

AD-A196 076

copy 2-710
**A REPORT TO
THE DEPUTY UNDERSECRETARY
OF DEFENSE FOR POLICY.**

Wash DC

(1)
**DTIC
ELECTE
MAY 16 1988**
S D
CD

**ANALYSIS OF THE EFFECTIVENESS OF THE
DEPARTMENT OF DEFENSE INDUSTRIAL
SECURITY PROGRAM AND
RECOMMENDATIONS FOR PROGRAM
IMPROVEMENT**

DISTRIBUTION STATEMENT A

Approved for public release
Distribution Unlimited

**DEPARTMENT OF DEFENSE
INDUSTRIAL SECURITY REVIEW COMMITTEE**

DECEMBER 10, 1984

RELEASED

88 4 26 081

~~FOR OFFICIAL USE ONLY~~

COMMITTEE MEMBERS

Daniel R. Foley, Co-Chairman
Deputy Assistant Inspector General, DoD
Criminal Investigations Oversight

John R. Hancock, Co-Chairman
Chief, Programs Management Division
Defense Investigative Service

Kathleen A. Buck
Assistant General Counsel (Legal Counsel), DoD

John E. Fields
Principal Assistant, Industrial Security
Office of the Director, Security Plans and Programs
Office of the Deputy Under Secretary of Defense for Policy

Alfred W. Hazen
Northwestern Regional Director
Defense Investigative Service

Alvin L. Madison
Program Director, General Intelligence
Office of the Assistant Inspector General for Auditing, DoD

INDUSTRY ADVISOR

Jerry M. Dolan
Director of Corporate Security and
Administrative Services, Aerojet General Corporation



Accession For	
NTIS CRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By <i>per. ltr.</i>	
Distribution	
Availability Codes	
<i>A-1</i>	Avail. and For Spec. Com.

TABLE OF CONTENTS

	<u>PAGE</u>
Executive Summary	vi
Study Methodology	xv
Issues and Recommendations	1
Section One: <u>Policy</u>	1
Increased Emphasis on Counter- intelligence and Human Reliability within the Defense Industrial Security Program.	1
Priority Emphasis on Security of Sensitive Contracts	7
Revision of the <u>Industrial</u> <u>Security Manual</u>	10
DIS Inspection of Special Access Programs	14
Strengthening the Adjudication Process	19
Centralization of the Adjudication Function within the Department of Defense	21
Revising the Frequency of Industrial Security Inspections	27
Reporting of all Foreign Travel by Contractor Personnel	33
Section Two: <u>Administration/Operations</u>	37
Creation of Separate Advisor and Inspector Roles of DIS Representatives	37
Establishment of a National Industrial Security Hotline	39
Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities	45

Establishment of a Graded Defense Industrial Security Program Inspection Rating System	48
Specialized Training Program for Accrediting Contractor Security Personnel	52
Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor Personnel	57
Section Three: <u>Legislation/Regulation</u>	59
Legislative Base for the Defense Industrial Security Program	59
Legislation to Limit Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures Themselves	62
Authority to Suspend and Debar Contractors for Serious Security Infractions	65
Section Four: <u>Personnel Security</u>	67
Revised Scope of Personnel Security Investigations	67
Enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances	74
Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations	103
Section Five: <u>Physical Security</u>	105
System of Controls Over After-Hours Access and Reproduction Equipment at Cleared Facilities	105
Section Six: <u>Information Security</u>	114
Access to the Defense Technical Information Center	114
Proactive Efforts by the DIS to Prevent Unauthorized Disclosures	118

Increased Emphasis on Classification Management	123
Prevention of "Bootlegging" of Classified Material	129
Summary of the Committee's Recommendations Regarding Changes in the Defense Industrial Security Program	130
<u>APPENDIX I</u>	141
Overview of the Defense Industrial Security Program	
<u>APPENDIX II</u>	155
Memorandum of the Deputy Under Secretary of Defense for Policy and Committee Charter	
<u>APPENDIX III</u>	159
Memorandum of the Acting Secretary of the Air Force	
<u>APPENDIX IV</u>	161
Memorandum of the Secretary of Defense	
<u>APPENDIX V</u>	160
Committee Letter to Defense Contractors/Government Agencies	
<u>APPENDIX VI</u>	167
Administrative Inquiry - Systems Control, Incorporated	
<u>APPENDIX VII</u>	174
Committee Questionnaire to DIS Personnel	
<u>APPENDIX VIII</u>	207
The Case of James Harper and Ruby Louise Schuler	

APPENDIX IX

217

The Case of William Bell and
Marian Zacharski

APPENDIX X

237

The Case of Christopher John Boyce

APPENDIX XI

239

DIS Categorization System

APPENDIX XII

242

Compilation of Personnel Contacted
During the Committee Study

REPORT OF THE DOD INDUSTRIAL SECURITY REVIEW COMMITTEE

EXECUTIVE SUMMARY

As a result of the arrest of James Durward Harper, Jr., for alleged espionage activity involving a Department of Defense (DoD) contractor facility, the DoD Industrial Security Review Committee was formed to "analyze the effectiveness of current industrial security requirements and develop recommendations for program improvement."

After a comprehensive study of the Defense Industrial Security Program (DISP), the Committee has completed its work and offers this summary of principal findings, conclusions and recommendations.

It is important to note at the outset that the Committee did not consider it a part of its mission to evaluate the performance or quality of service provided by the Defense Investigative Service (DIS), which is charged with administering and overseeing the DISP. Rather, it was to evaluate the overall system of security within defense industry with particular emphasis on identifying various methods of strengthening the program and formulating specific recommendations for improvement.

The defense industry is immense in size and scope. The DoD engaged in 14.7 million contractual procurement actions in 1983 at a cost of \$140.5 billion. It is recognized that each of these procurement actions did not involve a classified contract, but a significant portion did involve sensitive, leading-edge defense technology which requires security protection. Furthermore, considering the primary mission of the Department, which is to defend the security and national interests of the United States, lax security in sensitive

defense production presents awesome consequences. To perform its mission, the Department must maintain in peacetime an ample and secure industrial base to facilitate the preparation and successful conduct of military operations. A fundamental concept, therefore, which guided the Committee in its study, was the belief that industrial security policy and procedures must ensure the proper protection of classified information in industry in consonance with national policies and goals and not unduly encumber defense production.

Currently, there are nearly 14,000 cleared defense facilities, over 1 million cleared contractor employees and approximately 16 million classified documents entrusted to their safekeeping. To oversee the DISP, the DIS has less than 200 industrial security representatives (inspectors) in the field, a small number in comparison to the size and complexity of the cleared defense industrial establishment.

Committee Recommendations

POLICY

1. Increase emphasis on counterintelligence and human reliability factors in the administration of the Defense Industrial Security Program in order to provide enhanced protection against unauthorized disclosure of classified material.
2. Prioritize defense contracts according to the cognizant procurement activities assessed sensitivity of technology and apply commensurate DIS industrial security resources.
3. Where feasible, promulgate general security policy to replace much of the inordinate detail contained in the current

Industrial Security Manual (DoD 5220.22-M). Furthermore, tailor specific security requirements for individual contractor facilities into contractors' Standard Practice Procedures (Security Manual), taking into account the local hostile intelligence threat.

4. Establish a special group of DIS industrial security representatives to inspect special access programs and related "carve-out" contracts. To the extent practicable, program managers should be encouraged to relinquish inspection responsibility of such programs to the DIS. Furthermore, the Inspector General, DoD, during audits of special access programs, shall determine that each program has been properly established pursuant to Executive Order 12356, and the DoD implementation thereof, and assess reasonable adherence with DoD contracting practices, contractor performance and management of program funds.

5. Strengthen the personnel adjudication process through establishment of adjudicative standards as opposed to adjudicative guidelines which shall be uniformly applied throughout the DoD.

6. Duplicative reviews in the Industrial Security Adjudicative process should be eliminated, any potential conflict of interest be removed, and a centralized DoD clearance organization be established. Also, obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program.

7. Amend the current inspection schedule prescribed in the "Industrial Security Regulation" to take more effectively into account the volume and complexity of the classified activity at a particular DoD contractor facility. Discontinue routine inspections of "dormant" contractor facilities and

eliminate or significantly curtail inspections of "access elsewhere" facilities.

8. Require all contractor employees to report to the facility security department all instances of foreign travel for review by DIS representatives during the inspection effort.

ADMINISTRATION/OPERATIONS

9. The DIS establish a pilot program in which the industrial security representatives' duties as advisors to industry and regulatory inspectors are separate and distinct.

10. The DIS establish, publicize and administer a national DoD Industrial Security Hotline.

11. The DIS establish a pilot program, in coordination with industry and the military departments, for the assignment of industrial security representatives on a full-time or substantially full-time basis at extremely complex or particularly sensitive contractor facilities.

12. Alter the DoD security inspection rating system to provide for ratings of "superior," "satisfactory," "marginal" and "unsatisfactory" in order to provide a more meaningful evaluation of a contractor's system for safekeeping classified information.

13. The DIS provide a formal certification/accreditation training program for contractor industrial security personnel. The training program shall not be a mandatory requirement, however, the benefits of industry participation seem obvious, particularly smaller firms newly engaging in DoD classified contracts.

14. At the earliest practical time, DoD criminal investigative organizations should notify the DIS of criminal investigations indicating criminal conduct by cleared DoD contractors and contractor personnel.

LEGISLATION/REGULATION

15. Review current espionage laws that pose obstacles to the prosecution of individuals for the unauthorized disclosure of classified information.

16. Seek legislation limiting judicial and administrative review of DoD personnel security adjudications to the adjudicative procedures themselves and exclude the review of the adjudicative decisions of the Directorate of Industrial Security Clearance Review.

17. Amend the "Federal Acquisition Regulations" (FAR) or issue DoD implementing guidance to provide the authority to suspend and debar DoD contractors for serious security infractions.

PERSONNEL SECURITY

18. Negotiate the deletion of neighborhood and education interviews from the minimum investigative standards for a Special Background Investigation (SBI) mandated by Director of Central Intelligence Directive (DCID) No. 1/14. In addition, include subject interviews to the foregoing DCID as a mandatory investigative element of the SBI.

19. Enhance personnel security investigative standards and reduce the number and level of industrial clearances as follows.

a. Reprioritize the current system of selecting industrial personnel for periodic reinvestigation consideration. The present method of selecting personnel with the most dated investigations should be set aside in favor of a system which places priority on personnel who enjoy continuous or frequent recurring access to Top Secret, highly sensitive, or Sensitive Compartmented information.

b. Facility or personnel security clearances under the DISP should not be processed for defense contractors who provide services at sensitive facilities where access to classified information is not required.

c. DoD policy should be changed to permit the DIS cognizant security office authority to approve contractor employees for one-time or occasional access to classified information at a level higher than the personnel security clearance in effect. If recurring access is anticipated, approval would include initiation of the appropriate investigation.

d. Documentation for company granted Confidential personnel security clearance should be furnished to the DIS to be reviewed and recorded. In addition, such clearances shall be subject to automatic expiration 5 years from the date of issuance if justification for continued access is not provided. If justified, the clearance should be reissued by DIS following completion of a favorable national agency check.

e. DoD policy should be changed to permit use of the interim clearance investigative standards and criteria

presently provided for by the "Industrial Security Regulation" (DoD 5220.22-R) for all collateral personnel security clearance requests received for processing.

f. All Top Secret and Secret industrial personnel security clearances should be subject to automatic downgrade to the next lower level of clearance if justification to retain the higher level clearance is not received by the DIS within 5 years from the date of issuance.

g. A local agency check (LAC), employment check, and credit check should be added to the minimum investigative requirements for a Secret personnel security clearance. Furthermore, a national agency check, LAC, employment, and credit check should be repeated every 5 years.

h. All personnel security questionnaires submitted to the DIS for processing should be accompanied by a Clearance Justification Data Sheet. The data sheet should include certification by the employee applicant, immediate supervisor, and responsible management official that the applicant for clearance requires access to classified information, as well as a completed counterintelligence questionnaire.

20. Contractor Standard Practice Procedures should prescribe disciplinary action for employee security violations.

PHYSICAL SECURITY

21. An affirmative system of controls should be established over after-hours access and reproduction equipment at cleared facilities. While universal control requirements should not be mandated, the individual contractor, in consultation with the DIS, should establish an adequate system,

considering the particular circumstances of the facility, and incorporate the details into the Standard Practice Procedures.

INFORMATION SECURITY

22. The DoD Inspector General should schedule an audit of the Defense Technical Information Center to ascertain if internal controls are in place and working to preclude the unauthorized access and disclosure of its scientific and technical products and services. About 2,100 registered users are cleared for access to Secret and Confidential information on over 200 technical and scientific subjects ranging from aeronautics to space technology. Moreover, a military counterintelligence organization should conduct a hostile intelligence threat assessment of the Center.

23. The DIS conduct proactive efforts to oversee compliance with requirements pertaining to public disclosures regarding classified contracts and related brochures, promotional sales literature and reports to stockholders, as well as presentations at symposiums, conventions and so forth.

24. Increase emphasis on security classification management through training and oversight.

25. Strengthen procedures for prevention of "bootlegging" of classified material by establishment of a termination briefing and required execution of a form certifying that the executor possesses no classified material.

Committee Perspective

While adoption of some of the recommendations may appear costly and labor-intensive, some recommendations will result in savings in costs and labor. The thrust of the recommendations is focused at strengthening the DISP through concentration of DIS resources in the most vulnerable areas, revising some methods of operation, and eliminating activities of limited security value. A complete listing of all the Committee's recommendations is located at page 130.

STUDY METHODOLOGY

The report of the Defense Industrial Security Review Committee (the Committee) is presented in a single volume, supplemented by various appendixes, and is based on two distinct research approaches. The first consists of the collection and compilation of statistical data concerning the scope, magnitude, and operations of the Defense Industrial Security Program (DISP) and the DoD Personnel Security Program, the latter of which was largely limited to its application to industrial employees. These data are presented in several sections and appendixes of the report. They are based on replies to a Committee letter soliciting comments and recommendations on all aspects of the DISP and its administration by the Defense Investigative Service (DIS). The letter was sent to 350 large and small defense contractors as well as various Federal agencies. Furthermore, a comprehensive questionnaire was sent to all DIS job series 080 personnel and other personnel of DIS whose duties and responsibilities include substantial DISP involvement. Also included and subjected to Committee analysis were quantitative data compiled separately by the DIS and issued by that agency as Monthly Management Reviews. The results of these sources of data are reflected throughout the report in the various discussions, conclusions, and recommendations contained therein. An overview of the DISP is attached for information at Appendix I.

The second approach is generally qualitative in nature. It covers many elements which cannot be analyzed through statistical measurement. Statistical material is included, however, where available and pertinent. Aside from the DIS, substantial inputs were provided by cleared defense contractor facilities, by various industrial associations, by the Military Departments, by various other DoD components, by elements of the Office of the Secretary of Defense, and by other non-DoD

U.S. Government Departments and Agencies. The contractors and industrial associations drew heavily upon information voluntarily supplied by their professional industrial security staffs, employees, and general membership, respectively.

Material was drawn from responses to letters, personal interviews, the media and group discussion. The letters and forums served as means to solicit information on pertinent aspects of the DISP, the current administration of the DISP, any relevant criticism of the DISP, and suggestions and recommendations to improve the Program or its administration/implementation.

Study Chronology and Scope

In late October 1983, General Richard G. Stilwell, the Deputy Under Secretary of Defense for Policy, authorized the Director, DIS, to form a panel to examine events associated with the arrest of James Durward Harper, Jr., for alleged espionage activity. The panel was to study the modus operandi of Harper, Harper's wife, and the security conditions of the contractor facility from which the classified material was diverted (Systems Control Technology, Inc.). Within this context, the panel was to analyze the effectiveness of current industrial security requirements and develop recommendations for improvement.

The panel held its initial meeting in November 1983, to review the known facts of the Harper incident and to develop a general study methodology. However, in view of the policy implications and to assist the panel with its responsibilities, General Stilwell decided in early December to redesignate the panel as the DoD Industrial Security Review Committee and place it under his auspices (Appendix II).

As a related matter in November 1983, the Acting Secretary of the Air Force sent a memorandum (Appendix III) to the Secretary of Defense expressing concern regarding the Harper espionage case and suggested that the DoD Inspector General conduct an objective review of the Defense Industrial Security Program. The Secretary of Defense replied in a memorandum (Appendix IV) that the Committee had been formed to "...conduct a comprehensive evaluation of the effectiveness of the DISP...."

In late December 1983, the Committee solicited written comments and suggestions for program improvement from approximately 350 cleared defense contractors and from selected DoD and non-DoD organizations (Appendix V).

By the end of January the Committee had reviewed the administrative inquiry of Systems Control Technology, Inc. (SCT) conducted by the DIS (Appendix VI) and had completed a visit to the Silicon Valley area of California where SCT is located to gain insight into the special security and counterintelligence problems of locales with a concentration of firms engaged in high technology defense work. The visit included interviews with local DIS industrial security personnel and a meeting at the Stanford Research Institute's International Center in Palo Alto, California, to discuss pertinent issues with ranking management and security officials from 22 Silicon Valley contractor facilities.

In order to enhance the depth and scope of the ongoing review of the DISP, the Committee developed and distributed a comprehensive questionnaire to all DIS personnel with substantial industrial security duties and responsibilities. The questionnaire addressed all pertinent aspects of the DISP and its administration by the DIS. The Committee received 170 replies to the questionnaire, which proved most valuable in the

formation of initial issues and concerns warranting further analysis. A copy of the questionnaire, along with the compilation of the 170 responses received, is at Appendix VII.

The Committee made a number of visits to various Government activities to gather additional information deemed essential to a thorough examination of the relative strengths and weaknesses of the DISP. Accordingly, the Committee interviewed key officials during its travels to the Air Force Office of Security Police and the Air Force Systems Command (Contract Management Division), Albuquerque, New Mexico; U.S. Army Ballistic Missile Division, Huntsville, Alabama; Defense Technical Information Center, Alexandria, Virginia; Defense Industrial Security Clearance Office, Columbus, Ohio; Directorate, Defense Industrial Security Clearance Review, Office of the General Counsel, DoD, Arlington, Virginia; Department of Energy, Germantown, Maryland; National Security Agency, Fort George Meade, Maryland; Central Intelligence Agency, Tysons Corner, Virginia; the Federal Bureau of Investigation, Washington, DC; and DIS Headquarters. The Committee also attended and participated in the annual Security Committee meeting of the Aerospace Industries Association (AIA) in Tucson, Arizona. The Committee discussed many of its preliminary issues with the AIA membership as well as the eight attending DIS Regional Directors of Industrial Security.

The Committee conducted personal interviews with representatives from each of the Military Department counterintelligence organizations (Army Military Intelligence, Naval Investigative Service and Air Force Office of Special Investigations). These interviews included discussion of preliminary Committee issues and a solicitation of comments and recommendations. Details of the Harper, Bell/Zacharski and Boyce espionage cases, which are summarized at Appendixes VIII, IX and X, were also carefully reviewed and discussed.

A composite of Committee interim findings and suggested program improvements were presented, in draft form, to counterintelligence and security staff officials of the Office of the Deputy Under Secretary of Defense for Policy for their review and comment. These interim findings were also mailed to the Security Committee and Security Sub-Committee membership of the AIA and the National Security Industrial Association, respectively, for their review and comment. The response to these efforts was most enlightening and the comments received resulted in some adjustments to the Committee's conclusions and recommendations. Appendix XII is a compilation of personnel contacted during the study.

ISSUES AND RECOMMENDATIONS

SECTION ONE: POLICY

1. Increased Emphasis on Counterintelligence and Human Reliability Within the Defense Industrial Security Program (DISP)

Discussion:

Currently, the security inspection represents the primary tool of the DIS for monitoring a cleared contractor's compliance with the requirements of the DISP. Historically, the program has been an administrative effort that is conducted in a mechanical manner with principal emphasis on document and physical security controls. The principal benefits of these efforts are that they help prevent accidental losses of classified material and make it somewhat difficult to illegally remove classified documents. As a practical matter, however, rarely has classified material been illegally obtained through forced entry of classified vaults or containers. The weak link in the security chain is considered to be the cleared personnel having access to classified material. Hostile intelligence services recognize it is easier and far more effective to enlist the services of an individual that already has access rather than to forcibly penetrate a security system.

To more effectively take into account the hostile intelligence threat and the perceived human vulnerability factor, the DIS would have to adjust its current program emphasis. Fundamental to the adjustment would be a closer alignment of the DIS with the counterintelligence community at both the national and local levels. This would include access by the DIS to available counterintelligence production, known essential elements of information desired by hostile

intelligence services, and multidisciplinary threat assessments prepared by U.S. counterintelligence agencies. This data would form the basis for tailored security programs. The hostile intelligence threat and appropriate security countermeasures would vary depending on the presence of: accredited Sino-Soviet/Warsaw Pact diplomatic personnel; representatives of Eastern Bloc trading companies; university exchange students; merchant shipping; air carriers; military exchange students; United Nations employees; journalists and researchers, and so forth.

It is not suggested that the DIS assume an operational counterintelligence role but rather that the DIS more aggressively integrate available counterintelligence production into the performance of its primary responsibility--the administration and oversight of the DISP. Department of Defense Directive 5220.22, "DoD Industrial Security Program" stipulates that the Secretaries of the Military Departments shall provide requested counterintelligence effort to the DIS in administering the DISP.

The DIS role would be primarily one of expert consultant to industry on security matters but include not only the administrative aspects of the DISP but an awareness of the current hostile intelligence threat (including human intelligence, signal intelligence and photo intelligence) and the capability to recommend appropriate security countermeasures to industry. This would necessitate that DIS industrial security personnel receive formal counterintelligence training.

Vital to counterintelligence emphasis are a comprehensive security education/hostile threat briefing program for industry, and development of a plan that encourages industry to initially screen employees and be continually alert to

behavioral changes and other circumstances that may affect an employee's continued suitability for classified access.

