically should be research to determine the optimum structure of background investigations. There should also be an analysis of the efficacy of the information elicited on personal history statements required to be filled out by clearance applicants; and there should be a similar analytic basis underpinning questions being asked of the subject by DIS investigators. None of this exists.

There should also be research into the efficacy of new techniques to supplement background investigations, such as psychological tests, behavioral tests (to determine such characteristics as compulsion to seek or reveal information received in confidence) and urinalysis, but, with the exception of work begun on the use of psychological tests, little has been accomplished in this area.

Research on the reliability and validity of the polygraph is also minimal. Although the NSA has initiated a promising new effort in the past year, the topic urgently warrants additional work.

Adjudication policies also beg for a firmer basis in research. DoD guidelines for denying security clearances should logically be based upon a credible analysis which demonstrates a logical link between the grounds used for denying a security clearance (e.g., excessive use of alcohol) and the likelihood that such behavior may reasonably be expected to lead to a compromise of classified information. Currently, there is insufficient research underpinning DoD adjudication policies.

There has been some improvement with respect to research on physical security devices and equipment. Under the direction of the Under Secretary of Defense (Research and Engineering), the Army, Navy, and Air Force are developing such devices as internal detection sensors, external sensors, and emergency destruction systems. Moreover, DoD has participated in interagency efforts which have led to improvements in secure storage containers and automated access devices.

There is, however, a paucity of research accomplished or contemplated within DoD with respect to devices or procedures which could detect or prevent the unauthorized removal of classified information from DoD or contractor installations or which could prevent or detect the unauthorized reproduction of classified information. In view of the technological advances in recent years, it would appear that such devices or procedures are well within the technical capabilities of modern industry.

With regard to information security, almost no research is available, ongoing or contemplated. And yet, research into how the classification system actually works in practice (i.e., how much improper classification is there? how much classified information is created? how much is destroyed?) would provide a clearer basis than presently exists to manage the system.

Only in communications security equipment and automated information systems security, both of which are managed by the NSA, did the Commission find well-defined research programs in being.

The deplorable state of research in the area of security can be attributed primarily to the fact that no one office is specifically charged with responsibility for coordinating and promoting all such activities. While such activities clearly have to compete with other DoD research priorities, funds have not, for the most part, been requested or programmed for these activities by any office or component. DUSD(P) agrees that such responsibilities rest with his office, but states that he lacks sufficient staff to coordinate and monitor research contracts or component activities in this area.

RECOMMENDATION:

58. Authorize substantially increased funding for security research to be coordinated through the DoD focal point (See Recommendation 57 above), to institute research at the earliest possible date into: (a) determining the efficacy of the elements of background investigations, including information required on personal history statements and in subject interviews; (b) the feasibility of the subject providing additional information to establish bona fides; (c) new techniques to supplement the background investigation such as

psychological tests, behavioral tests (e.g., to measure compulsion to talk, to divulge or acquire information or the propensity for carelessness or to explain away problems); and urinalysis; (d) polygraph reliability; (e) the development of more precise adjudicative standards based upon conduct which is reasonably likely to result in compromise of classified information; (f) devices and equipment which could prevent or detect the unauthorized removal or reproduction of classified information; (h) how the classification system actually works in practice; and (i) physical security technology. The results of all such research efforts should be widely shared within the Department and its contractors.

D. Training

Security training, like other professional disciplines, has a direct bearing upon the quality of performance. DoD has certain specific training requirements, such as for polygraph operators, but generally the type and length of security training, particularly in non-technical areas, are left to the discretion of DoD components. DoD requires no minimal level of training, for example, for civilian or military employees who are performing security duties. In industry, contractors are encouraged to avail themselves of training courses provided at the Defense Security Institute, but attendance is not mandatory. As a practical matter, larger contractors with security staffs usually send representatives to these courses, while smaller contractors do not. The great majority of industrial employees who perform security duties receive no formal security training.

As stated earlier, there is no formal training, apart from occasional seminars, given to persons who must adjudicate security clearances. There exists a clear need to instruct such personnel in the application of DoD adjudication criteria to particular and recurring fact situations to ensure greater consistency of results.

RECOMMENDATIONS:

59. Establish minimal levels of required training for DoD military and civilian personnel who perform security duties. Task the Defense Security Institute and National Security Agency, as appropriate, to develop and provide basic courses of instruction for such personnel, supplemented as necessary by component courses of instruction. A course of instruction on adjudication of security clearances should be developed by DSI in coordination with the DoD General Counsel, and made mandatory for all DoD personnel assigned adjudication functions.

60. Require all DoD contractor security officers, or those otherwise performing security duties for a cleared contractor, to complete some type of uniform training. This could take the form of a required correspondence course administered by the Defense

61. All training in the security area should result in appropriate certifications by DoD (e.g., as a security specialist, adjudicator, industrial security specialist) to be recorded in the personnel file of the individual.

E. Career Development

Security professionals seek other careers when they cannot envision a clear path to higher positions of rank and responsibility; when untrained and unqualified persons are placed into positions which should be occupied by security professionals; and when they are qualified for advertised positions but are hampered by being classified under a job series which is too restricted. Unfortunately, in some DoD components, such conditions are already in evidence.

In part, this can be attributed to the fact that no DoD office is specifically charged with responsibility for career development of security professionals. Consequently, very little has been done in DoD as a whole to improve the career outlook for security specialists over the long-term. The Commission believes that this area merits serious attention and should be charged to an expanded Defense Security Institute (see Recommendation 57).

The OPM Job Classification Standard for Security (GS-080) is seriously out-of-date and does not accurately or completely describe the elements which currently need to be included to cover today's civilian security specialists (and their military equivalents). Moreover, current DoD and OPM standards do not require that security staff and leadership positions be filled by qualified security professionals. This permits situations that are demoralizing to security professionals.

RECOMMENDATIONS:

62. The Secretary of Defense should request OPM to revise immediately the Classification Standard for Security (GS-080), to include comprehensive and accurately graded descriptions of all modern security disciplines integral to DoD security programs.

F. Program Oversight

Without continuing program oversight, there can be no assurance that policy is being translated into practice in the field. Within most DoD components, oversight mechanisms are in place, although their scope and effectiveness vary widely. At the top of the DoD security structure, however, program oversight is poor. While the Commission unanimously agreed that program oversight was appropriately a function of the OSD staff, very little oversight is being performed at that level due to lack of sufficient staff. For example, OSD staff rarely conducts component headquarters inspections, much less examines compliance of field

elements with DoD security policy. Similarly, in some components, shortfalls in staff often result in partial or incomplete implementation of DoD security policy at the operating activity level.

In industry, 225 DoD Industrial Security Representatives are inspecting on a periodic basis 13,000 cleared defense contractors to ensure compliance with industrial security requirements. Although the time spent by these inspectors at each cleared facility varies with the volume and level of cleared information possessed, as a practical matter, their inspections are necessarily circumscribed. The Commission concludes that this function is seriously understaffed.

G. Resource Management

The Commission did not delve in detail into the resource management aspects of the DoD security program, since it considered the subject tangential to its primary task. However, even on the basis of cursory examination, several conclusions are evident.

Some elements of counterintelligence and security are managed as separate programs or separate line-items in programs (e.g., foreign counterintelligence, background investigations, COMSEC); but counterintelligence and security is not "resource-managed" as an entity. Indeed, there appears no useful purpose served by attempting to do so. Many security expenditures are so deeply embedded in other budgets/programs (e.g., physical security, operation security) that attempting to isolate them would be a time-consuming and ultimately unrewarding exercise.