It is generally accepted that employee awareness and understanding of security vulnerabilities and countermeasures will increase voluntary acceptance and adherence to security policies. Both productivity and security are accomplished through people. People who are informed and understand an issue are more likely to be content with its ramifications and remain productive and properly motivated employees. The goal of proper protection of classified information in industry will be difficult to achieve without cleared personnel knowing and understanding their responsibilities in carrying out the DISP.

A security education/hostile threat briefing should be developed by the DIS, in coordination with the Federal Bureau of Investigation and appropriate military department counterintelligence organizations. The briefing should be continually updated based on the perceived local threat, and modified according to the locale and audience. Varied methods of presentation would enhance acceptance and broader application of the program. Specially trained and qualified DIS speakers would be available for presentations or the briefing material could be provided to industry in lesson plans, slides/script, video cassette or film versions for presentation by facility security personnel.

A complete security education program should include the following topics and preferably be presented in several segments:

- a. Localized multidisciplinary hostile intelligence threat from a problematic standpoint.
- b. Reporting of contacts with Sino-Soviet/Warsaw Pact personnel and any attempt by unauthorized persons to obtain national security information.

- c. Espionage exploitation of human weaknesses and recruitment techniques.
- d. Elements of the offense of espionage.
- e. Warning that a defector in place will likely provide indicators of espionage acts despite ingenuity and cleverness of the perpetrator (i.e., espionage is a high risk proposition).
- f. Security vulnerability of the telephone.
- g. Possible espionage indicators such as unusual or inordinate foreign travel to Western Europe and Mexico. Special considerations relevant to travel to designated foreign countries.
- h. Fundamental security practices.

Various studies have shown that the principal motivation for espionage is greed. Desire for financial reward, however, has generally been accompanied by apparent mental or emotional problems which are manifested through real or imagined grievance, dissatisfaction or disgruntlement. (Refer to Appendixes VIII and IX for a detailed description of recent espionage cases manifesting these characteristics.) Alertness to espionage indicators is crucial to a sound security program. First-line supervisors, with proper security indoctrination, working closely with corporate security personnel in partnership with the DIS is considered the most effective way of ensuring the strength and integrity of the DISP on a day-to-day basis. Neither periodic security inspections conducted by the DIS nor the current personnel security investigation program will adequately fill this role.

A personnel security investigation is usually a one-time inquiry, or at best an inquiry conducted at 5 year intervals in cases of particularly sensitive access, regarding an individual's background, character and reputation. Without a volunteered indication of a problem, Government scrutiny of an individual's suitability for classified access ceases upon

completion of a favorable personnel security investigation. Moreover, the majority of industry personnel¹ involved in the DISP possess a secret security clearance based solely on a one-time National Agency Check (NAC) and no field investigation whatsoever. All the NAC reveals is that the individual does or does not have an existing criminal or subversive record at a Federal or local law enforcement agency.

The DIS should develop a program of indoctrination and regular guidance to appropriate industry representatives in the selection and screening of their firm's applicants for security clearances as well as continued alertness to behavior and attitude changes and other circumstances which may affect continued security suitability of cleared employees.

This indoctrination program and follow-on guidance by the DIS would encourage corporate alertness and sensitivity to the following types of employee actions which may have security ramifications and would warrant assessment by the DIS.

- a. Willful violation of security regulations or attempts to obtain or reproduce classified information unrelated to an individual's duties.
- b. An attempt to remove classified material from the facility or possession of a camera or recorder in a secure area.
- c. Excessive overtime or unusual and unnecessary working hours.

1. United States General Accounting Office letter of June 11, 1984, subject: "Polygraph and Prepublication Review Policies of Federal Agencies," reflects that there are 900,000 DoD contractor employees with a Secret clearance and 111,000 with a Top Secret clearance. Additionally, 10,808 contractor employees have Sensitive Compartmented Information (SCI) access and 21,250 are assigned to non-SCI special access programs.

- d. Unexplained affluence or excessive indebtedness.
- e. Apparent mental or emotional problems; adverse behavioral or attitudinal patterns.
- f. Serious unlawful acts.
- g. Unusual or inordinate foreign travel, such as trips to Western Europe and Mexico.

Recommendation:

The DIS administration and oversight of the DISP should include a balance of administrative inspections and attention, in partnership with industry, to the human reliability aspects of the program with emphasis on the hostile intelligence threat. This would necessitate a closer alignment of the DIS with the counterintelligence community and development of a viable threat awareness program.

2. Priority Emphasis on Security of Sensitive Contracts

Discussion:

Executive Order 10865, "Safeguarding Classified Information Within Industry," states inter alia that "... it is mandatory that the United States protect itself against hostile or destructive activities by preventing disclosure of classified information relating to the national defense." The Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M) establishes the requirements for safeguarding all classified information that the Government loans to Defense contractors in connection with the performance of a classified contract, including precontract and postcontract activities. The DIS is charged with the responsibility for administering the DoD Industrial Security Program (DISP) and uses periodic security inspections as a principal method of oversight. Such inspections are intended to ensure that procedures, methods, and physical safeguards employed by contractors are adequate for the protection of classified information entrusted to them. Where problems are identified inspectors make suggestions to enhance security procedures at Defense contractor facilities.

The Industrial Security Operating Manual (DISM 31-4) is an internal guide designed to assist industrial security representatives to carry out their responsibilities relating to the safeguarding of classified information in the custody of industry. According to the Manual, the DIS categorizes each cleared contractor facility according to number of cleared employees, volume of classified documents, number of classified contracts, number of controlled areas, and so forth. While sensitivity of classified material held (specifically, Top Secret, North Atlantic Treaty Organization, Critical Nuclear Weapons Design Information) is a factor considered in assigning

category designations, it is an insignificant factor since it is the lowest ranked consideration according to DISM 31-4 guidance. The categories are used to allocate resources for inspections, i.e., whether the inspection should be an individual or a team effort. Furthermore, the frequency of security inspections as outlined in the "Industrial Security Regulation" (DoD 5220.22-R) is governed by the level of possession of classified material, as follows:

<u>Level of Possession</u>	<u>Frequency of Inspections</u>
Top Secret	6 months
Secret	6 months
Confidential	9 months
All "Nonpossessing" facilities	9 months

The above procedures represent a uniform approach in the administration and oversight of the DISP, which according to DIS representatives, is applied to about 13,000 cleared DoD contractor facilities by slightly less than 200 industrial security representatives (field inspectors).

Considering the current number of industrial security representative resources, the magnitude of the responsibility appears overwhelming. It was reported, however, that 95 percent of all classified documents are located at approximately 4 percent (520 facilities) of 13,000 cleared facilities. This suggests a reassessment of current procedures. The inflexible, blanket approach to oversight of the DISP conducted uniformly across the entire spectrum of cleared facilities (using only classification to determine sensitivity) at prescribed intervals (6 or 9 months) appears lacking in perspective and effectiveness.

Conclusion:

The most effective and prudent method of safeguarding classified information released to industry should entail a system of prioritization wherein contracts evaluated as most sensitive receive the most intensive DIS security attention. Prioritization should be accomplished by the primary users--the individual Military Services based on specific apportionments. For example, each military department would evaluate and select its 50 most sensitive collaterally classified contracts. Lesser users, such as Defense and non-Defense agencies and departments, would be provided proportionately smaller apportionments. The DoD Master Urgency List pertaining to National (Project BRICK-BAT) and Department of Defense (Project CUE-CAP) critical defense production programs shall be considered by the users, where appropriate, in the evaluation and prioritization process. Both Project BRICK-BAT and Project CUE-CAP pertain to approved National Department of Defense urgency determinations for critical defense production programs and each program is assigned a relative priority ranking for determining allocations support.

Recommendation:

DoD procurement activities, employing a reasonable apportionment system, should prioritize classified contracts according to assessed sensitivity. Commensurate DIS resources would be applied to these contracts based on the assessed sensitivity.

3. Revision of the Industrial Security Manual

Discussion:

The current authority for the DISP is Executive Order 10865, "Safeguarding Classified Information Within Industry," which provides that the Secretary of Defense and other specified officials of the Executive Branch shall, by regulation, prescribe such specific requirements, restrictions, and other safeguards necessary to protect classified information within industry. Department of Defense Directive 5220.22, "DoD Industrial Security Program," implements Executive Order 10865 and assigns to the Director, DIS the responsibility for security cognizance for all contractors and industrial facilities under the DISP (see Appendix I). The directive further provides for issuance of the Industrial Security Manual for Safeguarding Classified Information (ISM) (DoD 5220.22-M), which prescribes the specific requirements, restrictions, and other safeguards considered necessary, in the interest of national security, for the safeguarding of classified information within industry. It assigns responsibility to the Director, DIS to develop appropriate changes to keep the ISM current and effective.

The issue which must be considered is whether current ISM policy guidance prudently ensures the proper protection of classified information in industry in consonance with national policies and goals and does not unduly encumber defense production.

The current ISM (March 1984), which supersedes the ISM of January 1983, is a 345-page manual which some have described as overly detailed, confusing, conflicting and inflexible. It spells out in minute detail the various procedures and rules to be followed by U.S. industry engaged in classified contracts.

The ISM is regularly revised and amended resulting in more detailed refinement of procedures in an apparent attempt to address the universe of procedural possibilities. The end result may be encumbering to both industry and the DIS program manager.

The Committee believes that, to the extent possible, the ISM should contain general policy that provides procedures for the most efficient and effective protection of classified information in industry in accordance with applicable statutes and executive orders. The policy guidance must ensure that the DISP is a cooperative program in which primary responsibility is placed with the information custodian - industry, with Government establishing the safeguarding requirements. To accomplish this the policy must have a two-fold objective: (1) minimize the unauthorized disclosure of classified information, (2) facilitate the efficient, secure completion of classified contracts by ensuring that the information is available to those who have appropriate need-to-know. The policy must incorporate flexibility to accommodate management contingencies involved in industrial application of DoD mandated personnel, information, physical and technical security measures. The policy should provide the responsible information custodian (industry) a voice in determining the necessary protective resources that must be employed on the basis of threat, environment and vulnerability. Finally, the DIS program manager and his regional directors must have the authority, autonomy and resources to properly administer and oversee the DISP.

The ISM currently requires that a contractor submit a Standard Practice Procedure (SPP) "... in sufficient detail to place into effect all security controls required by the DD Form 441 (Department of Defense Security Agreement) and this manual which are applicable to the operations of the facility."

Considering the procedural detail currently incorporated in the ISM, there appear to be only limited opportunities for contractor flexibility. To universally apply the same rules irrespective of the perceived threat, environment and vulnerability of a particular contractor is imprudent and possibly counterproductive. In some instances standard rules may provide inadequate safeguards and in other unnecessary security requirements, either of which is detrimental to secure, efficient completion of defense contracts.

The SPP should be a carefully crafted document embracing both general security policy, and specific details unique to each cleared facility. The threat, environment and vulnerability of a particular contractor would be fundamental factors in determining necessary security safeguards, as well as subsequent compliance inspection requirements. Also, the professional capability of the corporate security staff and overall security reputation of the contractor would be key considerations in these determinations.

The foregoing represents a more positive and integrated approach to the protection of classified information in industry. It embodies decentralized operations and responsibilities on the part of DIS regional directors with coordination and oversight by the Program Manager at DIS Headquarters. It provides for security policies and procedures to be a function of vulnerabilities and real threats which will accommodate the situation in the time and place applied.

Conclusion:

To the extent possible and prudent, superfluous detail should be replaced with general security policy throughout the ISM (DoD 5220.22-M). In this connection, greater reliance should be placed on the Standard Practice Procedures to capture

specific and detailed requirements pertinent to individual contractor facilities. In addition, large segments of the ISM should be extracted and put in supplement or handout form, as appropriate, because of their limited application to the universe of cleared facilities, e.g., international operations, automatic data processing, sample clearance forms, etc. The ISM should also be restructured and rewritten to enhance its use for reference purposes and to eliminate numerous grammatical and syntactical shortcomings.

Recommendation:

Where feasible, promulgate general security policy to replace much of the inordinate detail in the current Industrial Security Manual (DoD 5220.22-M). In addition, large segments of the Industrial Security Manual that have limited applications should be extracted and put in supplement or handout form. Furthermore, tailor specific security requirements for individual contractor facilities into contractors' Standard Practice Procedures (Security Manual), taking into account the local hostile intelligence threat.

4. DIS Inspection of Special Access Programs

Discussion:

Special access programs are established in intelligence or intelligence-related areas and for sensitive research and development programs. Some special access programs are SCI (Sensitive Compartmented Information) and are controlled and approved by the Director of Central Intelligence. Within DoD, the Secretary of Defense and the Secretaries of the Military Departments approve the establishment of special access programs. Programs are normally established for scientific breakthroughs, advanced technological developments or unique technological applications. Authority to establish special access programs is contained in Executive Order 12356, "National Security Information." DoD 5200.1R, "Information Security Program Regulation," implements Executive Order 12356 and contains DoD policy governing special access programs and related reporting requirements.

The Deputy Under Secretary of Defense for Policy (DUSD(P)) is responsible for maintaining accounting control over established special access programs. Based on reports furnished by DoD activities, DUSD(P) personnel are required to account for all approved special access programs. The DUSD(P) personnel initially estimated that about 100 special access programs exist within DoD. This estimate now has been revised to about 200 programs. However, 200 programs may just be the "tip of the iceberg" as it appears that the programs in recent years have been perpetuated by DoD components and they have failed to report them. It has only been in the last year or so that the Military Departments have sought to centralize management control and oversight over special-access programs. Therefore, the Committee believes that the number of special access programs far exceeds the Office of the Deputy Secretary

of Defense for Policy estimate of 100-200 programs. While the Committee recognizes that valid reasons do exist for establishing special access programs, it also believes that program oversight presently rests with too few program management personnel who have vested interests. Further, there is to our knowledge, no formalized schedule for recurring inspections as exists under the Defense Industrial Security Program.

Special access programs can involve DoD contractors. Special access program contracts with proper approval can be "carved-out," that is, the DIS has been relieved of security inspection responsibility under the DISP. Security inspection responsibility for the most part has been retained by the Services. Only recently has the DIS been allowed to inspect a few programs established by DoD components. "Carve-out" contracts are estimated to number in the thousands and involve billions of dollars.

"Carve-out" contracts are getting more attention. The 1984 House of Representatives, Department of Defense Appropriation Bill states:

Unlike the majority of sensitive compartmented information (SCI) contracts whose existence are known to DIS, collateral "carve-outs" are exceedingly difficult to detect, and when detected, are generally discovered by accident during the course of normal DIS security inspections. In 1981, DoD officials estimated there were approximately 900 collateral "carve-outs." Other sources believe the number may actually be in the thousands.

Security, most often cited as the basis for establishment of "carve-out" contracts, is not the only, or even perhaps the primary, consideration. "Carve-outs" are often sole source awards

allowing program managers to escape the routine procurement bureaucracy, provide for a certain ease in contract administration and presumably reduce time expended in the procurement process. It is a strange anomaly that the creation of a "carve-out" contract may be accomplished by procurement activities who fail to consult with security officials during the procurement process. There is no obligation for them to do so. There is near unanimity among industry as well as some DoD officials that "carve-outs" afford less, sometimes considerably less, security than that available within the standard industrial security framework. The classification of most "carve-out" contracts at the Secret level raises the question as to the legitimacy of the "carve-outs" especially when the personnel investigative standard for access is no greater than that required to obtain a DoD building pass.

The House Committee on Appropriations recommended immediate action to:

Reduce the proliferation of programs which are excluded from the central industrial security procedures; an immediate review should be undertaken which will identify all collateral "carve-outs" and bring all such exceptions back into the central industrial security procedures unless there is a specific case by case determination made by the Deputy Under Secretary of Defense for Policy that overriding national security considerations dictate otherwise.

The Industrial Security Review Committee supports this recommendation. Access by DIS inspectors to "carve-out" contracts would not adversely affect exposure to sensitive DoD programs as thousands of contractor personnel already have special access authorizations. At present, there are only about 200 industrial security inspectors within the Defense Industrial Security Program and the number with special access could be limited.

Special access program managers refused to tell Committee members how many of their program personnel were involved in conducting industrial security inspections related to their programs and "carve-out" contracts. It appears that their personnel involved in making inspections may outnumber the 200 DIS inspectors responsible for conducting inspections of collateral facilities. Establishment of a specially indoctrinated, trained and compartmented DIS inspection team for "carve-out" contracts would be useful and cost effective if duplicative inspections by the DIS and special access program personnel could be eliminated. It would also provide for consistent security inspection procedures and policies.

During the Committee's tenure, the Department of Defense Inspector General established a special audit team to cover special access program operations. This effort was supported by the Office of the Deputy Under Secretary of Defense for Policy.

The Committee was informed that the first audit by the Inspector General's Office was initiated in August 1984. The Committee believes that this is a step in the right direction to ensure proper oversight over special access programs and to limit the potential for fraud, waste and mismanagement in such programs.

Recommendation:

a. That the Department of Defense Inspector General, during audits of special access programs, determine the adequacy of, and compliance with, DoD contracting practices, contractor performance, management of program funds and other areas of special access programs and carve-out contracts.

b. That the Office of the Deputy Under Secretary of Defense for Policy continue to support the audit efforts of the Department of Defense Inspector General and coordinate with DoD components the program access authorizations required by audit personnel.

c. That the DIS establish a special group of inspectors for special access programs and related "carve-out" contracts and that DoD components relinquish to the DIS inspection of these programs and contracts when determined appropriate by the sponsoring component.

5. Strengthening the Adjudication Process

Discussion:

Executive Order 10865, "Safeguarding Classified Information within Industry," does not provide guidance on criteria to be used when determining when an applicant for a security clearance is trustworthy. Executive Order 10450, "Security Requirements for Government Employment," does, however, provide guidance which can be applied in industrial cases. Executive Order 10450 establishes criteria to be used in judging reliability and trustworthiness. These categories, however, are only broadly described.

Pursuant to the criteria, adjudicative guidelines were developed within DoD 5200.2-R for use in the Defense Industrial Security Program. Although these guidelines are more detailed than the criteria listed in the Executive Order, there is still very broad latitude for adjudicators to decide on a case-by-case basis. In fact, the guidelines may be ignored if an adjudicator decides to do so. Guidelines are not mandatory: they merely provide a point of reference. In examining the security program the Committee observed that within the Department some components strictly construed the guidelines while other components did not.

To ensure uniformity in the application of the criteria, and to eliminate confusion for both applicants and adjudicators, the Committee believes that the guidelines should be amended to become requirements to be followed. This would help to ensure that similar cases are adjudicated in the same way. While the Committee recognizes that cases are handled on a case-by-case basis, the Committee believes that the adjudicators should use the guidelines as actual requirements.

Each clearance determination case should apply the adjudication requirements, and each adjudicator should be required to permanently record and document how clearance determinations were rendered applying the adjudication requirements. Also, the records should contain specific, clear statements how any mitigating information and factors were or were not applied in a particular case.

Recommendation:

The Committee recommends that the term "guidelines" be revised to read "requirements" and be applied uniformly in all cases.

6. Centralization of the Adjudication Function Within the Department of Defense

Background:

The adjudication of clearances is the process of reviewing and determining when there is sufficient derogatory information regarding an applicant or a person holding a security clearance to provide a basis for the issuance of a statement of reasons. A statement of reasons is a written statement sent to the applicant or person holding a security clearance to notify the individual of the specific grounds to deny or remove a clearance. Executive Order 10865, "Safeguarding Classified Information within Industry," DoD Directive 5220.6, "Industrial Personnel Security Clearance Program," and DoD Regulation 5220.22-R, "DoD Industrial Security Regulation," pertain to this process. Executive Order 10865 established procedures when a clearance is denied or to protect the rights of the individual applicant.

At the present time the adjudication function for industrial security clearances is split between the Defense Investigative Service and the Directorate for Industrial Security Review. In the Defense Investigative Service, the Adjudication Division of the Defense Industrial Security Clearance Office (DISCO) is responsible for screening cases for significant derogatory information. The information is obtained from the investigation conducted by the Defense Investigative Service. Cases with significant derogatory information are then forwarded to the Directorate for Industrial Security Review where the cases are again reviewed by a screening board. Each screening board consists of 3 members.

Duplicative Reviews and Lack of Centralized Adjudication:

Since each case with significant derogatory information is reviewed at least three times at the Defense Investigative Service and by the Directorate for Industrial Security Review before a statement of reasons can be issued, a great deal of time is used during this review process. There are multiple layers of review and staff assigned at each layer to perform the same function. As a result, the Committee believes that the existing structure should be evaluated to eliminate duplication. Merely shifting DIS personnel elsewhere does not address the fundamental problem of eliminating duplication of effort. For example, merely shifting the Adjudication Division of DISCO or any portion thereof to DIS Headquarters does not address this problem.

A common complaint regarding the security clearance process is the length of time taken to process a clearance through the elaborate structure which has evolved within the Department. One method of reducing the time required to process a file with derogatory information is to eliminate unnecessary reviews of the file. To address these complaints one proposed solution would be to centralize the adjudication process. Reorganization alone is, however, not the answer. The adjudication procedure should be streamlined to eliminate unnecessary layers of review.

One careful review by an adjudicator meets the requirements of Executive Order 10865 to comply with the due process procedures required in security clearance cases. It is clear that the current process which can take as long as 3 years or more is not acceptable for the Government and can create a hardship for both the contractor and the individual whose clearance has been suspended. A comparison of this

process with, for example, the judicial system reveals an administration process which is far more cumbersome.

Streamlining the procedure would address the time problem, but it would not address another complaint which has been raised, that of different components in the Department applying different standards in issuing clearances. All components in the Department are required to apply the adjudication guidelines set forth in DoD Regulation 5200.2-R. It is clear, however, based on the interviews conducted and statistics provided by various components, that the standards are not being applied in the same manner.

By way of illustration, the military department and industrial personnel security clearance denial/revocation rate for collateral clearances during FY 1983 is as follows:

- Army - 3 percent
- Navy - .6 percent
- Air Force - 2 percent
- Industry - .1 percent

Although case-by-case decisions will vary according to the facts, the Committee favors reevaluation of the way the guidelines are being applied by DoD components. The Committee's focus has been on the Industrial Security Program, but we have observed significant differences in adjudications of clearances of military and civilian personnel by each of the three military services and DoD agencies.