On the other hand, it may be prudent for DoD components to select for program management certain security elements which are not now programmed or budgeted as discrete line items but which involve large dollar expenditures. The objective would be to determine how resources are being spent and whether such expenditures are justified by the threat. The extent to which equipment is being shielded to prevent unintended emissions (TEMPEST) would appear to be a logical candidate since the costs of the requirement are estimated to run into the hundreds of millions of dollars annually. While TEMPEST protection may be essential in some overseas areas, the environment within the United States is dramatically different. Consequently, the once rigid TEMPEST policy was modified two years ago to prescribe shielding only when inspection verified that a threat existed. Yet, while the policy has changed, there is no means of verifying its implementation or impact.

Relatedly, there is no office in OSD which is charged with making assessments of the overall efficacy of the DoD security system and the relative balance among its several components. No office looks at counterintelligence and security resource expenditures as a whole (even those that are separately managed), or which looks at them in terms of the relative proportions of expenditures dedicated to the various security disciplines,

(e.g., how much is being spent on background investigations of personnel with access to automated information systems versus how much is being spent on the technical protection of such systems). The lack of this kind of evaluation could lead to funding levels being greatly disproportionate, in terms of their relative contribution to the overall DoD security program.

RESOURCE IMPACT

Implementation of the Commission's recommendations would have widely differing resource implications:

- Some could lead to substantial cost avoidance.
- Some could result in net savings.
- Some could require substantial added expenditures.
- Some could be simply inconvenient without representing added costs.

Overall, there is a price tag. The totality of enhancements recommended by the Commission will require more manpower and dollars than now allocated to security programs. Considering, however, overall defense expenditures as well as the monetary costs of successful espionage, these additional expenditures must be regarded as modest.

Precise estimates of net costs are not possible, since it is impossible to quantify the impact of either those recommendations which should save money, or those which will require it. In the area of personnel investigations, for example, recommendations 1-5 should logically result in fewer background investigations (and reinvestigations) being requested, although the magnitude of such reductions remains to be determined. In addition, it stands to reason that implementation of Recommendation 10 (which applies the procedures used for interim SECRET clearances to the processing of all such clearances) should mean considerable savings to the Department overall, eliminating production delays while employees and contractors are waiting for security clearances.

On the other hand, Recommendations 8, 9, and 14 call for significantly more investigations than are now being conducted (e.g., an expanded investigative scope for SECRET; higher numbers of investigations). It is clear that with respect to DIS, substantially more resources will be required than are now programmed.

The bulk of additional funds will be required for production of communications security equipment and research in automated information systems security. More modest amounts would be required for other categories of research, training, oversight, and the administrative costs associated with some of the Commission's recommendations (e.g., establishing a TOP SECRET billet system, PRP-type reliability programs, accounting for SECRET materials, supervisory appraisals).

In large part, these additional costs could be offset if DoD components would simply comply with the policy changes described above with respect to the purchase of "TEMPEST-approved" electronic equipment for use within the United States. Many defense contractors told the Commission that DoD components were continuing to require them to purchase shielded equipment, notwithstanding the recent policy change, at substantially higher costs than unshielded equipment. DoD components could also be reducing their own procurement costs substantially by complying with the stated policy.

In any case, it is clear that for those recommendations which are approved and have budgetary impacts, DoD components must begin to program and budget the enhancements needed to implement them. This process should begin upon approval by the Secretary.

RECOMMENDATION:

63. Recommendations of the Commission which require resource enhancements should be accommodated, as appropriate, by reprogramming in FY 1986 or FY 1987, incorporation in the Program Objectives Memoranda for FY 1988, or in the current Defense Guidance.

CONCLUSION

While no system of security can provide foolproof protection against espionage, it can make espionage more difficult to undertake and more difficult to accomplish without detection. In this respect, DoD's current security program falls short of providing as much assurance as it might that the nation's defense secrets are protected.

The Commission believes that increased priority must be accorded DoD security efforts. More resources should be allocated to security, even at the expense of other DoD programs. New safeguards must be added, and many old ones improved, even at a cost to operational efficiency. This is not to say that some resources cannot be saved or operational efficiency enhanced by eliminating burdensome and unproductive security requirements. Indeed, a number of such changes are recommended by the Commission. But, on the whole, DoD must be willing to pay a higher price, in terms of both resources and operational convenience, to protect its classified information.

The Commission arrives at this conclusion mindful that security plays only a supporting role in the successful accomplishment of DoD's operational mission. But the success of any classified project or operation must be judged short-lived at best if, at the same time, the results have been revealed to potential adversaries, who are enabled to develop countermeasures at a more rapid pace than otherwise. As bureaucratic and mundane as security sometimes appears, it offers the only systematic means available to protect and preserve the defense community's triumphs and advances over time. Security must be given its fair share of serious attention and its fair share of resources.

APPENDIX A

PERSONS WHO TESTIFIED BEFORE THE COMMISSION

Robert Allen	Director, Navy Security Policy
Maynard Anderson	Director, Security Plans and Programs, ODUSD(P)
[redacted]	STAT Chief, Polygraph and Personnel Security Research, National Security Agency
Allan Becker	Research Security Coordinator, Georgia Institute of Technology
Arthur E. Brown, Lieutenant General, US Army	Director of the Army Staff
Americo R. Cinquegrana	Deputy Counsel for Intelligence Policy, Office of Intelligence Policy and Review, Department of Justice
Donald Doll	Chairman of the Industrial Security Committee, Aerospace Industries Association of America
John F. Donnelly	Director, Counterintelligence and Investigative Programs ODUSD(P)
Richard E. Elster	Deputy Assistant Secretary of the Navy (Manpower)
Andrew Feinstein	Chief Counsel and Staff Director, Subcommittee on Civil Service, Committee on Post Office and Civil Service, US House of Representatives
STAT [redacted]	Chief, Multi-Discipline Counterintelligence Branch, Counterintelligence Division, Defense Intelligence Agency

Eli S. Flyer	Consultant to the Counterintelligence and Investigative Programs Directorate, ODUSD(P)
Daniel R. Foley	Deputy Assistant Inspector General for Investigations, DoD
Steve Garfinkel	Director, Information Security Oversight Office
Joseph S. Greene, Colonel, US Air Force	Deputy Director, National Computer Security Center
John Hancock	Chief, Programs Management and Physical and Information Security Division, Defense Investigative Service
Theodore G. Hess, Lieutenant Colonel, US Marine Corps	Special Assistant for Intelligence, Department of Defense, Legislative Affairs, OSD
Eleanore Hill	Minority Counsel, Senate Permanent Subcommittee on Investigations
	STAT Chairman, DCI Security Committee
	Soviet KGB Defector STAT
Guenther Lewy	Professor of Political Science, University of Massachusetts
John L. Martin	Chief, Internal Security Section, Criminal Division Department of Justice
Joseph Murphy	Deputy Director of Security, Central Intelligence Agency
Daniel Nauer	Aerospace Industries Association of America
Thomas J. O'Brien	Director, Defense Investigative Service

Phillip A. Parker	Deputy Assistant Director of the Intelligence Division, Federal Bureau of Investigation
George Paseur	Director, Information Security, Office of Security Police, Headquarters US Air Force
[redacted]	Chief, COMSEC Policy and Threat Analyses, National Security Agency
[redacted]	Director of Security, National Security Agency
John H. Shenefield	Member of the American Bar Association Standing Committee on Law and National Security
L. Britt Snider	Principal Director, Counterintelligence and Security Policy, ODUSD(P)
William O. Studeman, Commodore, US Navy	Director of Naval Intelligence
Francis X. Taylor, Lieutenant Colonel, US Air Force	Deputy Director for Operations, Counterintelligence and Investigative Programs Directorate, ODUSD(P)
James A. Williams, Lieutenant General, US Army	Director, Defense Intelligence Agency

STAT

STAT

APPENDIX B

SENIOR INDUSTRY OFFICIALS INTERVIEWED

BY THE COMMISSION

William H. Borten
President and Chief Operating Officer
Atlantic Research Corporation

Norman C. Witbeck
President
Columbia Research Corporation

Joseph V. Charyk
Chairman and Chief Executive Officer
COMSAT (Communications Satellite Corporation)

John W. Dixon
Chairman and Chief Executive Officer
E-Systems, Inc.

Henry Ross Perot
Chairman
Electronic Data Systems Corporation

Vince Cook
President
International Business Machines
Federal Systems Division

Frank J. Lewis
Senior Vice President
Harris Corporation

Robert Kirk
President and Chief Executive Officer
LTV Aerospace and Defense Company

Franc Wertheimer
President
ManTech International Corporation

Thomas G. Pownall
Chairman and Chief Executive Officer
Martin Marietta Corporation

Sanford McDonnell
Chairman
McDonnell Douglas Corporation

Thomas V. Jones
Chairman of the Board and Chief Executive Officer
Northrop

Wayne V. Shelton
President and Chief Operating Officer
Planning Research Corporation

Frederick F. Jenny
President and Chief Executive Officer
System Development Corporation

Ronald L. Easley
Chairman of the Board
System Planning Corporation

Jerry R. Junkins
President
Texas Instruments Incorporated

Sanitized Copy Approved for Release 2010/02/23 : CIA-RDP87M01152R000200130004-7

APPENDIX C

SENIOR INDUSTRY OFFICIALS WHO PROVIDED WRITTEN COMMENTS TO THE COMMISSION

Jack L. Heckel
Chairman
Aerojet General

T. A. Wilson
Chairman of the Board
The Boeing Company

J. A. Pikulas
Director, Administrative Services
Chrysler Corporation

J. J. Bussolini
Vice President
Grumman Aerospace Corporation

Carl D. Thorne
Vice President
Finance and Administration
Computer Sciences Corporation

Charles M. Williams
President
EG&G Washington Analytical
Services Center, Inc.

Emanuel Fthenakis
President
Fairchild Industries, Inc.

N. R. Duff
Vice President
Industrial Relations Staff
Ford Aerospace & Communications
Corporation

O. C. Boileau
President
General Dynamics Corporation

E. E. Hood, Jr.
Vice Chairman of the Board
General Electric

Boyd T. Jones
President
Control Data Corporation

John A. Young
President and Chief Executive Officer
Hewlett-Packard Company

Warde F. Wheaton
Executive Vice President
Aerospace and Defense
Honeywell

Allen E. Puckett
Chairman of the Board and
Chief Executive Officer
Hughes Aircraft Company

William G. McGowan
Chairman of the Board and
Chief Executive Officer
MCI Communications Corporation

Thomas L. Phillips
Chairman
Raytheon Company

Jack L. Bowers
Chairman and Chief Executive Officer
Sanders Associates, Inc.

Lawrence J. Howe, CPP
Vice President
Corporate Security
Science Applications International
Corporation

J. J. Yglesias
Chairman and Chief Executive Officer
SYSCON Corporation

John W. Pauly
Chief Executive Officer
Systems Control Technology, Inc.

Robert C. Gormley
President
Vitro Corporation

J. B. Toomey
President
VSE Corporation

Douglas D. Danforth
Chairman
Westingthouse Electric Corporation

Donald R. Beall
President and Chief Operating Officer
Rockwell International Corporation

APPENDIX D

THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

28 AUG 1985

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE (POLICY)
ASSISTANT SECRETARY OF DEFENSE (FORCE MANAGEMENT AND PERSONNEL)

SUBJECT: Security Evaluation of DoD Personnel with Access to Classified Information

The proper handling and protection of classified information are vital to the accomplishment of the mission of the Department of Defense. Each DoD member whose duties involves access to classified information must perform these functions in a manner ensuring the integrity of the information. Analysis of this matter within the Department of Defense reveals the need to increase supervisory attention to the trustworthiness of personnel for access to classified information and duties involving the handling and safeguarding of classified information.

Accordingly, prior to October 1, 1985 take the necessary action to incorporate the following requirements in appropriate regulations:

(1) Incorporate the following specific matters in regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information:

(a) Whether the supervisor is aware of any action, behavior or condition that would constitute a reportable matter under the respective department/agency's security regulations governing eligibility for access to classified information. If the response is affirmative, the supervisor should further indicate whether an appropriate report has been made.

(b) Comments regarding an employee's discharge of security responsibilities.

(2) Establish procedures to require a review by the immediate supervisor of the DD Form 398 (Statement of Personal History (SPH)) and related information submitted by employees in connection with a request for a periodic reinvestigation. Immediate supervisors will review the Statement of

Personal History to determine if any relevant personnel security information (in terms of the criteria delineated in paragraph 2-200, DoD Regulation 5200.2R) of which the supervisor is aware has been excluded. If the supervisor is unaware of any such additional information pertaining to the individual, the supervisor will append a certification to that effect on the SPH. However, If the supervisor is aware of such additional information, that fact will be reported in writing by the supervisor to the cognizant security adjudicative authority. This report should include any information provided by the subject by way of clarification or mitigation as well as any additional information known by the supervisor that is pertinent to the continued eligibility of the subject for access to classified information.

Initially, this requirement may be met by ad hoc procedures and entries. However, they should be incorporated in appropriate regulations and forms at the earliest practicable opportunity.

Provide for appropriate DoD components to report actions to implement these requirements to the Under Secretary of Defense for Policy by November 15, 1985.

William H. Taft, IV
Deputy Secretary of Defense

APPENDIX E

THE SECRETARY OF DEFENSE

WASHINGTON THE DISTRICT OF COLUMBIA

25 JUN 1985

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL
INSPECTOR GENERAL
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DEPUTY ASSISTANT SECRETARY OF DEFENSE (ADMINISTRATION)

SUBJECT: Commission to Review and Evaluate DoD Security Policies and Procedures

This memorandum is a follow-on to my recent announcement of the establishment of a Commission to conduct a review and evaluation of Department of Defense security policies and procedures. The Commission will identify any systemic vulnerabilities or weaknesses in DoD security programs, including an analysis of lessons learned from incidents which have occurred recently, and make recommendations for change, as appropriate. The Terms of Reference for the Commission is attached.

General Richard G. Stilwell, USA (Ret.), is hereby appointed to chair the Commission which shall be comprised of cognizant senior officials of the Office of the Secretary of Defense, Military Departments, Defense Agencies, and a representative from defense industry. Addressees should lend full cooperation to this important effort and provide personnel and information, as requested, to support the Commission's analysis and facilitate the early completion of the review.

A report of findings and recommendations will be submitted to me within 120 days of this date.

Attachment

Terms of Reference

Commission To Review DoD Security Policies and Procedures

The Commission will be responsible for conducting a review and evaluation of Department of Defense security policies and procedures, identify weaknesses, and make recommendations for change, as appropriate.

Membership

General Richard G. Stilwell, USA (Ret)	Chairman
Lt. Gen. Arthur E. Brown	Dir, Army Staff
R. Adm. John L. Butts	Dir, Naval Intelligence
Mr. Chapman B. Cox	DoD General Counsel
Mr. William O. Cregar	Dir, Security, E. I. duPont deNemours & Co.
Lt. Gen. Monroe W. Hatch	Inspector General, USAF
Mr. Robert W. Helm	ASD(Comptroller)
Dr. Fred C. Ikle	USD(Policy)
Dr. Lawrence J. Korb	ASD(MI&L)
Adm. Robert L. J. Long, USN (Ret)	
Lt. Gen. William E. Odom	Dir, NSA
Lt. Gen. Winston D. Powers	Dir, DCA
Lt. Gen. James A. Williams	Dir, DIA

Functions

- Examine existing DoD security policies and procedures.
- Review recent security incidents and reported deficiencies, with particular emphasis on potential vulnerabilities.
- Interview cognizant DoD officials and other individuals who are in a position to shed light on the areas under consideration.
- Examine DoD-wide security organizations and systems, to the extent required.
- Identify deficiencies in policies and systems and develop corrective actions which will accomplish the necessary improvements.
- Prepare a report of findings and recommendations for the Secretary of Defense.