Conflict of Interest:

Another criticism of the program is that the adjudication function within the Defense Investigative Service (DIS) is improper because DIS is responsible for the investigation of

the person and should not be responsible for adjudicating the case as well. This criticism is based on the Administrative Procedure Act, 5 U.S.C 554 (d) (2) which provides:

(1) "The employee who presides at the reception of evidence pursuant to section 556 of this title shall make the recommended decision of initial decision...Except to the extent required for the disposition of ex parte matters as authorized by law, such an employee may not - -

(2) "be responsible to or subject of the supervision or direction of an employee or agent engaged in the performance of investigative or prosecuting functions for an agency."

The Attorney General's Manual on the Administrative Procedure Act (APA) states that "554(d)(2) is intended to maintain the independence of hearing officers, and as a practical matter this means that an agency's hearing examiners should be placed in an organizational unit apart from those to which investigative and prosecuting personnel are assigned...."

"Section 554 APA applies in every case of adjudication required by statute to be determined on the record after opportunity for an agency hearing...." The legislative history of the APA indicates that it applies only to administrative hearings which are required by statute. The industrial security program is not, however, created by statute; it is created by Executive Order 10865. Thus, a literal reading of the APA places the program outside the scope of section 554. Moreover, section 554 does not apply to hearings "to the extent that there is involved the conduct of military or foreign affairs functions." 5 U.S.C. 554(a)(4).

If the program is not within the scope of 554 APA there may still be due process and functional concerns where an agency exercises both investigative and adjudicative functions.

While DISCO may not have a final adjudicative determination, cases are being reviewed with the intent of recommending issuance of a statement of reasons. From a functional standpoint, if DISCO is not in fact "adjudicating cases" the question is raised as to why it is necessary to have an adjudication division separate from that of the Directorate of Industrial Security Clearance Review.

Subpoena Power:

During the study, proposals were made to obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program. The Committee supports this proposal which is currently under consideration at the Office of Management and Budget. Under current procedures, witnesses cannot be compelled to appear at hearings and are requested to do so voluntarily. Moreover, access to records may be critical to presentation of the case. However, in some instances when relevant derogatory information is developed during an investigation, the information cannot be used when the individual furnishing such information refuses to testify or produce records. Although such situations reportedly occur infrequently, the lack of subpoena power for this program is a flaw which can be remedied by the enactment of legislation. Accordingly, the Committee believes that such legislation should become a part of the Administration Legislative Program.

Conclusion:

Pursuant to Executive Order 10865 any applicant denied a clearance or individual whose clearance is revoked is entitled to a written statement of reasons and a hearing. These procedures were established to protect the rights of the individual and it is essential that these procedures provide a reasonable time to prepare the case. It is equally important that action be taken to avoid unnecessary delays, which can also result in cost savings in the operation of the program.

Duplication of review procedures should be eliminated. This has been a matter under study by the Office of the Deputy Under Secretary of Defense for Policy and the Office of General Counsel for over a year. The Committee recognizes the efforts of that ongoing review and suggests that the study culminate with a decision on an organizational structure which will eliminate or greatly reduce duplicative review and potential conflict of interest.

Recommendation:

That the Deputy Under Secretary of Defense for Policy determine whether the Adjudication Division of DISCO is in fact performing adjudicative functions within the purview of the Administrative Procedures Act. Each case should be reviewed carefully once, subject to the approval of the individual in charge of the centralized adjudication function. Furthermore, that a separate study be conducted to assess the merits of centralizing the adjudication function (separately and distinctly from any investigative organization) within the Department of Defense for adjudication of all security clearances to include cases under the DISP. Finally, obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program.

7. Revising the Frequency of Industrial Security Inspections

Discussion:

The DoD policy governing the frequency of inspections for contractor facilities participating in the Defense Industrial Security Program is prescribed by the "Industrial Security Regulation," DoD 5220.22-R. The frequency of industrial security inspections is based on the highest level of classified material possessed, as follows:²

<u>Level of Possession</u>	<u>Frequency</u>
Top Secret	6 months
Secret	6 months
Confidential	9 months
Nonpossessing	9 months

The Committee considers the foregoing inspection schedule to be flawed. The current policy is based largely on the premise that the higher the level of classified material actually possessed by a facility, the more frequent the need to inspect. However, facilities possessing Top Secret and Secret are inspected on the same schedule, notwithstanding the clear distinction between the two classification levels. Moreover, the same is true of Confidential and nonpossessing facilities. The present system also fails to take into account the vast differences between facilities possessing the same level of material. It stands to reason that the need to inspect a firm possessing a single Confidential document would be nowhere

2. Facilities engaged in the graphic arts business and those cleared as commercial carriers are placed on a 6-month inspection frequency, regardless of the level of possession.

near that of a firm possessing 10,000 Confidential documents. Similarly, to inspect a firm possessing a single Secret document more frequently than another possessing a large number of Confidential documents is also difficult to rationalize.

The Committee believes a preferred system of determining the necessary inspection frequency would be one based on an assessment of many diverse elements of a facility's industrial security program and classified activity. The highest level of classified material possessed would be one element, but the system should also include other qualitative aspects such as an assessment of the facility's record of compliance with program requirements, effectiveness of existing security systems and subsystems, management and employee security awareness and attitude, the nature and location of access, and the relative sensitivity of the classified information concerned.

A more meaningful approach on which to base both the need to inspect and the interval between inspections would be adoption of a system similar to one in use by the DIS to determine workload requirements and resource allocations. All 13,000 plus facilities participating in the DISP are assigned an alpha designation from A through F under this category system. A description of each DIS category along with the formula used to determine the category assigned can be found at Appendix XI.

Aside from the overall system itself, any security policy that requires inspections of facilities that do not possess classified material should be examined. By way of explanation, facilities that do not possess classified material (nonpossessing) are designated by the DIS as either "access elsewhere" or "dormant." Access elsewhere facilities do not possess classified material on the premises, but their employees do have access at other cleared facilities or

Government installations, i.e., in connection with a visit, attendance at a classified conference or symposium, and so forth. Also included would be firms such as cleared guard companies or temporary help suppliers. Dormant facilities, on the other hand, neither possess classified material nor is access afforded anywhere off the premises. The Committee views the routine inspection of nonpossessing facilities to be a very costly and an unproductive way of addressing minimum security concerns.

The following figures reflect the number of cleared facilities as of March 31, 1984, by category and highest level of classified material possessed by each:

	<u>DIS Categories</u>	<u>No. of Facilities</u>	<u>Level of Possession</u>
	A	45	Top Secret
	A	<u>49</u>	Secret
Subtotal		94	
	B	22	Top Secret
	B	110	Secret
	B	<u>2</u>	Confidential
Subtotal		134	
	C	25	Top Secret
	C	180	Secret
	C	14	Confidential
	C	<u>1</u>	Graphic Arts
Subtotal		220	
	D	28	Top Secret
	D	3,387	Secret
	D	1,402	Confidential
	D	622	Graphic Arts
	D	<u>68</u>	Commercial Carriers
Subtotal		5,507	
	E	5,290	Access Elsewhere
	F	1,859	Dormant
Total		13,104	

As reflected above, there were a total of 13,104 cleared facilities in the DISP as of March 31, 1984. Of this total, 7,149 or about 54 percent of all cleared facilities, do not possess classified information. These nonpossessing facilities also represent 46 percent of the annual scheduled inspections, which appears to be a misdirection of resources.

It should be noted, however, that although nonpossessing facilities represent 46 percent of the scheduled inspections, a larger amount of inspection and inspection-related time is expended on the larger and more complex contractor facilities (DIS categories A and B). Therefore, even if all nonpossessing facilities were to be eliminated from the inspection schedule (routine), this would not, according to DIS representatives, result in a 46 percent reduction in the DIS inspection workload (time expended).

Accordingly, although category E and F (nonpossessing) facilities represent 54 percent of all cleared facilities and 46 percent of all scheduled inspections, a smaller percentage of DIS inspection resources are expended to complete them. Furthermore, very little actual "inspecting" now occurs in regard to these nonpossessing facilities and that which does take place is primarily limited to relatively unimportant and routine administrative checks. Furthermore, the Committee estimates that only about one-third of the time expended to conduct inspections of nonpossessing facilities involves actual in-plant time. The remaining time is devoted to preparation, travel and report writing. In summary, the foregoing facts and figures led the Committee to conclude that routine inspection of dormant facilities (category F) should be discontinued and the inspections of access elsewhere facilities (category E) should be eliminated or significantly curtailed. In this regard the Committee recognize that functions and services performed by cleared personnel of access elsewhere facilities

must continue to be inspected, which in most cases could be given appropriate oversight and attention when inspecting the industrial facility where access is gained. However, certain access elsewhere facilities will have to continue to be inspected under current procedures due to their access at numerous industrial facilities or because they are performing at Government installations where appropriate industrial security oversight is not provided.

A review of the inspection scheduling policy also led the Committee to conclude that sufficient flexibility may be lacking. Although inspection schedules may be advanced for cause, i.e., conducted before they normally fall due, the policy does not appear to permit the exercise of appropriate judgment at the field office level. The Committee believes local management to be in the best position to assess the relative security posture of its assigned facilities. Similarly, local management must have the flexibility to adjust its workload to eliminate "peaks and valleys," to be responsive to the needs of the program, and to make similar adjustments based upon recurring or unusual exigencies.

At present, inspections which are not completed during the month scheduled are considered "slipped" actions. Higher management frequently looks upon these slipped inspections in a negative way, e.g., unable to complete assigned workload. In fact, slipped inspections may be brought about for a variety of reasons, most of which are entirely justifiable and have nothing to do with resource or work performance shortcomings.

To assure a "favorable" slippage rate or one comparable to national averages, local managers sometime resort to playing the numbers game to improve statistics. For example, a category A or B facility may be slipped one or two months to enable inspection of scores of smaller facilities. Even more

alarming to the Committee is that stringent control and reporting of slipped inspections discourages local managers from advancing inspections for those facilities in need of greater assistance or oversight. If these managers concentrate effort at facilities of greatest need, they risk an increase in their slippage rate (and higher headquarters disfavor). Accordingly, any change to the inspection schedule policy must include the flexibility to permit local managers to manage.

Recommendation:

That the current inspection schedule prescribed by paragraph 4-103a, "Industrial Security Regulation," be replaced by a system that more effectively considers the volume and complexity of classified activity. The new system should also include sufficient flexibility to enable local managers to adjust workload and concentrate effort where most needed. Furthermore, that routine inspections of "dormant" facilities be discontinued and that inspections of "access elsewhere" facilities be eliminated or significantly curtailed.

8. Reporting of All Foreign Travel by Contractor Personnel

Discussion:

Current regulations require all cleared contractor employees to report "intended travel to or through a Communist country." Patterns of foreign travel to certain non-Communist

countries are also a potentially significant indicator of espionage.³

3. Recent news articles in the Washington Post highlight the significant relationship between espionage and foreign travel. An October 3, 1984 article, "East German Woman Charged with Spying," states:

... A Soviet national identified as 'Misha' approached a U.S. Army sergeant stationed in West Germany three years ago and asked him to work for the KGB.

After reporting the contact to the Army Intelligence Command, the sergeant pretended to go along with the approach, and, on KGB instructions, secured a job with Army Intelligence.

The sergeant later met twice with Soviet agents at the Soviet Embassy in Mexico City. He promised he could deliver confidential information, and in return received \$6,500 and promises of \$500 monthly.

An October 4, 1984 article, "FBI Agent Charged in Espionage," said:

The FBI said its agents separately trailed Miller from the FBI's Los Angeles Field Office and Ogorodnikova from her home on Sept. 12 to a rendezvous in a Los Angeles parking lot where he got into her car and handed her a legal-size envelope. It said Miller acknowledged last Friday that on that occasion he had met her to discuss traveling together to Vienna 'in order for him to meet a person whom Svetlana Ogorodnikova described as an important person in her government.'

An October 13, 1984 article, "Ex-Agent, Soviets Indicted as Spies," said:

A federal grand jury yesterday returned a 13-count conspiracy, espionage and bribery indictment against a former FBI agent and two Soviet immigrants

The indictment charged former FBI agent Richard W. Miller, Ogorodnikova and her estranged husband, Nikolai Ogorodnikov, in a scheme to deliver classified government information to the Soviet Union in exchange for \$50,000 in gold and \$15,000 in cash Miller was to receive after a trip to Mexico.

The only item of value Miller received from the Soviet couple, according to the indictment, was a \$675 trench coat bought for him before a proposed trip with Ogorodnikova to Poland.

Foreign travel was also a pertinent factor in the James D. Harper espionage case as well as previous espionage cases involving William Bell at Hughes Aircraft, Los Angeles, California, and Christopher Boyce and Daulton Lee at TRW Systems Group at Los Angeles. (See Appendixes VIII, IX and X.)

Senior representatives of one U.S. counterintelligence organization advised the Committee that recent experience with Communist intelligence services' operations indicate these hostile intelligence services (HOIS) are meeting with increasing frequency outside the United States in third countries.

A a simple "fill in the blanks" type of preprinted form could be used by cleared contractor employees to report all instances of foreign travel. The purpose for this travel need not be reported and it should not be construed that the individual is seeking either corporate or Government approval for foreign travel. Foreign travel is, of course, the right of any United States citizen. The reporting of foreign travel should be considered as a responsibility and obligation that accompanies the privilege of a security clearance. The reasons for the reporting requirement would be emphasized and explained to employees at security training sessions.

The reports would be submitted to the corporate security office and reviewed by the DIS industrial security representative at appropriate times for indication of a suspicious trend that should be referred to the Federal Bureau of Investigation to aid in neutralizing the HOIS threat in the United States. Reportedly, this requirement of reporting foreign travel should discourage eventually any would-be HOIS agents in defense industry from meeting in third countries and induce them into meeting elsewhere, perhaps in the United States where the risk of detection is greater.

Recommendation:

All cleared employees be required to report to the facility security department all instances of foreign travel for review by DIS representatives during the inspection effort.

SECTION TWO: ADMINISTRATION/OPERATIONS

9. Creation of Separate Advisor and Inspector Roles of DIS Representatives

Discussion:

Equally, as important as the scheduling, focus and application of security inspection assets is the substantive mechanics of the inspection function itself. During each security inspection, DIS industrial security representatives perform a critical review of the procedures, methods and physical safeguards employed by contractors to protect classified material. Concurrently, industrial security representatives are responsible for providing helpful advice and assistance to contractors. A cooperative spirit in providing assistance to contractors is considered vital to the Industrial Security Program. It would be inconsistent, however, to expect DIS industrial security representatives, who only visit a facility every 6 or 9 months, to be both a trusted advisor to the contractor and a critical inspector assiduously preserving the Government's interest. Indeed, the DIS currently maintains statistics on the number of major deficiencies discovered during security inspections. This indicates emphasis by senior management officials of DIS on quantifiable deficiencies rather than the furnishing of guidance to DoD contractors.

Conclusion:

Industrial security representatives of the DIS should be organized and function in a bifurcated manner--a cadre of capable and experienced personnel who would serve as advisors and consultants to DoD contractors; and, a cadre of regulatory inspectors who would perform oversight and ensure contractor

compliance with the Industrial Security Manual for Safeguarding Classified Information (ISM), as well as assess effectiveness of the support to industry provided by DIS advisory personnel. The advisors would consist principally of those DIS personnel selected for assignment on a full-time basis at complex facilities.

Specific responsibilities and frequency of contact of advisory personnel at a particular contractor facility will be determined by the user prioritized sensitivity of the contract, complexity of classified operations, number of cleared personnel, and other pertinent considerations. The Committee believes the unencumbered advisor/consultant function to be a key factor in strengthening security. In general, an advisor's responsibilities would include assisting the contractor in preparing an effective Standard Practice Procedure which adequately implements ISM guidance, as well as other appropriate consultant functions such as expert guidance regarding classification management, automated data processing systems security, operations security, visitor control, security education, foreign travel and public releases. Advisors should also assist DoD contractors in developing a program in which facility security personnel and first-line supervisors are alert to changes in cleared employees' attitude and behavior and other personal circumstances which could impact on the individual's continued security stability.

Recommendation:

DIS should adopt a pilot program in which individual industrial security representatives function either as advisors to industry or as regulatory inspectors.

10. Establishment of a National Industrial Security Hotline

Discussion:

A telephone Hotline could be a vital part of an effective program to safeguard classified information. It provides individuals with a means to report instances of potential espionage operations or the compromise of classified information. Often, people are unaware of the appropriate reporting channels to report instances where they believe classified information was compromised or otherwise inappropriately disclosed. Sometimes, they may have found that other reporting channels have proven unsuccessful, or the channels cannot be used without fear of reprisal.

The importance of federal employees and private citizens as a source of information on fraud and waste in Government programs has been highlighted by the findings in two studies. The Merit Systems Protection Board conducted a survey of 8,600 employees in 115 federal departments and agencies. The survey showed that 45 percent of the respondents had recently observed or had direct evidence of fraud, waste or mismanagement in Government programs and 9 percent had evidence of waste in excess of \$100,000. The Board's study did not include the Departments of Defense and Justice.

In another study, the General Accounting Office (GAO) analyzed 77,000 cases of fraud reported by 21 federal departments and agencies. The GAO analysis showed that less than 9 percent of the cases had been detected by audit, investigation and inspection organizations. Thirty-four percent of the fraudulent acts was detected by federal employees during the normal course of their day-to-day activities.

Based on the success of the DoD Fraud, Waste and Abuse Hotline and the findings of the Merit Systems Protection Board and the GAO, the Committee believes that the establishment of a national security Hotline within the Defense Investigative Service would provide a valuable means to supplement both the DoD Industrial Security Program and the DoD Information Security Program.

The objectives of such a program, to deter and identify unauthorized disclosures of classified information, should be clearly spelled out and included in a formal charter. Program oversight should be vested in the Office of the Deputy Under Secretary of Defense for Policy.

The DoD Security Hotline should have wide publicity, within and outside of the Government, and national security interests and patriotism should be emphasized as the motivation for callers using the Hotline as opposed to financial reward or personal recognition. Operating procedures for the DoD Security Hotline should provide that:

- in appropriate instances, the substance of calls to the Hotline will be shared with facility security managers.

- records of receipt and disposition of all Hotline calls will be maintained by the Defense Investigative Service.

- proper use of the DoD Security Hotline will be included in the security awareness briefings given by the Defense Investigative Service.

The DoD has experienced a problem with unauthorized disclosures of classified information. In a recent espionage case, it was estimated that the results of millions of dollars of research and development efforts in the antimissile defense

area were wasted through the unauthorized disclosure of classified documents. The Committee believes that DoD must use every lawful means available to respond to this problem, including such information sources as federal employees, DoD contractor personnel and private citizens. The real problem faced by the DoD is those instances where security violations occur but go undetected or unreported.

Initial industry skepticism regarding the viability of a national Security Hotline which is centrally administered by the DIS is recognized. Nonetheless, an exemplary Hotline program is currently being administered by the Office of the Inspector General, DoD which focuses on fraud, waste and abuse. During June 1984, the DoD Hotline received a total of 985 contacts (calls, 801; GAO referrals, 17; letters, 167). Of these, 276 merited formal processing for resolution. The DoD, Hotline currently has a total of 1,197 substantive allegations pending resolution. It should be noted that the OIG does not itself examine all substantive allegations. Many are forwarded to appropriate representatives of the Military Services or DoD agencies for investigation and reporting of disposition. Although the DoD Hotline is designed and publicized as a means of reporting (anonymously if desired) fraud, waste and abuse, the system has been frequently used to report allegations of security significance. The potential for security application of the technique is obviously present.

The principal advantage of a national Hotline is that it provides a confidential means for an individual to report a problem. It is imprudent to expect that a procedure such as

"6b.(1)⁴ reports" will achieve the same results as a Hotline. The "6b.(1) reporting" by contractors generally requires that an individual personally inform either corporate security personnel or a supervisor of a perceived problem. Even if other local means of reporting exist, an individual fears that his/her voice will be recognized, handwriting identified, or the substance of the allegation itself will identify the individual. An individual's fear of retaliation negates the practical value of the current reporting procedure. To expect employees to come forward and make adverse information reports to contractor personnel fails to recognize the frailties of human nature.

The ineffectiveness of the "6b.(1) reporting" procedure is further demonstrated by analysis of the Harper espionage case, which involved a relatively small Defense contractor with a limited professional security staff. Ruby Schuler, Harper's accomplice, was secretary to a chief executive officer and was allegedly an alcoholic. If a fellow employee noticed that she suddenly began carrying a briefcase to and from work, visited the company on weekends with James Harper, coupled with her alleged drinking problem, trips abroad, and unexplained affluence, is it likely such an employee would come forward and report these suspicions to corporate personnel? Even if you should answer this question "Yes," is it likely that the firm

4. Paragraph 6b.(1) of the Industrial Security Manual for Safeguarding Classified Information requires that "contractors shall submit reports ... of any information coming to their attention concerning any of their employees who have been cleared or who are in the process of being cleared for access to classified information, which indicate that such access or determination may not be clearly consistent with the national interest Only information which has been confirmed by the contractor as fact need be reported. Reports based on rumor or innuendo should not be made under this paragraph."

would file a "6b.(1) report" to the DIS regarding an executive officer's secretary? Realistically, the answer to both questions would be "No." A national Security Hotline, however, may have overcome the cited reporting impediments.

The value of a national Security Hotline is that it will surface problems and issues that would otherwise remain undisclosed under existing procedures. Problems of immediate interest to the Government, such as an allegation that an individual possessed sensitive classified material at his home, would be investigated by proper Government authorities. Allegations such as employee theft of contractor materials or abuse of sick leave would likely be referred to the facility security department for resolution. It is envisioned that many complaints would merely be recorded by the DIS and forwarded directly to the contractor security department for action deemed appropriate.