Reporting

A report will be submitted to the Secretary of Defense not later than 120 days from the establishment of the Commission.

Terms of Reference

Commission To Review DoD Security Policies and Procedures

The Commission will be responsible for conducting a review and evaluation of Department of Defense security policies and procedures, identify weaknesses, and make recommendations for change, as appropriate.

Membership

General Richard G. Stilwell, USA (Ret)	Chairman
Lt. Gen. Arthur E. Brown	Dir, Army Staff
R. Adm. John L. Butts	Dir, Naval Intelligence
Mr. Chapman B. Cox	DoD General Counsel
Mr. William O. Cregar	Dir, Security, E. I. duPont deNemours & Co.
Lt. Gen. Monroe W. Hatch	Inspector General, USAF
Mr. Robert W. Helm	ASD(Comptroller)
Dr. Fred C. Ikle	USD(Policy)
Dr. Lawrence J. Korb	ASD(MI&L)
Adm. Robert L. J. Long, USN (Ret)	
Lt. Gen. William E. Odom	Dir, NSA
Lt. Gen. Winston D. Powers	Dir, DCA
Lt. Gen. James A. Williams	Dir, DIA

Functions

- Examine existing DoD security policies and procedures.
- Review recent security incidents and reported deficiencies, with particular emphasis on potential vulnerabilities.
- Interview cognizant DoD officials and other individuals who are in a position to shed light on the areas under consideratio
- Examine DoD-wide security organizations and systems, to the extent required.
- Identify deficiencies in policies and systems and develop corrective actions which will accomplish the necessary improvements.
- Prepare a report of findings and recommendations for the Secretary of Defense.

Reporting

A report will be submitted to the Secretary of Defense not later than 120 days from the establishment of the Commission.

STATEMENT OF STEVEN GARFINKEL
DIRECTOR, INFORMATION SECURITY OVERSIGHT OFFICE
BEFORE THE
SENATE SELECT COMMITTEE ON INTELLIGENCE

NOVEMBER 20, 1985

MR. CHAIRMAN, MR. VICE CHAIRMAN, AND MEMBERS OF THE COMMITTEE,

I WELCOME THE OPPORTUNITY TO DISCUSS WITH YOU TODAY THE INITIATIVES THAT I HAVE RECOMMENDED TO THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS TO IMPROVE THE GOVERNMENT-WIDE INFORMATION SECURITY SYSTEM. I AM ALSO PLEASED TO INFORM YOU THAT THE ADMINISTRATION WELCOMES THE COMMITTEE'S INPUT ON THESE OR OTHER INITIATIVES THAT IT MAY PROPOSE.

AS I INDICATED IN MY EARLIER STATEMENT TO THE COMMITTEE, THE AGENCIES MOST INVOLVED WITH NATIONAL SECURITY INFORMATION WORKED WITH THE INFORMATION SECURITY OVERSIGHT OFFICE, OR ISOO, IN DEVELOPING THESE INITIATIVES. AS SOON AS THEY RECEIVE WHITE HOUSE APPROVAL, ISOO WILL COMMENCE THE ACTIONS NECESSARY TO PUT THEM INTO EFFECT. AS YOU WILL NOTE, THE DIFFERENT INITIATIVES REQUIRE VARIOUS MEANS OF IMPLEMENTATION, RANGING FROM THE AMENDMENT OF EXECUTIVE ORDER 12356, "NATIONAL SECURITY INFORMATION," TO THE TRANSMITTAL OF LETTERS WITHIN THE EXECUTIVE BRANCH. NO MATTER WHAT THE MEANS OF IMPLEMENTATION, THESE INITIATIVES WILL APPLY TO EVERY AGENCY THAT CREATES OR HANDLES CLASSIFIED INFORMATION.

IN THIS CONTEXT I EMPHASIZE THAT THE ISOO INITIATIVES DO NOT CONFLICT IN ANY RESPECT WITH THE RECOMMENDATIONS CONTAINED IN THE EXCELLENT REPORT PRODUCED BY THE DEPARTMENT OF DEFENSE SECURITY REVIEW COMMISSION. IN SEVERAL INSTANCES THE COMMISSION'S RECOMMENDATIONS PARALLEL THE ISOO INITIATIVES, AND IN EVERY OTHER INSTANCE THE COMMISSION'S INFORMATION SECURITY RECOMMENDATIONS AND THE ISOO INITIATIVES ARE COMPLEMENTARY.

THE ISOO INITIATIVES DO NOT ALTER THE BASIC STRUCTURE OF THE INFORMATION SECURITY SYSTEM. THE MEMBERS OF OUR INTERAGENCY WORKING GROUP UNANIMOUSLY AGREED THAT THE STRUCTURE OF THE SYSTEM ESTABLISHED BY PRESIDENT REAGAN IN 1982, IS FUNDAMENTALLY SOUND AND, FOR THE MOST PART, WORKING QUITE WELL. RATHER, THESE INITIATIVES SEEK INCREASED KNOWLEDGE AND INCREASED ACCOUNTABILITY AMONG THE MANY PEOPLE WHO ARE ENTRUSTED WITH MAKING THE SYSTEM WORK AS IT SHOULD. ALTHOUGH THESE INITIATIVES ARE FEW IN NUMBER AND QUITE MODEST IN COST, ISOO FIRMLY BELIEVES THAT THEIR IMPLEMENTATION SHOULD HAVE FAR-REACHING CONSEQUENCES FOR THE IMPROVEMENT OF THE INFORMATION SECURITY SYSTEM.

THE RECOMMENDED INITIATIVES ATTACK PERCEIVED PROBLEMS IN FIVE SUBJECT AREAS. THESE INCLUDE OVERCLASSIFICATION, OR UNNECESSARY CLASSIFICATION; THE OVERDISTRIBUTION OF CLASSIFIED INFORMATION; THE MANAGEMENT OF CLASSIFIED INFORMATION; THE EROSION OF THE "NEED-TO-KNOW" PRINCIPLE; AND UNAUTHORIZED DISCLOSURES.