Close cooperation between the DIS Hotline administrators and contractor security personnel should ensure that all substantive complaints are prudently and justly acted upon. Undoubtedly, the Security Hotline will be used to report some false and deceitful allegations. The Committee believes, however, that the professional judgment of the DIS Hotline administrators combined, where appropriate, with contractor security expertise will effectively recognize such allegations.

The cost of an "800" national toll-free telephone line is approximately \$11,000 per year. The DoD Inspector General Hotline administration staff consists of seven professionals and two clerical personnel.

The Committee believes that the establishment of a national DoD Security Hotline would provide a vital element of

an effective DoD information security program to deter and detect the unauthorized disclosure of classified information.

Recommendation:

Establish a 2-year pilot national DoD Industrial Security Hotline Program within the Defense Investigative Service and appropriately publicize it.

11. Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities

Discussion:

Based on a nationwide industrial security survey (1978), 95 percent of all classified documents possessed by industry are located at approximately four percent of all cleared facilities. The facilities included in this 4 percent represent the largest and most complex facilities participating in the Defense Industrial Security Program. It would stand to reason, therefore, that DIS industrial security field resources should be disproportionately allocated to such firms.

Present DoD policy requires an inspection of these complex facilities twice annually. Such inspections normally require from two to eight DIS representatives. Figures for the first 6 months of FY 1984 reveal that approximately 125.5 manhours were expended by the DIS on each such inspection, as opposed to an average of slightly more than 10.6 manhours per inspection for all other cleared facilities. The added time expended in these large and complex facilities is intended to increase the depth and scope of the review but sometimes only results in reviewing more areas, documents and containers.

The DIS has recently instituted an enhanced inspection effort at the larger more complex facilities which is designed to provide the inspector(s) a more detailed knowledge of the firm's organizational structure, principal customers, security apparatus and classified programs and projects. However, the application of this increased knowledge only used the inspection effort and not on a continuing day-to-day basis does not provide sufficient coverage for these type of facilities. The DIS representatives must be in a position to accurately assess contractor security systems and procedures, and to make

on-the-spot decisions, recommendations, and improvements daily. The DIS representative's visibility within each facility must also be significantly increased. The DIS representative would serve as an advisor between the contractor and the Government on all contractual aspects impacted by the Industrial Security Program. This ability would necessarily require greater knowledge of contractor operations and, more importantly, details associated with specific programs and projects. Regularly scheduled security inspections would be conducted by other DIS representatives.

The most promising method to achieve the necessary improvements is to encourage the assignment of DIS representatives to industrial facilities on a full-time or near full-time basis. To be effective, however, only the most critical contractors should be involved; industry and Government should jointly develop the guidelines to be followed; assignments of an individual should not be inordinately long or short; and the authority of the resident DIS representative should be expanded to enable the flexibility to make on-the-spot decisions of use to contractors under time sensitive circumstances.

The in-plant representatives approach was used sparingly during the 1950's and early 1960's with some success. However, in-plant assignments were slowly phased out following the implementation of Project 60 in 1965. Project 60 consolidated the Industrial Security Program along with most contract administration functions under the newly formed Defense Supply Agency (now the Defense Logistics Agency). Industrial Security had previously been jointly carried out by the Military Departments. The reasons for discontinuance of the in-plant concept were: poor use of resources, loss of objectivity, and fostering of mutual distrust. The Committee has carefully considered these and other alleged shortcomings and has

determined that if the resident or in-plant concept is implemented responsibly, its merits outweigh the possible disadvantages. It should also be noted that resident Government officials continue to be effectively used at contractor facilities engaged in Special Access Programs.

Conclusion:

The goals and objectives of the Defense Industrial Security Program (DISP) are not being satisfied to the extent possible or desired in regard to the existing system of inspecting and furnishing security oversight to the most complex and sensitive contractor facilities cleared under the DISP. Inasmuch as only approximately 4 percent of all cleared facilities possess 95 percent of all classified documents possessed by industry, to include access to some of our most sensitive programs, industry and Government responsibility indicates a need for an enhanced DIS presence. This presence must be available on a daily basis, tailored to the operations of the contractor and include detailed knowledge of specific classified programs and projects.

Recommendation:

The Director, Defense Investigative Service, should develop and initiate a pilot program in coordination with industry for the assignment of industrial security representatives on a full-time or substantially full-time basis at certain complex and particularly sensitive contractor facilities.

12. Establishment of a Graded Defense Industrial Security Program Inspection Rating System

Discussion:

The DoD should change the existing security rating system used to evaluate contractors' security systems established for the safeguarding of classified information. At present, defense contractors are estimated to possess approximately 16 million DoD classified documents to enable them to provide the goods and services that the Department has contracted for.

During a security inspection, Defense Investigative Service industrial security representatives evaluate the contractor's security system and prepare an Industrial Security Inspection Report (DD Form 696) on the results of the inspection. The inspection includes a multitude of elements ranging from examining documentation for facility security clearances to review of international operations of the contractor. The industrial security representatives making reviews are required to comment on deficiencies noted during the inspections and the on-the-spot corrective actions taken by the contractor. The industrial security representative is also required to provide narrative comments regarding the contractor's efforts to correct previously reported deficiencies and to make an evaluation of the contractor's security posture in relation to facilities of other contractors that are of a comparable nature and size. Outstanding features of the contractor's security system (e.g., training program, document control, and so forth) are also to be commented on by the industrial security representative.

Based on the overall evaluation of the contractor's security system, the industrial security representative must, under the current provisions of the "Industrial Security

Regulation," assign a rating of either "satisfactory" or "unsatisfactory" on the Industrial Security Inspection report.

Under current procedures, procuring organizations are advised of conditions disclosed by DIS inspections resulting in any unsatisfactory ratings. Upon reinspection in 30 days by DIS, if the condition is not corrected, the same organizations are so advised, and at their discretion may terminate the contractor's effort or withdraw their classified documents.

In FY 1984, the Defense Investigative Service only had 14 inspections of contractor facilities result in an "unsatisfactory" rating. In FY 1983, only 5 contractors received an "unsatisfactory" rating.

The low number of "unsatisfactory" inspection ratings given contractor's facilities may be considered a tribute to the efforts of the contractors to maintain effective security systems to safeguard classified information entrusted to them. On the other hand, it could be indicative of a reluctance on the part of the industrial security representative to assign "unsatisfactory" ratings because of the adverse impact on the contractor.

The Committee believes that the latter could be just as true as the former and that the industrial security representative may lean towards assigning a "satisfactory" rating when an inspection discloses deficiencies showing that the contractor's systems are marginal at best. While the Defense Investigative Service only rated 14 contractor facilities as "unsatisfactory" in FY 1984, the Committee found that 628 facilities were rated as having major deficiencies and 7,458 facilities received letters of requirements to correct administrative deficiencies. Usually, only major deficiencies (system failures) require a DIS reinspection within 30 days.

Generally, facilities having only minor deficiencies are not subject to reinspection. Contractors are currently allowed several major deficiencies without being rated "unsatisfactory."

The Committee feels that the DoD security program rating system should be changed to include "Superior," "Satisfactory," "Marginal" and "Unsatisfactory." The Committee also believes that industry management should be made aware of borderline conditions indicated by poor security practices detected by industrial security representatives during inspections of their facilities. The rating system recommended would:

- More accurately reflect the security posture maintained by the contractor;
- provide more information to contracting officers in the contract pre-award process for classified contracts.

With regard to the pre-award selection process, we also feel that the Defense Investigative Service should play an advisory role in the process. We found little evidence that contracting activities maintained a close liaison with the Defense Investigative Service before the award of classified contracts.

Satisfactory inspection ratings presently assigned by the DIS, which involve major reported deficiencies, are sometimes perceived by procurement activities and security administrators as reflecting a poor overall security posture of a facility, when in reality the overall security posture may be quite good but borders on unsatisfactory. This condition prevelantly exists with larger facilities where many major deficiencies may exist. Therefore, the Committee recommends that the additional rating of marginal be established to reflect an accurate evaluation of the overall security posture of the facility and to highlight borderline satisfactory ratings..

Superior ratings should only be assigned when a contractor has taken extraordinary measures to maintain an overall security posture in comparison with facilities of a comparable size and complexity. Such measures could include major capital expenditures to enhance the facilities security posture or extensive security awareness training of facility personnel and so forth.

Recommendation:

The DoD security inspection rating system be changed to provide for ratings of "Superior," "Satisfactory," "Marginal," and "Unsatisfactory." Moreover, DoD contracting activities should maintain close liaison with the Defense Investigative Service before the award of classified contracts.

13. Specialized Training Program for Accrediting Contractor Security Personnel

Discussion:

In today's business world professionalism is becoming more and more important, and certification is becoming the measure of a professional. The industrial security profession is no exception. As demands on today's industrial security professional increase, as their responsibilities grow in direct proportion to reliance upon them by chief executives and organization management, as business technology grows more and more complex - certification becomes much more than just a designation. Its mark of excellence may indicate professional recognition, career advancement and personal satisfaction.

The DoD Industrial Security Program provides the means for industry and the Government to share classified information, and the program benefits both. Through sharing, the Government can acquire the goods and services needed for our national defense, and industry reaps the benefits of participating in the vast economic market the DoD provides for products and services. Thus, both the Government and industry have a vested interest in protecting classified information entrusted to DoD contractors.

The first line of defense against the compromise of classified information and espionage is an effective industrial security program and qualified professional people to achieve the program objectives. The estimated 16 million classified documents entrusted to defense contractors for safeguarding and storage during the contracting cycle is of paramount interest to hostile intelligence services. Recent espionage cases support this thesis. Classified documents entrusted to contractor personnel cover a vital spectrum of information on

inexpensive spare parts to expensive, leading edge of technology weapons systems that must be protected in the national interest.

As part of the Committee's review, we sought to examine the career field for security personnel as it exists in industry. We found that an extensive formal training program for the career field was essentially nonexistent. We found that outside of a 1-week resident and field extension course presented by the Defense Security Institute, Richmond, Virginia, other security educational opportunities were minimal. The Security Institute's course was geared to familiarize the contractor personnel with the DoD Industrial Security Program.⁶ Attendance at the Institute's course was voluntary and was offered free to industry participants. During FY 1983, about 1,400 defense contractor personnel attended the course. However, there were no follow-up courses offered by the Defense Security Institute to focus on the operational and managerial aspects of a total security system.

Unless a contractor does or wants to do classified business with the Government, there is no involvement with the DoD Industrial Security Program. Thus, the genesis of security personnel in industry begins when contractors have interest to provide goods or services to the DoD under classified conditions. Consequently, industry has no available pool of expertise to tap for personnel knowledgeable of the Defense Industrial Security Program (DISP). In fact, industrial security personnel of the DIS are "fair game" for industry

6. DoD Manual 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," March 1984

recruitment. We recognize that it is the contractor's prerogative to select their employees to fill security positions.

Traditionally, people hired for security positions lack security expertise unless they are hired away from the Government or other contractors. This is especially true of the thousands of smaller defense contractors, which comprise the bulk of contractors participating in the DISP.

Many individuals appointed to security positions, and entrusted with safeguarding classified information, have only an administrative or clerical background. While these people may experience little difficulty in the administrative aspects of the program, the Committee believes that difficulty may be encountered in establishing and overseeing a "total system approach to security."

Once a contractor starts to conduct classified business with the Government, a Security Agreement (DD Form 441) is executed between the contractor and the Department. Under the terms of the agreement, contractors are required to adequately safeguard classified information under their control in accordance with the DoD Industrial Security Manual. This includes appointment of a security officer/supervisor. The Manual stipulates no specific qualifications for this official except that the person be a United States citizen and have an appropriate security clearance.

The consequences of inadequate information security systems are serious. For example, if information is compromised on a new weapon system, the DoD not only loses an investment of time, money, and research and development efforts, but it can also lose the military advantage the system may provide. In major technological breakthroughs, if we are

building a new system, any compromise of information concerning the system may allow our enemies to develop countermeasures to offset any technological/military advantage. Only part of the solution to such security problems can be corrected by issuing new security regulations or directives. Failure to adhere to existing security requirements is the real problem.

Despite concerted efforts by the Government and defense contractors, we have not eliminated security leaks, unauthorized disclosures and cases of espionage. Admittedly, security in most cases is a personnel problem. The contractor security officer is the first line of defense against unauthorized disclosures of classified information. Contractor security officers/executives have the ability to influence those personnel in their company working with classified information. They must set the example in good security practices and ensure that the security functions are properly financed and supported. They must be able to discern weakness in the security systems and indications that the reliability of persons entrusted to safeguard classified material may be suspect. The Committee's examination of past espionage cases revealed the following indicators to be present: unexplained affluence, attempts to gain unauthorized access to classified information, unauthorized removal of classified information, and patterns of foreign travel. But, the indicators were not acted upon until the damage was done.

Considering the absence of a formal career program in industry to develop industrial security personnel, and the limited training available through the Defense Security Institute, the Committee feels that the DIS should take the initiative and develop an optional educational program for industrial security personnel.

The comprehensive instructional program developed by the Service should lead to certification of individuals as Industrial Security Specialists. Program content should include industrial security procedures and reporting, physical security, information security, computer security, sensitive technologies, human reliability factors and hostile intelligence collection methods and procedures. This list of subjects is by no means complete. The developed program of instruction should be done in conjunction with industry and Government security managers, executives, and educators. Minimal educational and experience requirements should be prescribed for entrance into the program. Finally, the training program should not be mandatory, however, the benefits of industry participation seem obvious, particularly for smaller firms newly engaging in classified contracts. Costs of the program should be shared by industry and the Government.

Recommendation:

The DIS provide a formal certification/accreditation training program for contractor industrial security personnel. The training program need not be mandatory.

14. Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor Personnel

Discussion:

Currently, the DIS is seldom informed of criminal investigations involving cleared contractor facilities or cleared contractor personnel. At the earliest practical time, the DoD criminal investigative organizations - the Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Investigative Service, and the Air Force Office of Special Investigations, should notify the DIS of investigations indicating criminal conduct by cleared DoD contractors and contractor personnel. Such notification must be based upon a decision by the investigative authority that an ongoing investigation will not be jeopardized. The notification will influence the scope and intensity of the DIS industrial security oversight process or may result in revocation of clearance(s), as appropriate. Implementation of the recommendation will require each DoD criminal investigative organization to determine during each investigation of a DoD contractor or contractor employee whether the facility or individual has a clearance. In the case of a facility, this may be easily determined by contacting the nearest DIS regional office; in the case of an individual this may be determined by contacting the facility security officer or contacting the Defense Industrial Security Clearance Office.

Conclusion:

The absence of the criminal investigative information adversely affects the DIS industrial security responsibility.

Recommendation:

At the earliest practical time, DoD criminal investigative organizations should notify the DIS of criminal investigations that indicate criminal conduct on the part of cleared DoD contractors and contractor personnel.

SECTION THREE: LEGISLATION/REGULATIONS

15. Legislative Base for the Defense Industrial Security Program

Discussion and Background:

There is no general criminal statute that prohibits the public disclosure of classified information as such. There are statutes that prohibit disclosure of certain kinds of extremely sensitive classified or classifiable information (atomic secrets and communications intelligence information, see 18 U.S.C. 798 and 50 U.S.C. 783) and there is one statute that prohibits government employees from making unauthorized disclosures of classified information to foreign agents. (See 50 U.S.C. 783.) In addition, there are specific provisions set forth in 18 U.S.C. 798 which prohibit any person from disclosing to any unauthorized person certain specific kinds of classified information.

The Espionage Act, 18 U.S.C. 793, is very broad but it is doubtful that it could be interpreted to cover all foreign relations and intelligence matters. Section 793(a) and (b) prohibit entering an installation or obtaining or copying a document "connected with the national defense" for "the purpose of obtaining information regarding the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation." Section 793(c), (d) and (e) make criminal the knowing receipt of material obtained in violation of other espionage provisions, the communication of defense-related material or information to any person "not entitled to receive it," and retention of such information. Section 793(c) prohibits any "knowing" receipt, and 793(d) and (e) prescribe willful conduct. Activities relating to the gathering of

information, where the primary use is not to "harm the U.S." or "advantage a foreign nation" but rather to further public speech, is at least arguable beyond the reach of 793(a) and (b).

These statutes require that at a minimum the information disclosed be entered into evidence and that the prosecution prove that either it was classified or that it was in fact national defense information. To do this requires declassification of the information and confirms the accuracy of the information disclosed. It is important to note that the Government must further prove that the person disclosing the information could reasonably believe that the information could harm the United States or aid a foreign nation.

A law providing criminal penalties for the unauthorized disclosure of classified information would close a loophole that exists in the law. It would be consistent with other laws that punish the unauthorized disclosure of information. See 5 U.S.C. 552a(i)(1) (information disclosed in violation of the Privacy Act); 18 U.S.C. 1902 (disclosure of crop information); 18 U.S.C. 1905 (disclosure of trade secrets).

It should be noted that Congress recently passed criminal legislation regarding improper access to and disclosure of information stored in federal computer systems.

Conclusion:

The Committee believes that the way the current laws are drafted prosecution of individuals who release classified information to unauthorized individuals is difficult. The statutes do not cover all cases involving the release of information on foreign relations and intelligence.

Recommendation:

Establish a working group to draft new legislation that would carefully address the problems of prosecution including the need to declassify the information involved in the prosecution.

16. Legislation to Limit Administrative and Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures Themselves

Discussion:

In the last few years security clearances have been ordered reinstated by the Merit Systems Protection Board and the courts. Revocation and reinstatement of clearances are sensitive national security decisions which, throughout our country's history, have been made by the agencies. The Board has asserted jurisdiction over the revocation of a clearance as well as the removal action. The landmark case is Hoska v. Department of the Army, 677 F.2d 131 (D.C. Cir. 1982). In that case the United States Court of Appeals for the District of Columbia held that the Board had jurisdiction to examine the security clearance revocation when it formed the basis for a removal action. Following the Hoska decision, the Board began to assert jurisdiction on this issue. See, Schwartz v. Department of the Army, MSPB Docket No. NY0752811026 (September 27, 1983).

The "nexus" with which the Board is concerned has been defined by the Board as follows:

In law as well as logic, there must be a clear and direct relationship demonstrated between the articulated grounds for an adverse personnel action and either the employee's ability to accomplish his or her duties satisfactorily or some other legitimate government interest promoting the 'efficiency of the service.'

Merritt v. Department of Justice, MSPB Docket No. DH0752209058 at 16 (June 8, 1981), quoting Doe v. Hampton, 566 F.2d 265, 272 (D.C. Cir. 1977).

Historically, the courts have shown a reluctance to substitute their judgment for the "unique insights" of agencies in the national security area. See, for example, Military Audit Project v. Cases, 656 F.2d 724 (D.C. Circuit 1981). The issue to be decided is not performance but entrusting the individual with national defense intelligence, and foreign policy secrets. The issue of reliability in security clearance cases is not one of deciding satisfactory performance. The national security should not be risked to afford drug abusers and alcoholics the opportunity to prove they can safeguard our state secrets. Simply put, an individual who has not demonstrated reliability should not be entrusted with national security information.

Congress has evidenced an intent to preclude Board review of security matters. Title 5 U.S.C. 7532 grants heads of agencies the authority to suspend and remove employees "in the interest of national security." Congress specifically provided that suspensions and removals effected under this authority are not reviewable by the Board (Title 5 U.S.C. 7502, 7512). Disclosure of classified information can produce irreparable harm to the defense of the United States.

The Committee believes that such discretionary decisions of executive officials in the national security area are subject to judicial review but that review should be extremely limited. Barring agency deviation from its own regulations and procedures which may justify judicial relief, the courts should not look behind the exercise of that discretion.

Recommendation:

A panel should be formed to study legislative initiatives to limit administrative and judicial review of DoD personnel security adjudications to the adjudicative procedures and to exclude review of the adjudicative decisions of the Directorate of Industrial Security Clearance Review.

17. Authority to Suspend and Debar Contractors for Serious Security Infractions

Discussion and Background:

The authority set forth in Part 9 of the Federal Acquisition Regulations (FAR) to suspend and debar contracting authority has been successfully used to protect the Government from contractors that are not performing properly on contracts, are engaging in illegal conduct that is detrimental to our overall defense effort, and cannot affirmatively demonstrate their responsibility to perform on federal contracts.

While the DIS has the authority to remove a facility clearance, there is no general recognition within the DoD that the basis for removal of a facility clearance may also serve as the basis of suspension and debarment. In fact, as soon as corrections are made in the security program of the company, the DIS must reinstate the facility clearance. The Committee believes that additional authority is required to strengthen the program. The incentives to perform well on security issues are lacking. Failure to maintain adequate security on a contract is also a failure to perform in accordance with the requirements of the contract and should lead to consideration for suspension and debarment. Failure to perform properly on one or more federal contracts, or a willful failure to perform, are clearly grounds for debarment (FAR 9.409-2(b)). If a contractor was aware that the DIS could not only suspend the facility clearance but that the cognizant DoD suspension and debarment authority could also suspend the contractor for a particular length of time, there would be a greater incentive to improve the security program. Senior representatives of the Federal Bureau of Investigation expressed strong support for the expansion of such suspension and debarment authority.

Conclusion:

Any use of authority to suspend or debar must, of course, be applied judiciously by DoD. The Committee believes that to improve the existing industrial security program, the DoD suspension and debarment authorities should consider serious security violations as the basis for such administrative actions.

Recommendation:

The Committee recommends amending DoD FAR Supplement 9.470 to clearly identify security violations that may be used as the basis for suspension and debarment. The DIS should be required to provide notice to the cognizant DoD suspension/debarment authority of all significant security violations on the part of cleared contractors or their cleared employees.

SECTION FOUR: PERSONNEL SECURITY

18. Revised Scope of Personnel Security Investigations

Discussion:

The Department of Defense presently uses a multi-tiered investigative approach to clear individuals before giving them access to classified information. The investigative requirements and standards applicable to each tier generally depend upon whether the applicant is a DoD civilian employee, a uniformed member of the armed forces or an employee of a cleared contractor facility. There are exceptions, such as persons employed under any of the foregoing groups who require access to Sensitive Compartmented Information (SCI). All persons requiring access to SCI are subject to a Special Background Investigation based on investigative standards and procedures mandated by Director of Central Intelligence Directive (DCID) No. 1/14. The following is an overview of DoD investigative requirements.

INVESTIGATIVE REQUIREMENTS -
DoD-GRANTED CLEARANCES¹

<u>ACCESS AUTHORIZATION</u>	<u>CIVILIAN</u>	<u>MILITARY</u>	<u>CONTRACTOR</u>
SCI ²	SBI	SBI	SBI
<u>CLEARANCE</u>			
Top Secret	BI ³	IBI	IBI
Secret	NACI ⁴	NAC	NAC
Confidential	NACI ⁴	NAC	NAC

1 Excludes contractor-granted Confidential clearances.

2 Mandated by DCID 1/14.

3 Background Investigations (BIs) are mandated by E.O. 10450. They are the same as an IBI with the addition of neighborhood and education checks. The DIS conducts these investigations.

4 National Agency Checks with written Inquiries (NACI) are mandated by E.O. 10450. The OPM conducts these investigations. They consist of written inquiries and record searches covering specific areas of subject's background during the past 5 years. Includes written inquiries to employers, law enforcement agencies, educational institutions, and individual character references.

As concerns military and contractor personnel, two parallel types of investigations are currently conducted, namely a Special Background Investigation (SBI) or an Interview Oriented Background Investigation (IBI). The DIS investigative scoping and component parts of the NAC, SBI and IBI are indicated below:

<u>DIS INVESTIGATIVE SCOPE</u>		
<u>NAC</u>	<u>IBI (5 YRS)</u>	<u>SBI (15 YRS)</u>
<u>REQUIRED</u>	NAC	NAC
FBI - IDENTIFICATION CHECKS (CRIMINAL)	CREDIT CHECKS	CREDIT CHECKS
	LAW ENFORCEMENT CHECKS	LAW ENFORCEMENT CHECKS
FBI - IDENTIFICATION CHECKS (SUBVERSIVE)	EMPLOYMENT RECORD CHECKS	EDUCATION RECORD
DCII	EMPLOYMENT SUPERVISORS CO-WORKER INTERVIEWS	NEIGHBORHOOD INTERVIEWS
<u>OPTIONAL</u>		
INS (Foreign born)	DEVELOPED REFERENCE INTERVIEWS	EMPLOYMENT RECORD CHECKS
STATE (Foreign travel)	SUBJECT INTERVIEW	EMPLOYMENT SUPERVISOR/ CO-WORKER INTERVIEWS
CIA (Communist country travel)	SELECTED SCOPING AS NECESSARY	DEVELOPED REFERENCE INTERVIEWS
OTHER FEDERAL AGENCIES (Prior Federal employment)		SELECTED SCOPING AS NECESSARY

Other than the scope involved, significant differences between the IBI and the SBI involve only three elements, i.e., a subject interview is not required for an SBI and neighborhood interviews and education record checks are not required for an IBI. The fact that differences exist between these two types of investigations are not necessarily significant because of the increased concerns associated with access to SCI. Of significance, however, is the DIS-claimed value of the subject interview as opposed to the questionable merits of mandatory neighborhood interviews and education record checks.

The Committee is not suggesting that a single scope investigation be implemented for Top Secret and SCI access, although the single scope approach does offer certain advantages and has been recommended by various individuals and study groups in recent years.

The Select Panel review of the DoD Personnel Security Program in 1982, under the Chairmanship of the Deputy Assistant Secretary of Defense (Administration) favored adoption of a single scope background investigation that would meet requirements for all security clearances and special access authorizations above the Secret level. By way of background, the Select Panel discussion of its single scope proposal is repeated verbatim below:

The DOD policy regarding the scope of investigation required for access to various kinds of classified information above the SECRET level has evolved and been influenced by a variety of factors. Resources have played a predominant role in influencing DOD policy makers gradually to reduce the scope of a DOD BI so that at the present time the DOD does less than any other entity in the Federal government.

Prior to 1976, the DOD had a single scope background investigation that consisted of the following: National Agency Check, birth verification, checks of education and employment records, employment interviews, interviews with six listed or developed character references, plus checks

of local agencies (LACs) (primarily local police) and credit, covering the last 15 years of the person's life, or since the age of 18.

In 1976, due to severe cuts in manpower for the Defense Investigative Service (DIS) imposed by the Congress and the need to conserve resources, the DOD adopted a two-tiered scope of background investigation:

- (1) A standard BI covering only the latest five year period for collateral clearances of military, civilian, and industrial employees who require access to Top Secret information.

- (2) A Special Background Investigation (SBI) covering the latest 15 year period, to meet the scope of investigation prescribed in Director of Central Intelligence Directive 1/14, for access to SCI or other special access programs.

In June 1981, the Deputy Secretary of Defense authorized a new type of background investigation known as the Interview-Oriented Background Investigation (IBI) to be conducted by the DOD, in lieu of the standard 5-year scope BI, which would serve as a basis for granting a Top Secret collateral clearance. At the same time, it was proposed that the IBI also become a substitute for the SBI for granting SCI access. This proposal by the Deputy Secretary of Defense resulted in considerable objections from elements in the intelligence community as well as from others in the Executive Branch.

Since 1982, the IBI has been enhanced and some improvements have also been made to the SBI. Nonetheless, room exists for further improvement. Indeed, ever-increasing investigative demands on an already over-burdened Defense budget dictate that additional changes be made, provided they can be accomplished with no material impact or only negligible impact on the quality of the overall investigative effort. For example, the Director, DIS, advised in September 1984 that personnel security investigative cases opened in FY 1984 will exceed cases closed by about 10,000, in spite of the fact that DIS will complete 15,000 more investigations in FY 1984 than in any other year since its inception (1972).

In addition, under the provisions of revised DoD investigative policy initiated in early 1983, a periodic reinvestigation (PR) is required every five years for military, civilian and contractor personnel possessing a Top Secret (TS) clearance or SCI access. In this connection, the Director, DIS, estimated that by the end of FY 1984 there will be 280,000 persons with SCI or TS clearance five or more years old which will require a PR. Again, change appears necessary to thwart immediate and long-term problems.

In 1983 a Personnel Security Survey conducted under the auspices of the Director of Central Intelligence Security Committee (the Investigative Standards Working Group (ISWG) Study) concluded the following in regard to the productivity of various investigative sources:

In rank order, the most productive as unique sources of data resolved against the individual (clearance applicant) were the polygraph examination, the subject interview, the employment personal interview, the police check, and the developed source.

The rank order for productivity of adverse data placed the polygraph examination and subject interview first and second, respectively, followed by the police check, the developed source and the employment personal interview.

Personal interview sources generally appear to be more productive than record sources.

The residence check was a unique source in less than two percent of the adverse or the resolved against data but did overlap with other sources in slightly more than three percent of the resolved against data. As might be expected, education checks (both records and personal interviews) and listed references fared even worse as unique sources.

Given that a clear consensus of professional adjudicators also agree with the ISWG assessment of the relative value of the subject interview as well as the relative unproductive nature of education and residence (neighborhood) checks, the Committee concludes that appropriate adjustments are necessary.

Noteworthy is the fact that the subject interview is not now a routine element of an SBI but that neighborhood interviews and education checks are so included.

DCID 1/14 identifies the minimum standards for the SBI concerning education and neighborhood checks as follows:

Verification of the individual's financial status and credit habits through checks of appropriate credit institutions or, if such checks are not productive, through interviews with knowledgeable sources covering all areas of employment, residence, and education in the most recent seven (7) years. Interviews with neighbors in the vicinity of all the individual's residences in excess of six (6) months throughout the most recent five (5) year period. This coverage shall be expanded where the investigation suggests the existence of some questionable behavioral pattern.

Conclusion:

The Committee concludes that education and neighborhood checks should be eliminated from DCID 1/14 as required investigative coverage (although these leads may be conducted if circumstances warrant) and that DCID 1/14 include subject interviews as required investigative coverage. Therefore, the Committee opines that with the exception of the period of investigative coverage (5 years for IBI and 15 years for SBI), the "single scope" investigations so sought after in recent years should be adopted.

Recommendation:

That negotiations be initiated to amend the Director of Central Intelligence Directive No. 1/14, dated 1 September 1983, to require subject interviews as part of the minimum investigative standards for the SBI and that currently prescribed neighborhood and education check/verifications be deleted from said DCID as required elements of investigative coverage.

19. Enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances

Discussion:

Proliferation of Security Clearances

At the end of March 1984, a total of 1,031,151 active personnel security clearances were on hand for industry personnel. These clearances were broken down by classification level as follows:

Top Secret	114,726
Secret	911,521
Confidential	4,904

The foregoing figures do not include Confidential level security clearances granted by industry to its employees.⁶ The

6. Contractor employees who require access to classified information at a level no higher than CONFIDENTIAL may be eligible for a contractor-granted CONFIDENTIAL clearance. Such clearances may remain valid, unless otherwise revoked, so long as the individual is continuously employed by the same contractor. Only U.S. citizens who produce specific written proof of U.S. citizenship are eligible. Company-granted clearances are not valid for access to RESTRICTED DATA, FORMERLY RESTRICTED DATA, COMSEC, SCI, ACDA classified information, or classified NATO information (except NATO RESTRICTED). Criteria: Employment records check; no evidence that applicant is a representative of a foreign interest; no evidence that any prior clearances had been denied, suspended or revoked; and no information is known to indicate that applicant's access would not be clearly consistent with the national interest. In addition, the Government must review all cases in which an individual indicated that he/she has resided since 18th birthday or past 15 years in a Communist country or who lists relatives that reside in such countries.

outstanding number of company-granted Confidential clearances cannot be determined precisely because the records of such grants are not maintained by the Department of Defense (DoD). However, it is estimated that between 300,000 and 400,000 employees are currently cleared Confidential by their employers. Therefore, approximately 1.4 million people in industry are security cleared for access to classified information.

From fiscal year (FY) 1979 through FY 1983 the number of DoD personnel security clearances granted to industrial personnel increased nearly 44 percent. The DIS issued over 250,000 clearances in FY 1984 alone. In March 1984, the Defense Industrial Security Clearance Office (DISCO) received nearly 26,000 requests for personnel security clearances, the largest monthly figure ever recorded. The large number of clearances being requested severely taxes the ability of the DIS to produce a quality investigation within a reasonable timeframe. Either DIS personnel security and investigative resources must be enhanced or the number of clearance requests must be reduced, or a combination of the two. If one or the other does not occur in the near future, the backlog will increase until average processing times are unacceptable.

Certainly, some of this increase in recent years can be attributed to Reagan Administration initiatives to "re-arm America." The B-1 Bomber, Cruise and MX Missile programs alone require large numbers of industry personnel to possess security clearances. However, the years immediately following the end of the Vietnam War through the Carter Administration years, a period that witnessed a general decline in military buildup, failed to produce a corresponding decline in the number of personnel security clearance requests. Therefore, it stands to reason that current military buildup initiatives are only partly responsible for the extremely large number of personnel

security clearance requests received daily by the DISCO for processing.

Based on information furnished by the DIS and the Office of the Secretary of Defense (OSD), far more can be achieved through increased oversight of clearance requests. However, given that all clearance requests are required to be based on a bonafide need for access to classified information, any measure aimed at reducing the number of clearances would appear to be at cross purposes with our goal of security clearing whatever number of personnel are required to get the job done.

During the past year, a concerted effort has been made by industry, under the general direction of the DIS, to review all clearance requests and eliminate those which were not considered truly necessary. Further, at the request of the OSD, the DIS has been asked to participate and oversee the Clearance Reduction Program Within Industry. This requires, in part, DIS security inspectors to critically review, during each inspection, contractor requests for clearance to assure that proper justification exists. The increased vigilance by industry and Government is expected, however, to provide only negligible short term relief. Similar concerted efforts over the years have not achieved significant or lasting success.

A large number of personnel security clearance requests received each year for processing involve contractor employees who do not require access to classified information. By way of example, in July 1984, the Director, Directorate of Industrial Security Clearance Review (DISCR) cited several examples of clearance applications which he felt were suspect. The Director noted that plumbers, electricians, and custodial personnel were being processed for clearances when access to classified information for such personnel would be highly

unlikely. The DISCR is the DoD office responsible for adjudicating industrial cases where significant adverse information is present in the applicant's background. That office sees less than five percent of all cases processed. Accordingly, if the cases cited by the DISCR are representative of all clearance applications processed by the DISCO, and there is little reason to believe differently, it would appear that a serious problem exists and that our current system of review is in need of major overhaul.

The Director, DIS, has also taken notice and expressed concern with these suspect personnel security clearance actions. In this connection, he recently asked industrial security field personnel to redouble their efforts at insuring contractor compliance with the provisions of paragraph 20a of the Industrial Security Manual (ISM). This paragraph states, in part, that an industrial employee will not be permitted access to classified information unless the contractor determines that access is necessary in the performance of tasks or services essential to the fulfillment of a classified contract or program and that the contractor process for clearance the minimum number of personnel possible, consistent with contractual obligations. The Director, DIS has similarly requested that increased attention be devoted to contractor compliance with the administrative downgrade and termination provisions of the ISM.

Although personnel security clearances can be administratively terminated if no current or foreseeable future requirement for access to classified information exists, in practice this action is infrequently carried out. Based on information furnished by the DIS, only about 6,000 clearances were administratively terminated in FY 1983. Moreover, numerous contractors have upwards of 90 percent of their total employee population security cleared. By way of example, one

major contractor in California has a total of 35,557 employees and all but 705 are security cleared. Of those 705, it would not be unreasonable to assume that perhaps 400 to 500 of them are in-process for a security clearance. In addition, in May of this year a security official informed the DIS that during a recent company's annual internal Security Awareness Program meeting, 2,360 cleared employees who attended were asked whether they had received access to any level of classified information during the preceding 18-month period. Slightly more than half of them (1,185) responded that they had not. This particular case represents only a microcosm of the problem. Although clearly warranted, material success over the years at administratively downgrading personnel security clearances no longer required has been most disappointing.

Another factor which has contributed greatly to a proliferation of personnel security clearances is what the Committee has characterized as the controlled area mentality. A controlled area generally consists of a building, room, or similar interior space physically separated from a surrounding area and controlled separately. All persons who work or have reason to enter such areas on a regular or intermittent basis are security cleared, usually to the highest level of classified material stored therein. Too little attention is paid to determining precisely what information a person should be entitled to or required to have based on assigned duties or whether access to classified information is required at all. Little distinction is sometimes made between an engineer assigned to a controlled area and a janitor who must enter periodically to perform custodial services. Both are processed for a personnel security clearance although only the former requires knowledge of, and access to, classified information.

The controlled area mentality frequently contravenes the most basic of security precepts, i.e., the need-to-know

principle. In addition, it enables classified document custodians to, in essence, be relieved of their individual responsibility to protect classified material under their personal custody and control from unauthorized persons. Total reliance on a personnel security clearance to determine whether a person is "authorized" is contrary to established DoD security policy, it engenders a false sense of security, and it permits access to our nation's secrets by individuals who do not require knowledge of the information.

The Industrial Security Manual defines an authorized person as one who has a need-to-know for access to specific classified information, coupled with possession of the appropriate level of personnel security clearance. Of these two access prerequisites, need-to-know is clearly the more important eligibility criterion. Notwithstanding this fact, strict adherence to the need-to-know principle is all too often glossed over or ignored in many of the established "controlled" environments.

Many security practitioners themselves justify this unfortunate misconception by arguing, for example, that need-to-know is satisfied if it can be established that a person must regularly enter a controlled area or is otherwise assigned to work in such areas. Such rationale is frequently based on the convenience of not having to escort visitors around the area. It is the responsibility of each document custodian to safeguard the classified material entrusted to him and to prevent access by unauthorized persons, regardless of whether the unauthorized persons are security cleared or not. In summary, the responsibility to protect classified material rests squarely with the user exercising control over it. It does not disappear simply by virtue of security clearing all persons who must work in the proximity of the material involved. Moreover, persons are often assigned to work in

these areas for other reasons when they more properly should have been assigned elsewhere. The controlled area mentality not only contributes to the proliferation of personnel security clearances, but even more importantly, it results in a proliferation of access to the information itself. It is absolutely essential that the need-to-know principle be stressed and adhered to. By so doing the number of clearance requests will be reduced and DoD investigative resources will not be expended unnecessarily.

The problem of excessive personnel security clearances cannot be discussed intelligently without also discussing a parallel problem involving excessive facility security clearances. It is DoD policy that a firm or individual be processed for a security clearance only if there is a need for access to classified information. Personnel security clearances are not permitted to be granted to an employee of an uncleared firm. A facility security clearance must be based on sponsorship by a Government contracting activity or a cleared contractor who wishes to utilize the services of another contractor in a capacity requiring access to classified information. As of March 31, 1984, the number of cleared facilities was over 13,000, an increase of about 20 percent in approximately the last three years. Given the inexorable link between cleared facilities and cleared personnel, the question arises whether the existing and ever-increasing number of cleared facilities is fully justified.

A management oversight visit of a regional office of the DIS in October 1982 revealed that approximately 50 facilities were currently cleared and another 12 to 15 in-process for clearance that did not appear to satisfy clearance eligibility requirements. In a few instances the sponsoring activity actually stated that "access to classified information is not required." The facilities were cleared to perform toilet

cleaning, painting and similar maintenance or service-oriented activities, principally on behalf of a Military Department. Performance of maintenance and custodial services at cleared contractor facilities and user agency installations will rarely require access to classified information. Moreover, the fact that such services may be supported by a classified contract only raises doubt as to the propriety of the assigned classification.

The Committee considers this a nationwide problem and little evidence has been produced to suggest that the problem is being sufficiently resolved. One solution is to eliminate these unwarranted facility clearance requests by adhering to existing procedures specifically designed for the purpose. Paragraph 3-601, DoD 5200.2-R, "DoD Personnel Security Program Regulation," authorizes the conduct of a National Agency Check for contractor employees who require access to sensitive DoD activities under circumstances that do not involve access to classified information. Employees subject to this screening process are permitted unescorted entry when the activity's mission is vital to the national security and its vulnerability to sabotage requires a determination as to the trustworthiness of such contractor personnel. Requests for investigation under the cited paragraph requires the approval of the Deputy Under Secretary of Defense for Policy.

Unfortunately, the above process is relatively unknown and only occasionally used by the Military Departments and DoD components. Consequently, many facilities under contract to perform various service-oriented tasks on installations or aboard vessels that otherwise qualify for processing under paragraph 3-601 of DoD 5200.2-R are routinely processed for a facility security clearance pursuant to the DISP requirements. Although the precise number of such facilities so cleared is unknown, the Committee conservatively estimates that they

number in the hundreds. It is conceivable that as many as one to two thousand facilities may be so cleared. It follows, therefore, that literally thousands of unwarranted personnel security clearances also exist and the problem continues to be compounded daily. Each facility unjustifiably processed for clearance requires large expenditures of resources which would not otherwise be incurred, e.g., security clearance of corporate officials, the conduct of recurring security inspections, and so forth.

At present, contractors are faced with a powerful incentive to process their employees for clearance and to clear them at the highest conceivable level. This is the "real world" aspect of the defense contracting business. Many contractors who have succeeded in holding clearance requests down to the minimum are often victimized by the system for having done so. They may, for example, discover themselves to be at a distinct competitive disadvantage with other contractors who do not strictly enforce DoD personnel security clearance eligibility requirements. The competition, by abusing the system, has an ample supply of cleared personnel to perform on new classified contracts.

To offset this tendency to clear everyone requires that flexible new policies be placed into effect to neutralize the causative factors responsible for the abuse. Until the processing time can be reduced, the tendency for some contractors to use a "shotgun approach" in requesting clearances will continue. Industry cannot afford to have its employees idle for months, or to place employees in a temporary position while they await the granting of their clearance. Workload notwithstanding, there is a benefit derived from having employees cleared or in-process for clearance even though immediate or foreseeable access to classified information is not in evidence.

A major 1982 review of the DoD Personnel Security Program⁷ confirmed the deleterious effects of the excessive time lag experienced in receiving the results of a DIS investigation. The review did not address the parallel and potentially more damaging effects incurred by industry from such time lags. To delay the full participation of thousands of contractor employees on classified programs and projects while they await the results of DIS investigations, especially considering that only about one in 1,400 applicants is ultimately denied an initial clearance, is extremely costly and encumbers defense production.

In summary, a proliferation of personnel security clearances does exist and a substantial percentage of the investigative workload is avoidable. Although elimination of all unnecessary clearance requests is simply not attainable, significant improvement is well within reach and should be pursued with vigor by both Government and industry. Government cannot and should not be expected to solve this problem alone. Each sector shares a joint responsibility to rigidly scrutinize initial clearance requests and to carefully monitor continued clearance requirements. In addition, a way must be found to permit the timely granting of those personnel security clearances that are truly required. Only bold new initiatives can be expected to achieve an immediate and long-term solution.

Interim Clearance Procedures

The "Industrial Security Regulation" (DoD 5220.22-R) currently includes an interim clearance procedure which may, if

7. Select Panel Review of the Department of Defense Personnel Security Program, March 16, 1982.

widely practiced, provide the necessary relief. This interim clearance procedure is currently used only in emergency situations in order to avoid critical delays in pre-contract negotiations or contract negotiations or under similar conditions of contract performance. The policy permits the issuance of a personnel security clearance based on completion of lesser investigative requirements than would normally be required for a given level of collateral clearance. The current interim personnel security clearance investigative requirements are as follows:

TOP SECRET

- (1) Absence of significant derogatory information on Personnel Security Questionnaire (PSQ);
- (2) Completion of a favorable National Agency Check (NAC); and
- (3) Initiation of a Background Investigation (IBI).

SECRET/CONFIDENTIAL

- (1) Absence of significant derogatory information on PSQ;
- (2) Favorable DCII check pending completion of the NAC.