THE PLACEMENT OF OVERCLASSIFICATION AS THE FIRST PROBLEM AREA WAS INTENTIONAL. ALTHOUGH THE PROBLEM OF OVERCLASSIFICATION IS NOT NEARLY AS SEVERE AS THE POPULAR MEDIA WOULD LEAD US TO BELIEVE, IT IS A CONTINUING NUISANCE THAT EATS AWAY AT THE CREDIBILITY OF THE ENTIRE SYSTEM. CRITICS TELL US THAT OVERCLASSIFICATION IS THE MECHANISM WE USE TO HIDE OUR MISTAKES, TO SHIELD US FROM EMBARRASSMENT, AND TO COVER-UP OUR MISDEEDS. IN ISOO'S EXPERIENCE, THE PRINCIPAL CAUSES OF OVERCLASSIFICATION ARE FAR LESS INTRIGUING. VERY FEW CLASSIFICATION DECISIONS ARE THE PRODUCT OF A COVER-UP, ALBEIT EVEN ONE CASTS A SHADOW ON THE WHOLE SYSTEM. INSTEAD, I SUGGEST THAT ONE OR MORE OF THE FOLLOWING REASONS ACCOUNTS FOR JUST ABOUT EVERY INSTANCE OF INITIAL OVERCLASSIFICATION. FIRST, OVERCAUTION. MANY CLASSIFIERS BELIEVE, AND WITH SOME REASON, THAT IT IS BETTER TO ERR ON THE SIDE OF PROTECTION THAN ON THE SIDE OF DISCLOSURE. SECOND, ROTE CLASSIFICATION. IT IS ALMOST ALWAYS EASIER TO DO THINGS THE WAY THEY'VE BEEN DONE BEFORE. INDEPENDENT THOUGHT TAKES TIME AND EFFORT. THIRD, STATUS OR PRESTIGE CLASSIFICATION. SOME INDIVIDUALS BELIEVE THAT IT ELEVATES THEIR STATURE TO ELEVATE THE PROTECTION OF THEIR PRODUCT. FOR STATUS CLASSIFIERS, "CONFIDENTIAL" IS NEVER HIGH ENOUGH, AND "SECRET" IS ONLY TOLERABLE. FOURTH, AND RELATED TO STATUS CLASSIFICATION, IS WHAT I CALL EXCLUSIONARY CLASSIFICATION. THIS OCCURS WHEN AN OFFICIAL DECIDES THAT THE CLASSIFICATION OF HIS PRODUCT WILL ESTABLISH A MORE EXCLUSIVE ENVIRONMENT, FREE FROM ROUTINE OVERSIGHT.

FIFTH, INCORRECT, INADEQUATE OR NONEXISTENT CLASSIFICATION GUIDANCE. POOR GUIDANCE RESULTS IN INACCURATE DERIVATIVE CLASSIFICATION ACTIONS AND, QUANTITATIVELY, IS PROBABLY THE MOST SIGNIFICANT CAUSE OF OVERCLASSIFICATION. SIXTH, THE LACK OF PORTION MARKINGS IN DOCUMENTS USED AS SOURCES FOR DERIVATIVE CLASSIFICATION. IF THE ENTIRE TEXT OF A DOCUMENT IS CLASSIFIED, EVEN THOUGH SOME PORTIONS NEED NOT BE, DOCUMENTS DERIVED FROM THOSE PORTIONS WILL BE NEEDLESSLY CLASSIFIED. AGAIN, I SUGGEST THAT THESE SIX SITUATIONS ACCOUNT FOR ALMOST ALL INITIAL OVERCLASSIFICATION.

TO ATTACK THE PROBLEM OF OVERCLASSIFICATION, ISOO HAS PROPOSED THREE INITIATIVES. FIRST, ISOO PROPOSES TO ISSUE A DIRECTIVE THAT ESTABLISHES MINIMUM REQUIREMENTS FOR MANDATORY TRAINING OF ORIGINAL AND DERIVATIVE CLASSIFIERS, INCLUDING THE PROMULGATORS AND USERS OF CLASSIFICATION GUIDES. TOO OFTEN THESE OFFICIALS ARE RECEIVING LITTLE OR NO TRAINING ABOUT THE CLASSIFICATION SYSTEM AND PROCESS. ISOO WILL ALSO REQUIRE THAT AGENCIES KEEP RECORDS OF THE TRAINING THAT EACH OF THESE OFFICIALS RECEIVES.

SECOND, ISOO PROPOSES TO ISSUE A DIRECTIVE ON AGENCY SELF-INSPECTIONS THAT ESTABLISHES MINIMUM CRITERIA FOR INTERNAL OVERSIGHT. THIS DIRECTIVE WILL INCLUDE THE REQUIREMENT THAT AGENCIES PERIODICALLY AND ROUTINELY EXAMINE A SAMPLE OF THEIR CLASSIFIED PRODUCT TO ENSURE THE VALIDITY OF CLASSIFICATION AND

THE EXISTENCE OF APPROPRIATE MARKINGS. MOST CURRENT AGENCY SELF-INSPECTIONS CONCENTRATE ALMOST EXCLUSIVELY ON PHYSICAL SECURITY AND LARGELY IGNORE THE INFORMATION BEING PROTECTED.

THIRD, ISOO PROPOSES THAT THE PRESIDENT AMEND E.O. 12356 TO REQUIRE EMPLOYEES TO REPORT INSTANCES OF IMPROPER CLASSIFICATION. CURRENTLY, THE SYSTEM ENCOURAGES EMPLOYEES TO REPORT CLASSIFICATION ACTIONS THAT THEY BELIEVE TO BE INCORRECT. IN PRACTICE, THIS RARELY OCCURS. ISOO ALSO PROPOSES THAT THE ORDER BE AMENDED TO REQUIRE AGENCIES TO ESTABLISH EFFECTIVE PROCEDURES FOR EMPLOYEES TO CHALLENGE IMPROPER CLASSIFICATION FREE FROM THE FEAR OF RETALIATION. THE FEAR OF RETRIBUTION IS BELIEVED TO BE A PRIMARY REASON THAT EMPLOYEES AND CONTRACTORS ARE NOT CHALLENGING CLASSIFICATION DECISIONS TODAY. IN PROPOSING THIS INITIATIVE, ISOO RECOGNIZES THAT ITS ENACTMENT MAY RESULT IN MANY UNFOUNDED COMPLAINTS. THIS SEEMS TO ISOO TO BE A REASONABLE PRICE TO PAY FOR IMPROVING THE QUALITY OF OUR CLASSIFIED PRODUCT.

THE OVERDISTRIBUTION OF CLASSIFIED INFORMATION HAS BECOME A VERY SERIOUS PROBLEM IN RECENT YEARS. THE WIDESPREAD AVAILABILITY OF COPIERS AND AUTOMATED INFORMATION PROCESSING SYSTEMS HAS MULTIPLIED THE WHOLESALE DISTRIBUTION OF CLASSIFIED INFORMATION. INCREASED DISTRIBUTION RESULTS IN INCREASED SECURITY COSTS AND INCREASED VULNERABILITIES.

TO ATTACK THE PROBLEM OF OVERDISTRIBUTION, ISOO HAS PROPOSED THREE INITIATIVES. FIRST, ISOO PROPOSES THAT THE PRESIDENT ISSUE A STATEMENT TO THE HEADS OF AGENCIES THAT ADDRESSES, AMONG OTHER PROBLEM AREAS, THE OVERDISTRIBUTION OF CLASSIFIED INFORMATION. ISOO BELIEVES THAT A PRESIDENTIAL STATEMENT WILL HIGHLIGHT OVERDISTRIBUTION AS A PROBLEM THAT MERITS FAR MORE ATTENTION THAN IT HAS BEEN RECEIVING.

SECOND, ISOO PROPOSES TO AMEND ITS GOVERNMENT-WIDE DIRECTIVE TO REQUIRE AGENCIES TO REVIEW AT LEAST ANNUALLY THE AUTOMATIC OR ROUTINE DISTRIBUTION OF ALL CLASSIFIED INFORMATION. BOTH DISTRIBUTORS AND RECIPIENTS WOULD BE REQUIRED TO UPDATE AUTOMATIC DISTRIBUTION LISTS, AND DISTRIBUTORS TO VERIFY THE CONTINUING "NEED-TO-KNOW" OF RECIPIENTS. THIS INITIATIVE SHOULD REMEDY THE TOO FREQUENT SITUATION IN WHICH A ONCE BONA FIDE RECIPIENT IS PLACED ON AN AUTOMATIC DISTRIBUTION LIST AND CONTINUES TO RECEIVE THE CLASSIFIED PRODUCT OF THE DISTRIBUTOR.

THIRD, ISOO PROPOSES TO AMEND ITS GOVERNMENT-WIDE DIRECTIVE TO ENCOURAGE ORIGINATORS OF CLASSIFIED INFORMATION TO WIDEN CONTROLS ON ITS REPRODUCTION, UNLESS THERE ARE COUNTERVAILING REASONS TO PERMIT UNCONTROLLED REPRODUCTION. CURRENTLY, "TOP SECRET" INFORMATION MAY NOT BE REPRODUCED WITHOUT THE PERMISSION OF THE ORIGINATOR. ALTHOUGH ORIGINATORS MAY PLACE SIMILAR CONTROLS ON THE REPRODUCTION OF "SECRET" AND "CONFIDENTIAL" INFORMATION, THEY RARELY DO SO. WITH COPIERS AVAILABLE IN JUST ABOUT EVERY OFFICE,

COPIES OF CLASSIFIED DOCUMENTS PROLIFERATE. THIS INITIATIVE SHOULD INCREASE BOTH CONTROL AND ACCOUNTABILITY, AND REDUCE THE OVERDISTRIBUTION OF NATIONAL SECURITY INFORMATION.

ISOO TERMED THE THIRD PROBLEM AREA "CLASSIFICATION MANAGEMENT." IN ISOO'S DEFINITION OF THIS TERM, IT REFERS BROADLY TO THE MANAGEMENT OF CLASSIFIED INFORMATION BY CLASSIFIERS, SECURITY SPECIALISTS, AND OTHERS WHOSE WORK HAS A SIGNIFICANT IMPACT UPON ITS CREATION AND HANDLING. BECAUSE IT IS A GENERAL TERM, THE INITIATIVES THAT ISOO IS PROPOSING IN THIS AREA IMPACT AS WELL ON EACH OF THE OTHER PROBLEM AREAS.

FIRST, ISOO PROPOSES THAT THE PRESIDENT AMEND E.O. 12356 TO IDENTIFY THE MANAGEMENT OF CLASSIFIED INFORMATION AS AN AREA REQUIRING AGENCY HEAD ATTENTION. SPECIFICALLY, THIS INITIATIVE WOULD REQUIRE THAT THE RESPONSIBILITIES FOR MANAGING CLASSIFIED INFORMATION BE INCLUDED AS CRITICAL ELEMENTS IN THE PERFORMANCE RATING SYSTEMS OF CIVILIAN AND MILITARY PERSONNEL WHO ARE ORIGINAL CLASSIFIERS, SECURITY MANAGERS, OR WHO ARE OTHERWISE SIGNIFICANTLY INVOLVED IN MANAGING CLASSIFIED INFORMATION. PERHAPS MORE THAN ANY OTHER, THIS INITIATIVE WILL CONFIRM THAT PERSONAL ACCOUNTABILITY IS THE MOST EFFECTIVE MEANS OF IMPROVING THE OPERATION OF THE INFORMATION SECURITY SYSTEM.

SECOND, ISOO PROPOSES THAT THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS CALL UPON THE DIRECTOR OF THE OFFICE OF PERSONNEL MANAGEMENT TO REVIEW AND REVISE THE SECURITY SPECIALIST POSITION SERIES, TO INCLUDE PROPER RECOGNITION FOR THE SPECIAL SKILLS NECESSARY FOR THE MANAGEMENT OF CLASSIFIED INFORMATION. IN MANY RESPECTS SECURITY SPECIALISTS OCCUPY THE LOWEST RUNG OF THE PROFESSIONAL LADDER. THEY RECEIVE LITTLE RESPECT, LOW SALARIES, AND FEW OPPORTUNITIES FOR ADVANCEMENT. ALL TOO OFTEN THE BEST PEOPLE LEAVE THE SECURITY FIELD AS QUICKLY AS THEY CAN. AS A SOCIETY WE ARE BEGINNING TO APPRECIATE THE IMPORTANCE OF MOTIVATED, COMPETENT SECURITY PERSONNEL. THIS INITIATIVE IS INTENDED TO IMPROVE THE PROFESSIONAL STANDING OF SECURITY SPECIALISTS, SO THAT WE CAN ATTRACT AND RETAIN BETTER PEOPLE TO PERFORM THESE CRITICAL JOBS.

THIRD, ISOO PROPOSES THAT THE PRESIDENT DIRECT THE SECRETARY OF DEFENSE TO STUDY THE FEASIBILITY OF EXPANDING THE DEFENSE SECURITY INSTITUTE TO PROVIDE BASIC TRAINING FOR ALL EXECUTIVE BRANCH SECURITY PERSONNEL. SECURITY EDUCATION PLAYS A FUNDAMENTAL ROLE IN ASSURING THE EFFECTIVENESS OF THE INFORMATION SECURITY PROGRAM. TODAY, HOWEVER, BASIC SECURITY TRAINING IS NOT ALWAYS AVAILABLE TO THOSE WHO NEED IT. THE DEFENSE SECURITY INSTITUTE OFFERS AN EXISTING SCHOOL WITH EXCELLENT INSTRUCTORS IN THE NECESSARY SECURITY DISCIPLINES. THE DEMAND FOR ITS COURSES FAR EXCEEDS ITS CURRENT CAPACITIES. TO INCREASE THE INSTITUTE'S

COURSE OFFERINGS AND ENROLLMENT, THE SECRETARY OF DEFENSE SHOULD HAVE THE OPTION OF SEEKING REIMBURSEMENT FROM THE AGENCIES WHOSE EMPLOYEES AND CONTRACTORS WOULD BENEFIT FROM ITS EXPANSION.

THE CRITERIA FOR ACCESS TO CLASSIFIED INFORMATION HAVE LONG BEEN THE CLEARANCE PLUS THE "NEED-TO-KNOW". WITH THE PROLIFERATION OF CLEARANCES, RELIANCE UPON "NEED-TO-KNOW" BECOMES EVEN MORE CRITICAL. INSTEAD, WE HAVE BEEN WITNESSING WIDESPREAD INDIFFERENCE TO THIS PRINCIPLE. IN ISOO'S VIEW, THE OBVIOUS SECURITY THREAT IS NOT THE ONLY UNFORTUNATE CONSEQUENCE OF THE RELAXED ENFORCEMENT OF THE "NEED-TO-KNOW" PRINCIPLE. ANOTHER IS THE INCREASING USE BY AGENCIES OF SPECIAL ACCESS PROGRAMS TO HELP PROTECT CLASSIFIED INFORMATION. THESE PROGRAMS HAVE ALL TOO OFTEN SUBSTITUTED FOR THE ABSENCE OF ENFORCED "NEED-TO-KNOW".

THE INITIATIVES THAT ISOO HAS PROPOSED TO ATTACK THE OVERDISTRIBUTION OF CLASSIFIED INFORMATION SHOULD ALSO SERVE TO REVITALIZE THE "NEED-TO-KNOW" PRINCIPLE. IN ADDITION, ISOO SEEKS TWO OTHER INITIATIVES. FIRST, ISOO PROPOSES THAT THE PRESIDENT ISSUE A STATEMENT TO AGENCY HEADS THAT STRESSES THE IMPORTANCE OF REVITALIZING THE "NEED-TO-KNOW" PRINCIPLE. TO AVOID DUPLICATION, THIS WOULD BE PART OF THE PRESIDENTIAL STATEMENT PROPOSED BY ANOTHER INITIATIVE.

SECOND, ISOO PROPOSES THAT THE PRESIDENT AMEND E.O. 12356 TO REQUIRE AGENCY HEADS TO ENSURE EFFECTIVE INTERNAL OVERSIGHT OF SPECIAL ACCESS PROGRAMS, INCLUDING PERIODIC RECONFIRMATION OF THEIR CONTINUED NEED. AT PRESENT, MANY SPECIAL ACCESS PROGRAMS ACTUALLY RECEIVE LESS SECURITY OVERSIGHT THAN COLLATERAL PROGRAMS. IN ADDITION, A NUMBER OF THESE PROGRAMS ARE PROBABLY UNNECESSARY. THIS INITIATIVE AIMS FOR BOTH IMPROVED SECURITY AND INCREASED SCRUTINY OF THESE COSTLY PROGRAMS.