The use of interim personnel security clearance procedures offers several distinct advantages. Paramount is the rapid turn-around time between the clearance application and the issuance of the interim clearance. The slowest turn-around time involves the granting of an interim Top Secret clearance based on a completed National Agency Check (NAC) and initiation of the background investigation. Except for periods of unusually high activity, the normal turn-around time for completing standard NACs is about 15 to 30 days. Compared with the average time of just under 100 days to finalize Top Secret clearances based on a completed IBI (DIS April, 1984, Quarterly Report), use of interim clearance procedures would permit the granting of Top Secret clearances in an average of 15 to 30 days, a substantial savings in processing time with no

substantive reduction in investigative coverage. The issuance of Secret clearances would be reduced from a total processing time of just under 60 days to about 7 to 14 days using interim clearance procedures. This savings in processing time would permit industry to increase its efficiency in performing on classified contracts which would also tend to reduce overall contract costs. Adoption of a standard system incorporating interim procedures would not reduce currently required investigative coverage, it would simply permit access by individual employees on an accelerated basis with no appreciable increase of risk.

DIS records indicate that from FY 1978 through FY 1983, the DISCO granted 63,329 interim personnel security clearances, 1,933 Top Secret, 60,659 Secret, and 737 Confidential. Nearly 13,000 interim clearances were granted by the DISCO in FY 1983 alone, which represents 6 percent of the total clearances issued. Given that issuance of clearances under interim procedures has not proven unduly risky, i.e., evidence suggests that all such clearances were ultimately made final upon completion of required investigative requirements, and were accomplished timely (normally between 1 to 30 days), the Committee believes similar procedures could be used system-wide. Nationwide, clearance denials are much less than one percent annually (.04 in FY 1982 and .06 in FY 1983) and any additional perceived risk, albeit negligible, may be more than offset by the strengthened scoping and 5 year reinvestigative refinements recommended elsewhere in this report. In addition to the timeliness factor, adoption of such a system would reduce substantially unnecessary clearance requests by reducing the tendency of contractors to submit clearance applications as a contingency measure.

One-Time Access

An additional innovation that should be given consideration is development of a procedure to permit a higher level of access when unique circumstances are known to exist. DIS should, for example, upon receiving appropriate justification, be authorized to approve contractor employees for access to classified information one level higher than the personnel security clearance in effect. This would only be used under time-sensitive circumstances when one-time or occasional access is required and should only be extended to employees already cleared and investigated by the Government. Such flexibility would tend to discourage contractors from requesting higher level clearances when higher level access is not in evidence at the time of the initial application. To be successful, this procedure must involve a minimum of paperwork and permit same-day approval, by telephone if necessary. Adoption of such a policy would also discourage contractors from being tempted to deliberately permit improperly cleared personnel access to sensitive information for economic/ expediency reasons.

When faced with a powerful incentive to permit access by uncleared personnel, or to permit higher level access, deliberate compromise sometimes occurs. Although usually done without the knowledge of contractor security personnel and carried out only when the alternative is felt to be unacceptable (loss of opportunity to bid a contract or failure to overcome time-sensitive engineering problem with large amounts of money at stake), this problem is real and has grave and potentially damaging consequences. The Committee believes an inflexible bureaucratic process should not contribute to undesirable actions (compromise) that revised policy may prevent.

The Weakest Link - Secret Clearances

The Committee considers the policy concerning the granting of Secret clearances to be among the weakest aspects of the Industrial Personnel Security Clearance Program. Under normal circumstances, a Secret personnel security clearance is based on a NAC alone with no periodic update whatsoever. These two shortcomings, which include a highly suspect investigative basis for a Secret clearance and which permits Secret clearances to remain valid without any periodic update, were widely criticized during the course of this study.

A 1980 Director of Central Intelligence sponsored study⁸ determined that the NAC alone was insufficient investigative coverage. Nonetheless, this same study indicated that the NAC was a valuable determinant in 17 percent of the instances in which "resolved against" (the applicant) data was developed. Therefore, it follows that the NAC should not be abandoned as an investigative source but rather supplemented with additional productive sources of investigative coverage. In this regard, available information suggests that the NAC should be complemented by a LAC, credit check and employment check to serve as the basis for the granting of a Secret clearance.

A consensus of the comments received by the Committee supported increasing the scope of the initial investigation as well as a subsequent and continuing clearance eligibility assessment (periodic updates). The prevailing thought is the belief that personnel security risks commence after a clearance is granted (and access is afforded) and increases significantly

8. "PERSONNEL SECURITY SURVEY" Investigative Scope and Adjudicative Procedures Among Intelligence Community Agencies, DCI Investigative Standards Working Group, May 1980.

thereafter. The Committee concludes that a reinvestigation consisting of the above investigative scope should be conducted at 5-year intervals.

The largest number of cleared industrial personnel have Secret clearances (over 900,000) and yet the investigative basis for their clearance is quite limited. In fact, thousands of Secret cleared industrial personnel have access to classified information based on a NAC conducted more than 20 years ago.

Company Granted Confidential Clearances

Another inherent weakness, and one that contributes to the problem of clearance proliferation, is the relative ease associated with issuing an individual a company-granted Confidential clearance, especially in light of the fact that such clearances are normally not even recorded by the Department (DISCO). Although perhaps one-half of such clearances are issued to permit access pending completion of investigative action for a higher level clearance, the other half remain valid indefinitely. The frequently repeated axiom that it is not really classified--its only Confidential--may be a serious problem. By its very definition, the unauthorized disclosure of Confidential information could reasonably cause damage to the national security. It follows, therefore, that the issuance of a Confidential personnel security clearance should not be taken lightly.

Nonetheless, the Committee considers the risks associated with the granting of Confidential clearances by industry to be minimal and fully acceptable. In fact, many Government and industry personnel interviewed consider this system to be one of the most significant bargains involved with the Industrial Security Program. However, evidence of proper justification is

no less important for Confidential than for any other level of clearance. Accordingly, the Committee favors some tightening of the present system.

Copies of all company-granted Confidential personnel security clearances should be required to be furnished to the DISCO for record purposes and subsequent investigation, if necessary. This would also facilitate investigative follow-up if adverse information were received concerning an individual possessing a company-granted clearance. Since the DIS does not maintain records of company-cleared contractor personnel, a check of the clearance files following receipt of an adverse information report (or Hotline complaint) would not reveal the subject of the report as being security cleared. As a result, no further action would take place.

The Committee also favors automatic expiration of Confidential clearances 5 years from their date of issuance by the company. To remain valid for a longer period, an updated Personnel Security Questionnaire (PSQ) should be received by the DISCO before the scheduled expiration date. Each PSQ would be reviewed and, if otherwise appropriate, a Letter of Consent (clearance) issued to the contractor by the DISCO based on a favorable NAC. Once a DoD confidential clearance is granted, the clearance would remain valid for as long as the employee had a continuing need for access and remained employed by the same contractor. The increased investigative coverage, periodic update, and greater DoD involvement are considered essential improvements over the present system.

Administrative Downgrading of Clearances

Also offered for consideration is the adoption of a systematic administrative downgrading of personnel security

clearances when justification to retain a higher level of clearance is not specifically certified to the DISCO.

The Industrial Security Manual presently provides that when an employee cleared at the Top Secret level has not had access to Top Secret information during a preceding 18-month period and such access is not anticipated in the foreseeable future, the contractor is required to downgrade the clearance to the next lower level of classified information required for access by submitting written notice to the DISCO. In practice, however, only a relatively few Top Secret clearances are downgraded in this fashion each year. There are simply too many competing motives for contractors to comply with this provision. Moreover, with rare exception, administrative downgrade actions must be initiated voluntarily by industry. Consequently, the number of Top Secret clearances continues to grow even though the need for Top Secret access in many instances is no longer justified.

Accordingly, the Committee recommends an affirmative system, expanded to include Secret-cleared personnel, that would require contractors to justify existing clearance levels to the DISCO at 5-year intervals. If retention of the existing or higher level clearance is not clearly justified, the clearance shall be routinely downgraded (administratively) to the next lower level of classification. In other words, evidence to support continuation of personnel security clearances at the Top Secret and Secret level would be required initially and periodically.

The Committee believes that a large percentage of the nearly 115,000 Top Secret clearances now in effect may be downgraded and/or eliminated under the proposed procedure. It is considered noteworthy that the foregoing system, if implemented, would not require a change in DoD policy, but only

a procedural change requiring more accurate and systematic review of initial clearance qualification and confirmation of continuing clearance eligibility.

Clearance Justification Data Sheet

In order to reduce initial clearance requests and to downgrade or eliminate systematically all personnel security clearance requests that cannot be justified, more precise clearance justification information shall be recorded and submitted to the DISCO, or maintained by the contractor, as appropriate. The Committee proposes that more individuals be included in this process, i.e., the employee applicant, the applicant's immediate supervisor, and a responsible member of facility management, and that such individuals be required to make a similar recertification every 5 years thereafter.

At present, a representative of the contractor makes a certification on the PSQ that the applicant is a bonafide employee and has a need for clearance to perform on classified contracts. This certification is often made at lower management echelons or by security personnel at the contractor facility. Furthermore, the employee applicant currently certifies only that the information on the PSQ is accurate to the best of his/her knowledge. The applicant does not certify that a security clearance is necessary. Although immediate supervisors are usually in the best position to know whether a security clearance is really necessary, and are generally responsible for initiating clearance actions, they are not specifically required by DoD policy to certify in writing that the clearances they request are required. The Committee proposal would include all three persons in each clearance request, to include periodic updates, and require that all three be aware of the consequences of willfully making false or misleading statements. A separate "Data Sheet" would no longer

be necessary once the information has been incorporated into a revised PSQ.

The Clearance Justification Data sheet should contain essentially the following information:

(a) Applicant certification that the duties and responsibilities of current position require access to (specify) information;

(b) Immediate supervisor certification that applicant occupies a position which requires access to (specify level) information and the applicant is believed to be suitable for classified access; and

(c) Confirmation by a cleared owner, officer, director or other responsible official of the firm, other than the security supervisor, that the request has been reviewed and that the clearance is fully justified.

The Clearance Justification Data Sheet shall also include a statement consisting substantially as follows: Knowingly submitting or confirming false information on this Data Sheet is contrary to DoD policy and U.S. national security interests and any person determined to have done so is subject to having his/her personnel security clearance denied, suspended or revoked.

Periodic Reinvestigations

The DIS estimates that by the end of FY 1984 there will be 280,000 persons with Sensitive Compartmented Information or Top Secret clearances 5 or more years old which will require a bring-up background investigation referred to as a periodic reinvestigation (PR). The investigative resource implications are significant. It has been estimated that it may take a decade or more to conduct a PR on all persons who require such updates. The DIS PR quota for FY 1984 was about 40,000 cases; however, they were only able to complete 32,000 PRs.

The Committee believes the conduct of periodic reinvestigations of cleared personnel is substantially more important than the original clearance investigation. However, PRs are currently initiated using a quota system because the existing and projected PR workload cannot be totally accomplished by the DIS with existing resources. Contrary to the view of some DoD officials who advocate resolution of the PR problem by a massive infusion of additional manpower, the Committee offers an alternative approach.

Periodic reinvestigations are required for all Top Secret cleared personnel. With nearly 115,000 persons cleared Top Secret in industry alone, the Committee favors focusing the priority for the selection and conduct of PRs on those individuals who have continuous or recurring access to Top Secret information as opposed to the current system of focusing on the oldest cases for such investigative coverage. It appears illogical to conduct a PR on an individual who has never or seldom had access to Top Secret material while skipping over a more recently cleared person who has continuous or frequent Top Secret access.

Although specific confirmation data is not available, the Committee estimates that perhaps 90,000 to 95,000 of the 115,000 Top Secret cleared industrial personnel do not have continuous or frequent access to Top Secret information. In fact, probably no more than 35,000 to 40,000 of the contractor personnel cleared at the Top Secret level have ever had access to Top Secret information.

Therefore, priority consideration for the conduct of PRs should be reserved for those cleared personnel with access to Top Secret information. Unfortunately, records that indicate who in industry has such access are not maintained by the DIS, however, a system could be devised to obtain this data.

The maintenance of Top Secret access records by the DIS is considered essential if the DoD is to avoid the conduct of unnecessary PRs. The Industrial Security Manual already requires industry to maintain up-to-date records of all persons who are afforded access to Top Secret information. It would, therefore, not be unduly burdensome for industry to furnish their Top Secret access lists to the DIS or for the DIS to develop some alternative system. Thereafter, those Top Secret cleared personnel who have continuous or recurring Top Secret access (and perhaps SCI) would be given priority PR consideration. Similarly, the DUSD(P) should delete from automatic PR consideration those contractor personnel who have only occasional Top Secret access or no access whatsoever.

Counterintelligence Questionnaire

The Committee also notes that the clearance system places primary emphasis on an applicant's suitability and trustworthiness for access to classified information by general lifestyle data. Although no particular issue is taken with this approach, greater emphasis should be placed on loyalty aspects along with activity involving unauthorized disclosures or contacts, to include any knowledge of such activity. The privacy portion of the PSQ currently addresses Communist Party membership and other organizational affiliation with groups that advocate the overthrow of the U.S. Government. Such questions do not go far enough. For example, a person engaged in espionage for profit or for ideological reasons would not currently be required to make false statements on a PSQ to conceal such conduct.

Accordingly, the Committee endorses use of a counterintelligence questionnaire to be used with each clearance application and periodic update. Use of such a questionnaire would not eliminate false statements from being

made in this regard, but it would focus attention on the seriousness of any related activity and would be useful to Federal prosecutors during any subsequent espionage trial. It might also tend to discourage some from engaging or becoming entangled in such activity and it could also, depending on the questions selected, provide pertinent information on which to initiate or expand an investigation involving espionage or unauthorized contacts. A separate counterintelligence questionnaire would no longer be necessary once the questions have been incorporated into a revised PSQ. The counterintelligence questionnaire should contain essentially the following questions:

(a) Have you ever engaged in espionage or sabotage against the United States?

(b) Do you have knowledge of anyone who is or may be engaged in espionage or sabotage against the United States?

(c) Have you ever been approached to give or sell any classified information or materials to unauthorized persons?

(d) Have you given or sold any classified information or materials to unauthorized persons?

(e) Do you have knowledge of anyone who has given or sold classified information or materials to unauthorized persons?

(f) Do you have any contact with representatives of "designated countries"? If so, please explain.

The counterintelligence questionnaire should include a statement consisting substantially as follows: I certify that I know that any misrepresentation or false response made by me herein may subject me to prosecution under Title 18, U.S. Criminal Code, Sections 793, 794, 798, and 1001.

Overview of Recommended Personnel Security Clearance Changes

The following represents an overview of the Committee's recommended investigative and clearance changes, by clearance level:

RESUME OF PROPOSED PERSONNEL SECURITY
CLEARANCE SYSTEM

Top Secret

Clearance Request - Initial

Must submit:

- a. Personnel Security Questionnaire (PSQ) and fingerprint card
- b. Counterintelligence Questionnaire
- c. Clearance Justification Data Sheet

Interim Clearance Based on:

- a. Favorable review of:
 - PSQ
 - Counterintelligence Questionnaire
 - Clearance Justification Data Sheet
- b. Favorable National Agency Check
- c. Initiation of interview-oriented background investigation (IBI)

Interim Clearance Valid Until:

- a. Suspended, revoked, or withdrawn
- b. Supplanted by final clearance

Final clearance based on:

- a. Completed IBI

Final clearance valid until:

- a. Suspended or revoked
- b. Administratively downgraded or terminated
- c. Automatically downgraded to Secret at 5 years

Subsequent 5 year periods (to retain):

- a. Favorable review of updated:
 - PSQ
 - Counterintelligence Questionnaire
 - Clearance Justification Data Sheet
- b. Favorable periodic reinvestigation

Secret

Clearance Request - Initial

Must submit

- a. Personnel Security Questionnaire (PSQ) and fingerprint card
- b. Counterintelligence questionnaire
- c. Clearance Justification Data Sheet

Interim Clearance based on:

- a. Favorable review of:
 - PSQ
 - Counterintelligence Questionnaire
 - Clearance Justification Data Sheet
- b. Initiation of National Agency Check (NAC) plus Defense Central Index of Investigations (DCII) check

Interim clearance valid until:

- a. Suspended, revoked, or withdrawn
- b. Supplanted by final clearance

Final clearance based on:

- a. Completed NAC, local agency check (LAC), credit check, and employment check
- b. Selected scoping as necessary

Final clearance valid until:

- a. Suspended or revoked
- b. Administratively downgraded or terminated
- c. Automatically downgraded to Confidential at 5 years

Subsequent 5 year periods (to retain):

- a. Favorable review of updated:
 - PSQ
 - Counterintelligence Questionnaire
 - Clearance Justification Data Sheet
- b. New NAC, LAC, credit check and employment check

Confidential
(Government-Granted)

Clearance Request - Initial

Must submit:

- a. Personnel Security Questionnaire (PSQ)
- b. Counterintelligence Questionnaire
- c. Clearance Justification Data Sheet

Interim Clearance based on:

- a. Favorable review of:
 - PSQ
 - Counterintelligence Questionnaire
 - Clearance Justification Data Sheet
- b. Initiation of National Agency Check (NAC) plus
Defense Central Index of Investigations (DCII)
check

Interim clearance valid until:

- a. Suspended, revoked, or withdrawn
- b. Supplanted by final clearance

Final clearance based on:

- a. Favorable NAC, local agency check and credit
check
- b. Selected scoping as necessary

Final clearance valid until:

- a. Suspended or revoked
- b. Administratively terminated

Confidential
Company-Granted)

Same procedures as currently provided for except as follows:

1. Copies of Personnel Security Questionnaire (PSQ), Counterintelligence Questionnaire and Clearance Justification Data Sheet must be forwarded to the DISCO for recordation, review, and a DCII check upon issuance of any company granted clearance.
2. New clearance forms shall be submitted to the DISCO within five years from date of company granted Confidential clearance. If not, clearance shall expire and employee would be debriefed accordingly.
3. If the review of the PSQ, Counterintelligence Questionnaire and Clearance Justification Data Sheet is favorable, and upon completion of a favorable National Agency Check, the DISCO shall issue a letter of consent (clearance) at the Confidential level.
4. Thereafter, the clearance would remain valid for so long as the employee has a continuing need for access and remains employed by the same contractor.

Conclusions:

A substantial number of facility and personnel security clearance requests and a substantial number of facilities and personnel already cleared do not require classified access and should not have been cleared under the Defense Industrial Security Program. The various ongoing initiatives by industry and Government to verify the need for classified access, both facility and personnel, can reasonably be expected to achieve only limited success. In many respects, the current DoD personnel and industrial security policies, procedures and practices actually contribute to the proliferation of facility and personnel security clearance requests and grants.

Present policies and procedures do not adequately address the need to rejustify, on a periodic basis, current personnel security clearances. In regard to Secret and Confidential clearances, pertinent policies are considered deficient in that they fail to take into account that personnel security risks usually begin after a clearance is granted (and access afforded) and increase significantly thereafter. The Committee concludes, therefore, that some reinvestigation action should be conducted periodically. Moreover, some additional investigative coverage appears warranted for Secret and Confidential clearances.

Personnel security clearance processing time is excessive and wasteful. Industry cannot afford to have its employees remain idle for months, or to place employees in temporary positions, while they await the granting of a personnel security clearance. Even if the processing goals established by the DIS are achieved, the time between the application for clearance and the clearance grant will remain excessive. This excessive processing time encourages industry to abuse the clearance system by requesting clearances regardless of

immediate or foreseeable need and usually at the highest conceivable classification level.

Recommendations:

a. The Deputy Under Secretary of Defense for Policy should revise the current system used to determine priority consideration for the conduct of periodic reinvestigations (PRs). The new system should identify those Top Secret-cleared (and perhaps those with Sensitive Compartmented Information access) who have continuous or recurring access to Top Secret information and should subject only those individuals to the PR requirements. Those who have never had access to Top Secret or who rarely have such access should be eliminated from PR consideration or placed on a low priority listing, as appropriate.

b. Clarify the policy to ensure that contractor personnel determined eligible to be processed for a NAC under physical-access-only circumstances do not qualify and shall not be processed for a personnel security clearance under the Defense Industrial Security Program.

c. The cognizant security office should be authorized, upon receipt of appropriate justification, to approve contractor employees for one-time or occasional access to classified information at one level higher than the personnel security clearance in effect.

d. All company-granted Confidential personnel security clearance documentation should be furnished to the DISCO for review, recordation, and a DCII check.

e. All company-granted Confidential personnel security clearances should automatically expire 5 years from date of

issuance unless the need is rejustified. To remain valid for a longer period, an updated PSQ, Clearance Justification Data Sheet and Counterintelligence Questionnaire shall be received by the DISCO for review before the scheduled expiration date. Reissuance by the DISCO, if otherwise appropriate, shall be based on a favorable National Agency Check and shall remain valid as long as the employee has a need for access and remains employed by the same contractor.

f. Industrial personnel security clearance policies and procedures must be changed to permit the use of interim clearance procedures prescribed by the "Industrial Security Regulation," DoD 5220.22-R; and remove the requirement for contracting officer or higher level approval, for all personnel security clearance requests.

g. All Top Secret and Secret industrial personnel security clearances shall be subject to automatic downgrade to the next lower level of clearance when DISCO does not receive justification to retain the higher level clearance within 5 years from the date of issuance.

h. All Secret industrial personnel security clearances should be based initially on a National Agency Check, local agency check, credit check and employment check which shall be repeated every 5 years thereafter.

i. All personnel security questionnaires submitted to the DISCO, regardless of level, should be accompanied by a Clearance Justification Data Sheet.

j. All personnel security questionnaires submitted to the DISCO, regardless of the level of clearance requested, shall be accompanied by a completed counterintelligence questionnaire.

20. Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations

Issue/Discussion:

One of the suggestions resulting from this study concerned the establishment of a requirement for contractors to detail in their Standard Practice Procedures (SPP) company policy for disciplinary action for security violations. Of some concern is the suspicion that disciplinary action taken, if any, for security violations, varies widely from one contractor to another. Although the Committee does not propose to infringe on the contractor's prerogative to determine policy on disciplinary actions, we believed that the discipline administered should be commensurate with the violation.