THE FIFTH AND FINAL PROBLEM AREA THAT THE INTERAGENCY GROUP EXAMINED WAS THAT OF UNAUTHORIZED DISCLOSURES. BECAUSE IT IS A SUBJECT THAT HAS BEEN EXPLORED REPEATEDLY IN RECENT YEARS, WE ARE PROPOSING ONLY TWO INITIATIVES. FIRST, ISOO PROPOSES THAT IT COORDINATE WITH THE SECURITY COMMITTEE OF THE INTELLIGENCE COMMUNITY IN THE DEVELOPMENT OF EDUCATIONAL MATERIALS, BOTH UNCLASSIFIED AND CLASSIFIED, THAT ADDRESS THE DAMAGE CAUSED BY UNAUTHORIZED DISCLOSURES. ISOO IS PARTICULARLY INTERESTED IN THE DEVELOPMENT OF EFFECTIVE, UNCLASSIFIED MATERIALS, ALTHOUGH WE RECOGNIZE THAT THE PRODUCTION OF THESE IS A FAR MORE DIFFICULT TASK WHEN WE MAY NOT USE CLASSIFIED EXAMPLES.

SECOND, ISOO PROPOSES THAT THE PRESIDENT CALL UPON THE ATTORNEY GENERAL TO REVIEW AND REVISE EXISTING GUIDELINES ON THE INVESTIGATION OF UNAUTHORIZED DISCLOSURES. THESE GUIDELINES WOULD COVER BOTH INTERNAL AGENCY INVESTIGATIONS AND EXTERNAL

INVESTIGATIONS BY THE DEPARTMENT OF JUSTICE AND FEDERAL BUREAU OF INVESTIGATION. CURRENTLY, INVESTIGATIONS OF UNAUTHORIZED DISCLOSURES RARELY LEAD TO SUCCESSFUL PROSECUTIONS OR EVEN ADMINISTRATIVE SANCTIONS. IT IS HOPED THAT REVISED INVESTIGATIVE GUIDELINES MAY IMPROVE UPON THIS RECORD.

MR. CHAIRMAN, MR. VICE CHAIRMAN, AND MEMBERS OF THE COMMITTEE, I HAVE NOW DESCRIBED THE THIRTEEN INITIATIVES THAT I HAVE PROPOSED TO THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS TO IMPROVE THE INFORMATION SECURITY SYSTEM. I BELIEVE THAT THEY REPRESENT A GOOD FAITH EFFORT TO REMEDY SOME SERIOUS PROBLEMS IN THE IMPLEMENTATION OF WHAT IS A VERY GOOD INFORMATION SECURITY SYSTEM. I LOOK FORWARD TO YOUR COMMENTS AND SUGGESTIONS.

SENATE SELECT COMMITTEE ON INTELLIGENCE

20 November 1985
0930-1200

"Personnel and Information Security"

WITNESS LIST

25X1 [redacted]	Director, Intelligence Community Staff
GEN Richard G. Stilwell, USA (Retired)	Chairman, Defense Security Review Commission
Mr. Steven Garfinkel	Director, Information Security Oversight Office, GSA
Mr. Craig Alderman	Deputy Under Secretary of Defense for Policy
25X1 [redacted]	Director, Office of Security, NSA

ACCOMPANIED BY:

Miss Eloise R. Page	Deputy Director, Intelligence Community Staff
Mr. L. Britt Snider	Director, Counterintelligence and Security Policy, Office of the Deputy Under Secretary of Defense for Policy
CAPT George L. Jackson, USN	Staff Director, Defense Security Review Commission
Mr. Fred Hutchinson	NIO for Foreign Denial and Intelligence Activities, CIA
Mr. Tom O'Brien	Director, Defense Investigative Service
[redacted]	Chief, Security Committee, ICS

25X1

ALSO ATTENDING:

Mr. Charles A. Briggs	Chief, Office of Legislative Liaison, CIA
Mr. Dave Major	National Security Council
Lt Col Ted Hess, USMC	Office of Legislative Affairs, OSD
Mr. Dan Carlin	Chief, Technical Security, Department of State
Mr. Forest Singhoff	Chief, Community Counterintelligence Staff
25X1 [redacted]	Legislative Affairs Office, NSA
Ms. Ethel Tneis	Senior Program Analyst, Information Security Oversight Office, GSA
25X1 [redacted]	Chief, Information Security, NSA
	Legislative Liaison, Intelligence Community Staff

14 NOV 1985

SECRET

Statement on Personnel Security for
Senate Select Committee on Intelligence
by the Chairman, DCI Security Committee

Personnel security is the sine qua non of any effective security program. Without strong personnel security, expensive programs to provide physical, technical, communications and information security will be ineffectual. Counterintelligence measures can support but cannot substitute for a balanced personnel security program. Recent espionage cases demonstrate vividly that a cleared insider working for the opposition can overcome virtually every effort to protect the secrets which are vital to our nation's defense and survival.

Although absolute secrecy 100% of the time is an unattainable goal, there are effective ways to identify potentially unreliable individuals and deny them access to classified information, to discourage breaches of security by those who have been cleared, and to uncover those cleared individuals who have breached security before they have caused irremediable damage. Counter-intelligence operations can be effective against the cleared insider, but only when we have thoroughly penetrated the hostile service to which he is providing information.

U.S. Government personnel security programs are based upon Executive Order 10450, which makes department and agency heads responsible for their operation. The execution of these programs will vary, depending upon management priorities, resource constraints and other factors not directly related to security. The investigations conducted by the Departments of State and Defense, the Federal Bureau of Investigation and the Office of Personnel

Management may vary in scope and thoroughness. Unmanageable backlogs of cases result in decrements in the quality of investigative programs. They cause managers to search for shortcuts. Investigative coverage may be curtailed when it should be expanded.

There is nothing mysterious about personnel security. In essence, it is the decision to give an individual access to classified data, based upon the best information available about that individual's ability to safeguard the data. Inadequate or inferior information about the individual can lead only to inappropriate clearance actions.

Personnel security is the most manpower intensive of the security disciplines. It requires large numbers of investigators, polygraphers, analysts and adjudicators, and they must be people of keen insight, strong reasoning ability and excellent judgment. Even in totalitarian countries, the security screening process sometimes fails. In our open society, the job is infinitely more difficult, and we must try harder to avoid the Walkers, Whitworths, Kampileses, Boyces, Bells, Harpers, and others who would betray our secrets.

Clearance decisions may be affected by such considerations as resource constraints, management pressure for immediate clearances, and legal considerations. We have discussed the pitfalls of inadequately resourced clearance programs. It is debilitating to management to have people awaiting clearances who are needed immediately to work on vital projects. Their impatience is understandable, but it doesn't enhance the quality of the personnel security program.

The personnel security program has been weakened by legal and societal changes. Access to criminal history records at various levels of government is being denied to non-law enforcement investigative organizations with substantial security responsibilities. Legislation may be needed to make available once again such records, which are essential to informed decisions on security clearances. The Merit Systems Protection Board recently decided it did not have the authority to review (and reverse) security clearance decisions. Prior to that decision, the possibility of an external review by a body not responsible for security had a chilling effect upon those charged with making clearance decisions. Recent trends toward public release of information from investigative files has unquestionably affected the willingness of those interviewed by investigators to give derogatory information. The long term effect of such external factors upon personnel security programs is of considerable concern.

As mentioned earlier, personnel security standards and their implementation are not uniform throughout the government. In general, background investigations are conducted for access to Top Secret material. Secret clearances, in most cases, are granted on the basis of National Agency Checks (NACs), as are Confidential clearances. The absence of identifiable information on the subject of the investigation is presumed to be non-derogatory and to justify issuance of a clearance. In most cases, NACs will not even serve to detect an assumed identity.

This poses a particular threat to certain intelligence sources and methods. Overhead imagery, long held at the compartmented (SCI) level, has, in recent years, been partially decompartmented. The release of such data to

individuals cleared on the basis of an NAC, and who will remain cleared in perpetuity without a security revieiw, places that information at severe risk.

A recurring proposal to reduce the need for resources is the elimination of checks with educational institutions and with neighbors of the subject. Even though our mobile society makes it more difficult to interview knowledgeable neighbors, they often are the best sources of information on personality and character traits bearing upon eligibility and suitability for security clearance. For younger persons especially, the educational check should be exploited more, rather than less. A member of the Georgetown University faculty recently wrote an op-ed column in The Washington Post complaining that no investigator ever asked if the subject cheated, a certain indicator of trustworthiness.

Although department and agency heads operate their own clearance programs, there are special categories of intelligence which are subject to national policy. Pursuant to the National Security Act of 1947, which makes the Director of Central Intelligence (DCI) responsible for protecting intelligence sources and methods, and E.O. 12356, the DCI establishes programs to protect Sensitive Compartmented Information (SCI). Personnel security standards for access to SCI are promulgated under Director of Central Intelligence Directive 1/14, which applies to all recipients of SCI, including government employees, military personnel and contractors.

DCID 1/14 embodies the most vigorous personnel security standards in the U.S. Government. It requires a full background investigation of unequalled scope, periodic reinvestigations, and the application of stringent adjudicative criteria in determining elegibility for access to SCI.

Because the standards of DCID 1/14 are applied in several agencies of the Intelligence Community, the SECOM conducts week-long seminars for adjudicators from throughout the Community. Their purpose is to encourage homogeneity in the application of the standards, to afford the adjudicator a broad view of the security decision process for SCI, and to encourage interagency dialogue on personnel security matters. More than 400 adjudicators have attended these seminars, and each presentation is oversubscribed, indicating its perceived value to the Community. It is the only Community-wide personnel security education program in existence.

DCI Directive 1/14 authorizes polygraph testing as a prerequisite in those agencies which have polygraph programs. Until now, this has meant CIA and NSA, in practical terms. The President has now issued NSDD 196, which establishes as policy the use of counterintelligence-scope polygraph examinations for all individuals with access to SCI and certain other designated data. This policy should significantly upgrade the personnel security program for SCI. Such a policy has been considered and sharply debated in the DCI Security Committee, which formulates DCID 1/14 for the DCI's approval. Opposition to adoption of such a policy has rested primarily on the nonexistence of polygraph programs in most of the government. Presumably, such programs will now be developed.

Polygraph testing for all SCI recipients is a fair and rational policy. The intelligence information received by an official of the Department of Agriculture has the same potential for compromising sources and methods as it did in the hands of an NSA or CIA employee. The same standards should apply to all persons receiving SCI.

A study conducted in 1980 under Security Committee auspices demonstrated that the polygraph was, for those agencies using it, the single most productive source of adverse security data supporting denials of security clearance. There are areas in the life histories of candidates for security clearance that cannot always be explored thoroughly by background investigations. Today, more than ever, people spend significant periods of time overseas as a result of military, government or private business assignments, or on personal travel. We can't always or with reasonable expenditure of effort determine what those people did overseas that might be of security concern. Drug usage by employees or prospective employees is frequently impossible to detect through normal investigation because of the consensual nature of drug transactions. Involvement in unauthorized disclosures or unauthorized removal of classified documents are usually not detectible through investigation. The polygraph is indispensable for identifying security problems in such areas. The source is unimpeachable - the individuals involved, themselves.

Expansion of the use of the polygraph needs to be done carefully, however, because the utility of the instrument depends so greatly upon the competence of the operator. Training of new polygraphers is a lengthy process, and training capacities are limited, even though they are being expanded. Increased use of the polygraph must be phased in gradually. Most examinations under any expanded program will be limited to counterintelligence questions. Such questions have more utility for current than for new employees. First-time applicants for security clearance by definition will not have participated in security violations, unauthorized disclosures or

provision of classified information to foreign nationals. The full benefit of the polygraph can be obtained only through "lifestyle" coverage, which includes critical areas of vulnerability in espionage cases. As is the case for background investigations, polygraph examinations must also be updated at periodic intervals.

One of the most critical information security issues today is the unauthorized disclosure of classified information by those who are trusted to protect it. The numbers and severity of such disclosures are alarming. It is impossible to maintain the credibility of our security system if we are confronted constantly by news stories, books, and television shows which contain classified information.

During the past two years, the DCI Security Committee has received more than 180 reports of the publication of classified information. More than seven times a month, on the average, classified material appears in the public media. There are administrative rules to prevent this, or to penalize those who do it. There are even laws against it. But leaking also is a consensual crime, and finding a leaker is extremely difficult.

Leaks of sensitive intelligence are especially damaging. They tell our opposition what we know, how we know it, and often, what we don't know. They lead to the shutting down of valuable sources of information, both human and technical. They leave us susceptible to disinformation. They force us to spend millions to develop new collection systems to replace those compromised. And they make it difficult for those subject to the security system to have any faith in it, leading to more unauthorized disclosures. Leaks beget leaks.

Public revelations of classified information are a reprehensible breach of trust and technically constitute espionage. The recent conviction of Samuel L. Morison under the Espionage Act will encourage those who do not believe we need a law to deal specifically with unauthorized disclosure of classified information to a party not associated with a foreign government. The Morison Case is unique. The evidence was overwhelming. The only issue was whether his actions violated the espionage laws. It is not likely that any similar case will occur in the foreseeable future. One conviction for leaking in the almost 70-year history of the Espionage Act will do little to slow the seven-plus intelligence leaks per month we are now experiencing. Legislation is needed to criminalize leaks of classified information. Passage of such a bill would demonstrate that Congress has reached the limit of its tolerance of this pernicious practice.

The attitudes and motivations that lead to leaking may not be far removed from those that result in cleared individuals committing espionage.

Interagency meetings of security officers and behavioral scientists under DCI SECOM auspices have tentatively identified personnel security areas requiring further study. One is a finding that most of those who have betrayed their country have an exaggerated sense of entitlement--an attitude based on self aggrandizement and an absence of responsibility to society, which says "I have a right to use for my own benefit anything I can acquire, even if my country suffers as a result." We are learning that motivations for espionage may be much more complex than ideology or simple greed.

Psychological research aimed at identifying behavior and attitudes which may signify potential threats to scurity is needed. There has been little funding for such research. Security Committee members have unanimously endorsed a proposal to interview persons convicted of espionage and their associates in an effort to improve our understanding of motives and behavior patterns. SECOM has provided support for a program involving screening of military personnel discharged for suitability reasons after having been granted security clearances. This effort seeks to determine whether a defect in the security process resulted in failure to identify and act upon suitability weaknesses that were subsequently confirmed. Significant research will be needed to fully assess the raw data from these projects and to attempt to integrate their findings into the security process.

In summary, personnel security is of paramount importance in protecting our national secrets. Progress is being made in the provision of resources to these programs, but there is much to do. The new directive authorizing greater use of the polygraph is a great step forward. More study is needed of the motivations and behavioral patterns of those who betray the secrets entrusted to them. In training investigators and adjudicators, more emphasis needs to be placed on what kinds of people commit treason and espionage. Finding "card-carrying Communists" has gone the way of high-button shoes. Today's personnel security specialist must be a student of human behavior, especially that behavior which can lead a man or woman to give away the nation's vital secrets while maintaining that he or she is an American.