Many large contractors have already incorporated detailed policy provisions for disciplinary action in their SPP. At present, the Industrial Security Manual (ISM) does not require contractors to document their policy on disciplinary actions for security violations, nor does it call for oversight of their policy by the DIS. There are, however, somewhat oblique references indicating that disciplinary action is expected when a violation has occurred.

While not all-inclusive, the following represents some of the probable benefits from instituting the recommended policy:

a. Experience has shown that many contractors have not addressed this issue; therefore, when confronted with a security violation, they administer no disciplinary action or are inconsistent in the action taken. In requiring that the policy be delineated in the SPP, this confusion would be eliminated.

b. By prescribing a written policy, employees are apprised of the consequences of their failure to follow security practices. Since there is then an established cause and effect, employees are more likely to be cautious and sensitive to the ramifications of their failure to follow security procedures. This is particularly true when the policy is not only established, but enforced.

c. The contractor demonstrates his commitment to the Defense Industrial Security Program by giving "public notice" of his shared responsibility in the enforcement of DoD policies and procedures as outlined in the Industrial Security Manual. The establishment of a written and publicized policy that has a direct impact on the responsible individual is one of the most effective deterrents to security violations caused by carelessness or a general disregard for security.

Recommendation:

That contractors be required to establish in their SPPs company policy on disciplinary action to be taken against employees involved in security violations when culpability is established. The DIS shall be limited to advising and assisting the contractor in its preparation of the policy if requested.

SECTION FIVE: PHYSICAL SECURITY

21. System of Controls Over After-Hours Access and Reproduction Equipment at Cleared Facilities

Discussion:

After-Hours Controls

A review of the various facts and circumstances associated with the espionage cases summarized at Appendixes VIII, IX and X indicates rather clearly that unsupervised access to classified material within an environment that affords a low probability of detection, i.e., a lack of sufficient internal and external (perimeter) security control, is a serious problem. We know, for example, that the vast majority of the general population is law-abiding and mindful of the rights of others, and yet we keep police departments busy around the clock responding to the aberrations of the few. Similarly, cleared personnel will, in the main, properly and dutifully discharge their individual responsibility for safeguarding classified information. The opportunity to misappropriate property is stronger when controls and supervision are lax. Under the DISP, too much reliance is permitted to be placed on personnel security clearances and employee integrity, particularly during nonworking hour periods. Cleared employees are frequently left to police themselves under such generally uncontrolled conditions.

The Industrial Security Manual contains extensive requirements dealing with the storage of classified material. These requirements delineate the various repositories, such as cabinets, vaults, strongrooms and controlled areas which contractors must use to secure classified material under their charge. Also included are details concerning the use of alarm

systems and cleared guard patrols. While these contractually binding storage and control requirements apply under both normal and nonworking hour conditions, they neither prevent cleared personnel from having unauthorized access nor inhibit such personnel from removing the contents from the premises. DoD approved storage repositories are designed to keep unauthorized personnel from the material secured therein and, failing that, to reveal evidence of forced entry. In short, they offer adequate protection against surreptitious entry only. It should also be noted that a cleared classified document custodian could very well be an unauthorized person if access to his/her security container occurs after scheduled working hours.

Cleared guard and/or alarm service protection is, under normal circumstances, only mandated in connection with the storage of Top Secret level material and under conditions where the level of classified material involved exceeds that authorized for a particular type of repository. They are not required and are only rarely used to control entry and exit at cleared plant sites. Employees, cleared and uncleared, are normally free to enter cleared contractor facilities during nonworking hours and to bring along friends and family too if they wish. The Industrial Security Manual does not require contractors to monitor such visits or to record their occurrence.

Many cleared contractors demonstrate little concern with inner security at their facilities during nonworking hours, weekends and holidays. This was quite evident in the James D. Harper espionage case. As a rule, cleared employees are free to work or visit during such hours and may open security cabinets and work with classified material without supervision. In many instances they are encouraged to do so. Normally, keys to doors are not closely controlled, locks are seldom changed,

and no records are maintained of who enters and exits. Accordingly, a cleared employee, in a worst case scenario, could visit the office at any late hour, open a security cabinet and spend several hours reproducing or photographing the classified material, put the material in a briefcase and walk out the door. The employee could even bring along several accomplices to assist in reproducing and removing the classified documents. Paradoxically, a supermarket employee may encounter far greater difficulty in stealing a loaf of bread.

Walking out the door with classified documents is only slightly less difficult during working hours. Again, the DoD does not require constant or random briefcase searches or any other perimeter security measures. If the reproduction of large quantities of classified documents during working hours appears too risky, all that needs to be done is to carry the original or controlled copies home, reproduce them elsewhere and return them later in the evening. Or, as an alternative, and if time permits, simply carry two or three classified documents home each evening until the job is completed.

The foregoing illustrations are not intended to discredit existing DoD policies and procedures or pass judgment on those responsible for their implementation and oversight. The Industrial Security Program is based, out of necessity and congruent with our free society, on trust. Many of the "shortcomings" described above can be overcome, but only at a price. A tightly controlled defense establishment, such as can be found in the Soviet Union, would not eliminate theft of classified material, and imposition of stringent measures could prove prohibitively detrimental in many respects overall. The Committee does believe, however, that more can and should be done to improve physical security at cleared contractor facilities.

The principal concern is the period of greatest vulnerability, nonworking hours, and only with those contractors who actually possess classified material. The solution is not, however, to impose detailed and common requirements at all such facilities. The needs and vulnerabilities of all contractors are not the same and a sound requirement placed on one contractor might be ridiculous if imposed on another. In short, a uniform set of detailed physical security standards and procedures with across-the-board application would be unwise, impossible to enforce, and extremely costly. The Committee favors adoption of a policy mandating general security controls, the specifics to be developed and implemented by facility management, and followed up by periodic DIS reviews to ensure compliance with the policy. The DIS should also be consulted by contractor management during development of the safeguards and control measures.

The security system shall provide reasonable assurance that the physical presence of all persons working or visiting in the proximity of classified repositories or areas during nonworking hours are monitored by continuous or intermittent electronic surveillance, personnel oversight/escort, stringent lock and key controls, or other comparable security measures. The procedures developed will depend, in part, on the type of work performed, facility size and physical layout, classification level of material, security controls already in place, and the nature, volume, and location of the areas and repositories concerned. Accordingly, each facility's needs and corrective options must be considered unique. Therefore, the minimum acceptable controls will vary greatly, necessitating case-by-case development and tailoring, wholly dependent on the facts, circumstances and hostile intelligence threat present in each instance. Only general responsibility shall be mandated by the ISM. The specific measures selected

for use by industry management should not be subject to DIS approval per se. Such controls should, however, be subject to a DIS determination of adequacy before their placement into the firm's Standard Practice Procedures (SPP). Facilities, determined to have inadequate procedures should be reported by the DIS, following consultation with company management, to the Government contracting activity for which the classified material was received or generated. The DIS should have full authority to cite contractors for failing to adhere to the pertinent provisions of the SPP.

The relatively widespread practice of permitting cleared employees to be personal custodians of the classified material entrusted to them is a related but no less important problem. A typical example of personal custodianship is the engineer who has one or two approved security containers in his/her private office or work unit as a convenience. The number of classified documents under the direct control of this engineer could vary greatly, but it would not be uncommon to see anywhere from a score to several hundred documents so maintained in medium-to-large facilities. The possible adverse security implications are obvious. The following is a verbatim extract of comments furnished to the Committee pertinent to this problem by an east coast security manager:

During my years of experience in the DoD security arena (20 years military/10 years industrial security), I have formed the opinion that one of the most vulnerable areas in the current Industrial Security Program is the distribution and control of satellite containers in Government agencies and DoD contractor facilities. In the instances where employees are allowed to maintain a secure container and act as custodian of classified material and have access to that material (in many cases) 24 hours a day, seven days a week, acts of espionage are very hard to control or actually discover. While most facilities maintain after-hour logs and other security controls, espionage acts such as making copies/photographs of classified material and removing such from a facility is almost, if not, impossible to detect. In many facilities

it is possible the custodian of the classified material may be the only employee in a facility and, therefore, has access to the material without any restrictions.

I realize that the elimination of this privilege under provisions of the ISM may, and will, cause certain problems for individuals who must have daily access to classified material to accomplish their assigned functions. However, I believe there must be some additional controls or restrictions imposed on after hour access, if the privilege of maintaining satellite security containers is to remain in effect.

The DoD cannot and should not mandate to industry the precise measures and equipment to be used in all instances. This is a responsibility which must be shared by industrial management on a case-by-case basis. Contractors possessing classified material have a wide range of physical security control measures from which to choose. Nonetheless, the following control measures were suggested to the Committee by many of the individuals consulted during the course of this study.

- Intrusion detection devices
- Controlled entrances
- Closed circuit television
- Enhanced reproduction equipment control (lock-outs, key cards, etc.)
- Sign-in/sign-out logs
- Escorts
- Spot checks of briefcases and vehicles
- Safe check sheets - Safe Open/secured check-off sheets
- Lock and key control and accountability
- Procedures governing after hour access approval (advance approval and after the fact reports)
- Control document distribution and storage points
- Central Storage and "Sundown" Rule

Reproduction Equipment Controls

Inasmuch as the unauthorized reproduction of classified information is so interwoven with the illegal removal of material, some discussion on this subject is also warranted. The ready availability of reproduction equipment contributes to

the proliferation of classified documents which tends to increase unnecessary access opportunities and drives up security costs.

There is a wide range of office reproduction equipment in use today. This equipment is generally afforded little attention by industry security personnel, save the larger and more defense-oriented contractors. Even the large defense contractors make this equipment readily available and many of them have hundreds of reproduction machines on the premises. They have become commonplace and necessary office adjuncts in both the public and private sectors. The Committee's concern is limited to their use at facilities that possess classified material and the apparent lack of sufficient security control over them.

The DoD industrial security policy addresses reproduction in only basic terms, i.e., control and accountability of reproduced material, proliferation of document guidelines, personal control during use, posting of equipment authorized for classified use, and the like. Lacking are procedures designed to reasonably eliminate or detect the unauthorized reproduction of classified documents.

A consensus of individuals and organizations contacted during the course of this study believed that office reproduction equipment was a serious security hazard and that policies and procedures were inadequate. They suggested that one or more of the following security safeguards be imposed to enhance control:

- Built-in cameras
- Electronic sensors
- Centrally controlled use
- Card control access system
- Electronic surveillance
- Two person rule
- Locks after hours

The Committee was in basic agreement with the various professionals contacted on the reproduction issue. However, the Committee does not favor adoption of a policy which would require contractors to place into effect, in whole or in part, the specific security safeguards listed above. Contractors should, however, be required to develop a system capable of detecting the unauthorized reproduction of classified material around the clock (or reasonably preventing the possibility thereof). The specific methods shall be left to contractor management discretion, in consultation with the DIS, based on the circumstances in each case and set forth in the Standard Practice Procedures. The DIS security inspections shall oversee compliance with the prescribed reproduction controls.

It should be emphasized that the proposed security enhancements cannot guarantee that unauthorized disclosures will not occur. Absolute control of classified information is not desirable or attainable. The goal, therefore, is to achieve a level of control over national security information that is neither overly stringent nor irresponsibly weak and ineffective.

Conclusions:

DoD-mandated and contractor initiated-physical and personnel security controls during nonworking hours, to the extent they exist, are generally weak and ineffective, and as such, provide inadequate protection against unauthorized access or removal of classified material.

Despite universal acknowledgement of security vulnerabilities associated with reproduction equipment located in the proximity of classified material, DoD security policy does not effectively deal with the prevention of and detection of the unauthorized copying of classified material.

Recommendations:

a. The DoD should adopt a policy requiring cleared Defense contractors to develop and effectuate procedures that ensure that all persons working or visiting the proximity of repositories or areas used to store classified material during nonworking hours are monitored by continuous or intermittent means capable of preventing or detecting physical presence, unauthorized access, and removal of classified material from the premises.

b. The DoD should adopt a policy requiring cleared contractors to develop and place into effect procedures that ensure that reproduction equipment is monitored by continuous or intermittent means to prevent or detect the unauthorized copying of classified material. The specific control procedures shall be developed in consultation with the DIS and incorporated with the individual facility's Standard Practices Procedure and be subject to DIS inspections.

SECTION SIX: INFORMATION SECURITY

22. Access to the Defense Technical Information Center Classified Data

Discussion:

The Defense Technical Information Center provides services and products that make a vast amount of scientific and technical information available to agencies and components of the DoD, DoD-sponsored contractors, grantees, potential contractors, and other Federal agencies and foreign Governments as authorized by the DoD. The Center, under the operational control of the Defense Logistics Agency and policy guidance of the Office of the Under Secretary of Defense for Research and Engineering, acts as the centralized repository of scientific and technical information to support DoD research, development, engineering and studies programs. Mission responsibilities as set forth in DoD Directive 5100.36 include the acquisition, storage, retrieval, dissemination and utilization of technical information. In conjunction with the Office of the Under Secretary of Defense for Research and Engineering, the Center helps to formulate objectives and programs concerning scientific and technical information transfer among the Military Departments, defense agencies and others. Although functionally centralized at Cameron Station in Alexandria, Virginia, the Center operates 2 field offices and exercises management responsibility for 8 of 19 DoD Information Analysis Centers.

The Defense Technical Information Center's information transfer responsibilities cover essentially all fields of science and technology. Access to the information and products available through the Center can usually answer three questions: what DoD research is being planned; what research

is currently in process; and what results were realized by completed research.

Based on the registered field of interest at the Defense Technical Information Center, an individual or organization can have potential access to 1.6 million documents. Of these documents about 113,000 were either classified Confidential or Secret. In April 1984, the Committee determined that there was a total of about 3,840 registered users at the Center. Of the registered users, 2,126 had been cleared for access to classified technical information on 22 subjects ranging from aeronautics to space technology. Within these 22 subject areas there were about 200 subgroupings of information available to the Center's registered users. For example, in the area of space technology, the subgroupings were aeronautics, spacecraft, spacecraft trajectories and reentry, spacecraft launch vehicles and ground support.

Information services provided by the Center to registered users can be categorized in four product and service areas. They are subscription products, demand products, subscriber services and management reports and services. Subscription products are customized publications, which are forwarded automatically to users after an initial request is made. Demand products are issued in response to user requests for specific information. Subscriber services also include the Defense Research, Development, Test and Evaluation On-Line System (DROLS) which enables registered users direct access to the Center's data bases. Through terminals tied directly into the Center's computer, or via dial-up terminals, registered users can search, retrieve and input data and order documents. In April 1984, there were about 600 DROLS users. Management reports and services offered to registered Defense Technical Information users include publications, directories and library and referral services.

The Center is the primary information source within the DoD and offers a diversity of scientific and technical information products and services. Therefore, any unauthorized access to the Center's data base and products and services must be precluded. Based on interviews with management representatives at the Center, the Committee concluded that a system of internal controls were seemingly in place to prevent the unauthorized access to classified documents on a myriad of scientific and technical data and services. However, the Committee was not convinced that registered users were limiting their areas of interest to specific areas of contract interest or that "need-to-know" was thoroughly substantiated. About 500 contractors, government organizations, universities, etc, had registered in all 22 areas (200 subgroups) of interest for the Defense Technical Information Centers products and services. Many organizations had multiple registrations in the "all category." Those so registering also included "potential contractors" authorized under various DoD component and Federal agency potential contractor programs. Overall, there were about 1,200 potential contractor registrations in 2 to 200 subgroups within the 22 areas of technological interest. People interviewed at the Center and at other locations visited felt that Government contracting officers were too lenient with contractors because they approved broad "fields of interest" beyond the contractors' "need-to-know" or potential contract interests or capabilities.

While the Committee recognizes the importance of encouraging scientific and technological innovation, exchanging technical and scientific data and protecting the capability of the defense industry to compete successfully for DoD and other Government contracts, it should also be recognized that there has been substantial transfer of technical and scientific information with military applications to hostile intelligence services. This has saved our adversaries millions of dollars

as well as time and effort in research and development and enhanced their military capabilities.

Hostile intelligence services and others may have the potential to exploit the Center's products and services. Therefore, the Committee believes that an audit should be made of the Defense Technical Information Center's operations to determine whether internal controls are in place and are adequate to safeguard its classified data bases and products from unauthorized access and disclosure. Also, a vulnerability assessment of the Center's operations should be made by a DoD counterintelligence component to recommend countermeasures to neutralize any potential hostile threat.

Recommendations:

a. That the Inspector General, Department of Defense, schedule an audit of the Defense Technical Information Center to ascertain whether internal controls exist to preclude the unauthorized disclosure of and access to its scientific and technical products and services. The scope of the audit shall encompass procuring activity justification for authorizing the broad areas of interest for access by contractors.

b. That the Deputy Under Secretary of Defense for Policy designate a Department of Defense counterintelligence component to evaluate any potential threat to the Center from hostile intelligence services. In this regard, the appropriate countermeasures should be taken to protect its personnel, products, services and data base from potential compromise.

23. Proactive Efforts by the DIS to Prevent Unauthorized Disclosures

Discussion:

The overt collection of classified U.S. technology by hostile intelligence services is a serious problem. This loss is particularly difficult to combat because the facilitators frequently are not espionage agents but rather enterprising U.S. businessmen, academicians and research engineers at the leading edge of technology. The motivation of these individuals is either profit through increased sales, often to foreign buyers, or advancement of state-of-the-art technology. In zealous pursuit of these interests, classified information has been "leaked." Furthermore, in an effort to reduce unit costs, program sponsors of the Military Services have sometimes encouraged foreign sales.

Times Staff Writers, Robert C. Toth and Bill Sing reported in the Los Angeles Times on October 23, 1983:

Anti-security attitudes pervade many high-tech companies High-tech firms traditionally have maintained an open, campus-like environment that is believed to encourage creativity, sharing of information and individual trust. Also, engineers and other employees move from company to company, often taking sensitive knowledge and information with them Officials are aware that too much security can stifle creativity and the exchange of information which can hasten new developments, particularly in the fast paced areas of high technology. They are also aware that too close scrutiny of employees can violate privacy and civil-liberty guarantees of the Constitution.

Within the DoD, the DIS is responsible for conducting investigations of unauthorized disclosures ("leaks") on the national level involving components lacking investigative capability and on cases crossing component lines. Because of the nature of the offense, usually occurring in published

military hardware and technological journals as well as news articles, the success rate of these reactive investigations is relatively low. During calendar years 1981, 1982 and 1983, DIS conducted 9, 12 and 16 unauthorized disclosure investigations, respectively. Considered to be an equally serious problem is literature available and presentations made at high technology symposiums, trade fairs, job fairs, conventions and the like, many of which are widely publicized and open to the public. It is reasonable to assume that hostile intelligence services are alert to such opportunities and aggressively exploit them.

President Ronald Reagan emphasized the seriousness of "leaks" in a memorandum for federal employees which is obviously applicable to all cleared personnel.

Recent unauthorized disclosures of classified information concerning our diplomatic, military and intelligence activities threaten our ability to carry out national policy The unauthorized disclosure of our nation's classified information by those entrusted with its protection is improper, unethical and plain wrong The American people have placed a special trust and confidence in each of us to protect their property with which we are entrusted, including classified information. They expect us to protect fully the national security secrets used to protect them in a dangerous and difficult world We must also be able to protect our military forces from present or potential adversaries. From the time of the Founding Fathers, we have accepted the need to protect military secrets Even in peacetime, lives depend on our ability to keep certain matters secret.

The Committee contacted senior representatives of organizations responsible for counterintelligence operations within the Military Departments. These representatives considered the unauthorized disclosure of classified information to be a serious problem and cited specific examples of completed and ongoing investigations which may indicate security weaknesses:

(1) An overseas contractor employee provided a classified weapons system document to a foreign government in order to make a sale. During an interview, the employee said he knew this was wrong, but did it anyway.

(2) A professor from a private research institute made unauthorized disclosures of classified information during briefings presented overseas.

(3) Known representatives of a hostile power attended a U.S. Aerospace/Defense Hardware technical briefing and exposition by defense contractors in Washington, D.C.. Eighty-nine defense contractors, including most of the largest, were identified as exhibiting firms.

(4) A former military member currently employed by a defense contractor, illegally possessed Secret electronic warfare documents from his former command.

(5) At a recent conference, a civilian contractor discussed new computer security software measures being tested on a Top Secret data base. Attendees included representatives from the Services, other DoD agencies, civilian contractors and computer vendors. No disclaimer was given, and participants familiar with the test said they believed the briefing presented sensitive information that was inappropriate for the setting. The conference was held in an insecure, public area.

In June 1984, a Military Department widely publicized the following warning:

A major security violation occurred this spring when a ... affiliated speaker discussed classified technology at an unclassified, non-government meeting. Unauthorized transfer of classified technologies to foreign countries is a major national concern. Non-government, unclassified technical meetings, conference symposia, and educational courses are frequently a source of unauthorized technology transfers since most are open to foreign attendance. Security violations of this type disclose militarily relevant technologies to our adversaries and reflect poorly on security

The Industrial Security Manual for Safeguarding Classified Information (ISM) stipulates that a DoD contractor shall not disclose information pertaining to classified contracts or projects (with certain well-defined exceptions) without the

approval of the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs). Furthermore, a DoD contractor shall not publish or distribute brochures, promotional sales literature or similar material containing classified information without prior review and written authorization by the contracting officer concerned. The authorization for such publication and distribution shall be indicated on the document. Following are pertinent excerpts from a recent GAO report:

QUESTION

For each calendar year since 1979, how many books, articles, speeches, and other materials were reviewed during the prepublication review process?

RESPONSE

The following tabulations show the types and quantities of information reviewed during calendar years 1979 through 1983. Separate tabulations are shown for the Department of Defense (DOD) and the other respondents because DOD combined books and articles and because the Department of the Army responded in number of pages reviewed for 1982 and 1983.

The Department of Defense

	<u>1979</u>	<u>1980</u>	<u>1981</u>	<u>1982</u>	<u>1983</u>
Books/Articles	2,994	3,133	2,784	6,457	10,088
Speeches	1,320	1,360	871	2,237	2,020
Other	4,816	4,344	5,178	4,713	5,102
No. of pages--Army				92,918	77,404

QUESTION

How many unauthorized disclosures of classified information were there during calendar year 1983? How many of these were not reported to the Department of Justice?

RESPONSE

Four agencies reported 43 unauthorized disclosures of classified information. Of these, 34 were not reported to the Department of Justice. (NOTE: These statistics apply principally to DoD.)

Conclusion:

Currently, the primary method employed by the DIS to oversee compliance with prepublication review requirements is to interview personnel and examine DoD contractors' files of such activities during routine security inspections. The apparent drawback is that if the contractor did not follow the required approval procedures, no record will exist. Thus, the DIS industrial security representative shall have no reason to question this unless there was some indication of an unauthorized release in the review of other corporate records.

Recommendation:

The DIS should incorporate proactive efforts to oversee compliance with requirements pertaining to public disclosures regarding classified contracts and related brochures, promotional sales literature and reports to stockholders, as well as presentations at symposiums, conventions and so forth. Oversight may be accomplished by acquiring and reviewing material which is available upon public request and by random visits to conventions and symposiums that are open to the public.

24. Increased Emphasis on Classification Management

Discussion:

Executive Order 12356, "National Security Information," was signed by President Reagan on April 2, 1982, giving effect to the current rules governing the security classification of Government information and safeguards to protect such information from unauthorized disclosure. Under this order, the Defense Department establishes standards and procedures to achieve two objectives: (1) protect certain information when disclosure may damage national security, and (2) inform the American public about their Government's activities. Achieving the proper balance between these two equally important objectives is accomplished through effective classification management. By limiting classification to the minimum necessary to protect the national security, our ability to protect information that is properly classified is enhanced.

The classification process is the most fundamental component of the information security system. Original classification means an initial determination that information requires some degree of protection, for reasons of national security, against unauthorized disclosure, and the placement of markings to identify the information as classified. Once information is originally classified, it frequently serves as the basis for future classification actions. This is known as derivative classification. It is the determination that newly created information is, in substance, of the same sensitivity as information currently classified and thus the application of the same classification markings. Derivative classification currently accounts for about 95 percent of all classification actions. There are no original classifiers in defense industry; all classification actions in defense industry are

derivative actions based on Defense Department classification guidance.

Precise classification guidance is a prerequisite to the effectiveness of the Information Security Program and can ensure that security resources are expended to protect only that which truly warrants protection in the interest of national security. As such, greater emphasis is required of the classification management function.

Defense industry complaints of inconsistentcy incompleteness, or unavailability of security classification guidance are long-standing. The establishment of classification management positions in Defense Investigative Service Regional Offices has helped the situation somewhat, but more needs to be done. By way of example, in a 1983 memorandum to the Military Departments and other Defense components from the Acting Director of Information Security, ODUSD(P), it was stated:

... recent Information Security Program (ISP) reviews of selected Defense activities and contractors indicate a disquieting trend with respect to security classification guidance provided to contractors from DoD contracting activities. It has been found through sampling reviews of DD Forms 254 originated and received in activities visited that many of them are not properly prepared. Many DD Forms 254, for example, contain either insufficient or a total lack of guidance.

The Committee was also informed of a related concern regarding the potential compromise of information in the conceptual or research and development stage of a program or project. This allegedly occurs before the assignment of classification and requisite protective measures. The officials who expressed this concern were of the opinion that by the time a program or project is determined to be classified, and the particular classification parameters

established and promulgated, the existence of the program or project itself is widely known, along with many of the technical specifications. Much of this information is ultimately assigned a security classification. The concern, therefore, is that by the time the Department classifies certain information which is afforded expensive protection during the life cycle of a program, it may have already been compromised. This potentially serious problem could not be fully explored by the Committee but specific follow-up review appears warranted.

Additionally, a phenomenon that has caused industry concern over the years is the practice of furnishing an entire program/project classification guide to a contractor engaged in only a small portion or phase of a contract. This practice tends to undermine basic classification management principles and effective application of classification markings by industry. As defined within the Industrial Security Manual, classification guides are documents issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis. Although such guides are distributed along with a DD Form 254 (DoD Contract Security Classification Specification), the latter is frequently limited to a statement in the "remarks" section of the form referring to the attached detailed classification guidance. The completed DD Form 254, under most circumstances, should be sufficient to convey necessary classification instructions independent of an attached guide.

Since defense industry is on the receiving end of classification guidance provided by the Government, the scope of the DIS inspections is generally limited to ensuring proper receipt of the guidance and enforcing adherence with the guidance received. The development, substance, scope and

promulgation of the guidance is a classification management function that needs to be dealt with at the Government policy level, not in defense industry or by the DIS inspectors.

The problem of defense industry and the DIS is significantly greater in regard to classification guidance prepared and furnished to subcontractors via the DoD Contract Security Classification Specification (DD Form 254). However, even in that regard the classification guidance furnished must necessarily reflect guidance previously provided to prime contractors by the Government. It is extremely difficult, and in some instances impossible, to promulgate effective classification guidance when the source documents are deficient. Once again, the solution must come from Government.

The past 30 years have seen large increases in the total volume of information being classified and significant increases in the amount of that information placed in the hands of industry. Accordingly, it is imperative that systems improvements be initiated to reasonably ensure that only information that requires protection in the interest of national security be identified for safeguarding and that security costs be kept to a minimum. The proliferation of defective classification guidance encumbers the achievement of both of these national objectives. In addition, one of the more serious consequences of inadequate guidance is that the potential for unauthorized disclosure of classified information is generally increased.

Conclusion:

For policy level authorities to properly execute their responsibilities they must aggressively pursue the following initiatives in order to provide the guidance, standards,

criteria, procedures, and requirements that are essential for a positive classification management program.

- Develop, direct, and oversee an active DoD-wide program comprising all aspects of security classification, downgrading, declassification, and marking of official information in the interests of national security.
- Develop and promote programs for information security education and orientation of security cleared personnel throughout the DoD and defense industry, with particular emphasis on project managers.
- Develop and establish security classification guidance covering specific subject matters of multiservice interest for application throughout the DoD and defense industry.

Each contractor performing on a classified contract should receive only the classification, regrading, and declassification specifications applicable to its particular contract requirements. As a rule, only the prime contractor and major subcontractors should be provided an entire classification guide. All other subcontractors should be furnished necessary details via the DoD Security Classification Specification (DD Form 254), and if appropriate, by applicable extracts of the basic guide.

Another problem identified during the Committee's study is the distribution of documents prepared under contract to all interested/related prime and subcontractors. Not only does this perpetuate the "need to know" problem but it also enables hostile intelligence services to target the information by having identified the participating contractors.

Recommendations:

a. The senior DoD official who is delegated the functional responsibility of administering and overseeing the DoD Information Security Program should have ample authority and staff to implement an aggressive and effective program, with particular emphasis on security education and classification management. Quarterly DoD/defense industry regional classification management seminars should be initiated. These seminars will enable responsible policy, procurement, and security officials to remain current with DoD component/industry implementation of established policy and to receive complaints and recommendations for overall classification management improvement. The seminars would also provide for the promulgation of the latest policy developments and concerns, a continuing education and training program for DoD project managers and contractor classification specialists, and for the establishment of more active dialogue between DoD and defense industry.

b. The classification management aspects of the DoD Information Security Program should be subject to a separate study by a panel of experts, to include defense industry representation. The study should particularly emphasize the adequacy of the existing practices and procedures for promulgating and disseminating classification guidance to cleared defense contractors. In addition, the panel should determine whether information developed in the conceptual and research and development stages of a potential program or project is afforded adequate protection against unauthorized disclosure before the assignment of a security classification.

25. Prevention of "Bootlegging" of Classified Material

Discussion:

The "bootlegging" of classified material (i.e. unauthorized retention or transporting of classified material) has been described as a serious problem. Frequently, professional and technical personnel who author classified projects or studies retain personal copies of their work product through a sense of "pride of authorship" or for future reference. Since changing jobs is commonplace in high technology industry, often such unauthorized documents are taken by employees from company to company, or worse taken to a private residence.

Recommendation:

Security training should be strengthened by focusing attention on the "bootlegging" problem. As a preventive measure, procedures should be established for seeking approval and legitimate transfer of classified material. Moreover, a debriefing specifically addressing "bootlegging" should be administered to all cleared employees before termination of their employment. In addition, each employee should sign a certificate that states he or she possesses no classified material and is aware of the consequences for violating the terms of the certificate. The certificate will be retained for use in the event that the executor is determined to have "bootlegged" classified material. Finally, appropriate sanctions should be established for contractors who knowingly and willingly assume custody of classified material known to have been "bootlegged."

**SUMMARY OF THE COMMITTEE'S RECOMMENDATIONS
REGARDING CHANGES IN THE DEFENSE
INDUSTRIAL SECURITY PROGRAM**

1. Increased Emphasis on Counterintelligence and Human Reliability Within the Defense Industrial Security Program (DISP)

The DIS administration and oversight of the DISP should include a balance of administrative inspections and attention, in partnership with industry, to the human reliability aspects of the program with emphasis on the hostile intelligence threat. This would necessitate a closer alignment of the DIS with the counterintelligence community and development of a viable threat awareness program.

2. Priority Emphasis on Security of Sensitive Contracts

DoD procurement activities, employing a reasonable apportionment system, should prioritize classified contracts according to assessed sensitivity. Commensurate DIS resources would be applied to these contracts based on the assessed sensitivity.

3. Revision of the Industrial Security Manual

Where feasible, promulgate general security policy to replace much of the inordinate detail in the current Industrial Security Manual (DoD 5220.22-M). In addition, large segments of the Industrial Security Manual that have limited applications should be extracted and put in supplement or handout form. Furthermore, tailor specific security requirements for individual contractor facilities into contractors' Standard Practice Procedures (Security Manual), taking into account the local hostile intelligence threat.

4. DIS Inspection of Special Access Programs

a. That the Department of Defense Inspector General, during audits of special access programs, determine the adequacy of, and compliance with, DoD contracting practices, contractor performance, management of program funds and other areas of special access programs and carve-out contracts.

b. That the Office of the Deputy Under Secretary of Defense for Policy continue to support the audit efforts of the Department of Defense Inspector General and coordinate with DoD components the program access authorizations required by audit personnel.

c. That the DIS establish a special group of inspectors for special access programs and related "carve-out" contracts and that DoD components relinquish to the DIS inspection of these programs and contracts when determined appropriate by the sponsoring component.

5. Strengthening the Adjudication Process

The Committee recommends that the term "guidelines" be revised to read "requirements" and be applied uniformly in all cases.

6. Centralization of the Adjudication Function Within the Department of Defense

That the Deputy Under Secretary of Defense for Policy determine whether the Adjudication Division of DISCO is in fact performing adjudicative functions within the purview of the Administrative Procedures Act. Each case should be reviewed carefully once, subject to the approval of the individual in charge of the centralized adjudication function. Furthermore,

that a separate study be conducted to assess the merits of centralizing the adjudication function (separately and distinctly from any investigative organization) within the Department of Defense for adjudication of all security clearances to include cases under the DISP. Finally, obtain subpoena power to compel attendance of witnesses and production of records at the hearings in the Industrial Personnel Security Clearance Program.

7. Revising the Frequency of Industrial Security Inspections

That the current inspection schedule prescribed by paragraph 4-103a, "Industrial Security Regulation," be replaced by a system that more effectively considers the volume and complexity of classified activity. The new system should also include sufficient flexibility to enable local managers to adjust workload and concentrate effort where most needed. Furthermore, that routine inspections of "dormant" facilities be discontinued and that inspections of "access elsewhere" facilities be eliminated or significantly curtailed.

8. Reporting of All Foreign Travel by Contractor Personnel

All cleared employees be required to report to the facility security department all instances of foreign travel for review by DIS representatives during industrial security inspections.

9. Creation of Separate Advisor and Inspector Roles of DIS Representatives

DIS should adopt a pilot program in which individual industrial security representatives function either as advisors to industry or as regulatory inspectors.

10. Establishment of a National Industrial Security Hotline

Establish a 2-year pilot national DoD Industrial Security Hotline Program within the Defense Investigative Service and appropriately publicize it.

11. Assignment of DIS Personnel to Extremely Complex or Particularly Sensitive Contractor Facilities

The Director, Defense Investigative Service, should develop and initiate a pilot program in coordination with industry for the assignment of industrial security representatives on a full-time or substantially full-time basis at certain complex and particularly sensitive contractor facilities.

12. Establishment of a Graded Defense Industrial Security Program Inspection Rating System

The DoD security inspection rating system be changed to provide for ratings of "Superior," "Satisfactory," "Marginal," and "Unsatisfactory." Moreover, DoD contracting activities should maintain close liaison with the Defense Investigative Service before the award of classified contracts.

13. Specialized Training Program for Accrediting Contractor Security Personnel

The DIS provide a formal certification/accreditation training program for contractor industrial security personnel. The training program need not be mandatory.

14. Notification of the DIS of Criminal Investigations Involving Cleared DoD Contractors and Contractor Personnel

At the earliest practical time, DoD criminal investigative organizations should notify the DIS of criminal investigations that indicate criminal conduct on the part of cleared DoD contractors and contractor personnel.

15. Legislative Base for the Defense Industrial Security Program

Establish a working group to draft new legislation that would carefully address the problems of prosecution of espionage including the need to declassify the information involved in the prosecution.

16. Legislation to Limit Administrative and Judicial Review of DoD Personnel Adjudication to the Adjudicative Procedures Themselves

A panel should be formed to study legislative initiatives to limit administrative and judicial review of DoD personnel security adjudications to the adjudicative procedures and to exclude review of the adjudicative decisions of the Directorate of Industrial Security Clearance Review.

17. Authority to Suspend and Debar Contractors for Serious Security Infractions

The Committee recommends amending DoD FAR Supplement 9.470 to clearly identify security violations that may be used as the basis for suspension and debarment. The DIS should be required to provide notice to the cognizant DoD suspension/debarment authority of all significant security violations on the part of cleared contractors or their cleared employees.

18. Revised Scope of Personnel Security Investigations

That negotiations be initiated to amend the Director of Central Intelligence Directive No. 1/14, dated 1 September 1983, to require subject interviews as part of the minimum investigative standards for the SBI and that currently prescribed neighborhood and education check/verifications be deleted from said DCID as required elements of investigative coverage.

19. Enhancement of Personnel Security Investigative Standards and Reduction of Industrial Clearances

a. The Deputy Under Secretary of Defense for Policy should revise the current system used to determine priority consideration for the conduct of periodic reinvestigations (PRs). The new system should identify those Top Secret-cleared (and perhaps those with Sensitive Compartmented Information access) who have continuous or recurring access to Top Secret information and should subject only those individuals to the PR requirements. Those who have never had access to Top Secret or who rarely have such access should be eliminated from PR consideration or placed on a low priority listing, as appropriate.

b. Clarify the policy to ensure that contractor personnel determined eligible to be processed for a NAC under physical-access-only circumstances do not qualify and shall not be processed for a personnel security clearance under the Defense Industrial Security Program.

c. The cognizant security office should be authorized, upon receipt of appropriate justification, to approve contractor employees for one-time or occasional access to

classified information at one level higher than the personnel security clearance in effect.

d. All company-granted Confidential personnel security clearance documentation should be furnished to the DISCO for review, recordation, and a DCII check.

e. All company-granted Confidential personnel security clearances should automatically expire 5 years from date of issuance unless the need is rejustified. To remain valid for a longer period, an updated PSQ, Clearance Justification Data Sheet and Counterintelligence Questionnaire shall be received by the DISCO for review before the scheduled expiration date. Reissuance by the DISCO, if otherwise appropriate, shall be based on a favorable National Agency Check and shall remain valid as long as the employee has a need for access and remains employed by the same contractor.

f. Industrial personnel security clearance policies and procedures must be changed to permit the use of interim clearance procedures prescribed by the "Industrial Security Regulation," DoD 5220.22-R; and remove the requirement for contracting officer or higher level approval, for all personnel security clearance requests.

g. All Top Secret and Secret industrial personnel security clearances shall be subject to automatic downgrade to the next lower level of clearance when DISCO does not receive justification to retain the higher level clearance within 5 years from the date of issuance.

h. All Secret industrial personnel security clearances should be based initially on a National Agency Check, local agency check, credit check and employment check which shall be repeated every 5 years thereafter.

i. All personnel security questionnaires submitted to the DISCO, regardless of level, should be accompanied by a Clearance Justification Data Sheet.

j. All personnel security questionnaires submitted to the DISCO, regardless of the level of clearance requested, shall be accompanied by a completed counterintelligence questionnaire.

20. Documentation in Standard Practice Procedures Relating to Disciplinary Action for Security Violations

That contractors be required to establish in their SPPs company policy on disciplinary action to be taken against employees involved in security violations when culpability is established. The DIS shall be limited to advising and assisting the contractor in its preparation of the policy if requested.

21. System of Controls Over After-Hours Access and Reproduction Equipment at Cleared Facilities

a. The DoD should adopt a policy requiring cleared Defense contractors to develop and effectuate procedures that ensure that all persons working or visiting the proximity of repositories or areas used to store classified material during nonworking hours are monitored by continuous or intermittent means capable of preventing or detecting physical presence, unauthorized access, and removal of classified material from the premises.

b. The DoD should adopt a policy requiring cleared contractors to develop and place into effect procedures that ensure that reproduction equipment is monitored by continuous or intermittent means to prevent or detect the unauthorized copying of classified material. The specific control

procedures shall be developed in consultation with the DIS and incorporated with the individual facility's Standard Practices Procedure and be subject to DIS inspections.

**22. Access to the Defense Technical Information Center
Classified Data**

a. That the Inspector General, Department of Defense, schedule an audit of the Defense Technical Information Center to ascertain whether internal controls exist to preclude the unauthorized disclosure of and access to its scientific and technical products and services. The scope of the audit shall encompass procuring activity justification for authorizing the broad areas of interest for access by contractors.

b. That the Deputy Under Secretary of Defense for Policy designate a Department of Defense counterintelligence component to evaluate any potential threat to the Center from hostile intelligence services. In this regard, the appropriate countermeasures should be taken to protect its personnel, products, services and data base from potential compromise.

**23. Proactive Efforts by the DIS to Prevent Unauthorized
Disclosures**

The DIS should incorporate proactive efforts to oversee compliance with requirements pertaining to public disclosures regarding classified contracts and related brochures, promotional sales literature and reports to stockholders, as well as presentations at symposiums, conventions and so forth. Oversight may be accomplished by acquiring and reviewing material which is available upon public request and by random visits to conventions and symposiums that are open to the public.

24. Increased Emphasis on Classification Management

a. The senior DoD official who is delegated the functional responsibility of administering and overseeing the DoD Information Security Program should have ample authority and staff to implement an aggressive and effective program, with particular emphasis on security education and classification management. Quarterly DoD/defense industry regional classification management seminars should be initiated. These seminars will enable responsible policy, procurement, and security officials to remain current with DoD component/industry implementation of established policy and to receive complaints and recommendations for overall classification management improvement. The seminars would also provide for the promulgation of the latest policy developments and concerns, a continuing education and training program for DoD project managers and contractor classification specialists, and for the establishment of more active dialogue between DoD and defense industry.

b. The classification management aspects of the DoD Information Security Program should be subject to a separate study by a panel of experts, to include defense industry representation. The study should particularly emphasize the adequacy of the existing practices and procedures for promulgating and disseminating classification guidance to cleared defense contractors. In addition, the panel should determine whether information developed in the conceptual and research and development stages of a potential program or project is afforded adequate protection against unauthorized disclosure before the assignment of a security classification.

25. Prevention of "Bootlegging" of Classified Material

Security training should be strengthened by focusing attention on the "bootlegging" problem. As a preventive measure, procedures should be established for seeking approval and legitimate transfer of classified material. Moreover, a debriefing specifically addressing "bootlegging" should be administered to all cleared employees before termination of their employment. In addition, each employee should sign a certificate that states he or she possesses no classified material and is aware of the consequences for violating the terms of the certificate. The certificate will be retained for use in the event that the executor is determined to have "bootlegged" classified material. Finally, appropriate sanctions should be established for contractors who knowingly and willingly assume custody of classified material known to have been "bootlegged."

APPENDIX I

Overview of the Defense Industrial Security Program

DEFENSE INDUSTRIAL SECURITY PROGRAM - OVERVIEW

Over the years, the Department of Defense (DoD) has developed a comprehensive Industrial Security Program designed to safeguard classified information released to industry. The current authority for the program is Executive Order (E.O.) 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by E.O. 10909, January 17, 1961. In addition to the Defense Department, eighteen other Federal agencies and departments use the services and procedures of this program, pursuant to authority granted by E.O. 10865. This is accomplished by an exchange of letters between the Secretary of Defense and the heads of non-DoD departments and agencies (User Agencies) for which the Secretary of Defense is authorized to act in rendering industrial security services. User Agencies include the Office of the Secretary of Defense (OSD) (including all boards, councils, staff and commands); DoD agencies and the Departments of the Army, Navy, and Air Force (including all of their activities); National Aeronautics and Space Administration; General Services Administration; Small Business Administration; National Science Foundation; Environmental Protection Agency; Federal Emergency Management Agency; Federal Reserve Board; General Accounting Office; U.S. Information Agency; U.S. Arms Control and Disarmament Agency; and the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice.

The Deputy Under Secretary of Defense for Policy (DUSD(P)) is responsible for developing and approving of all security policy under the Defense Industrial Security Program (DISP). The DISP is administered by the Director, Defense Investigative Service (DIS). DoD Directive 5220.22 implements E.O. 10865 within the Defense Department and authorizes publication of the "Industrial Security Regulation" (DoD 5220.22-R) and the Industrial Security Manual (DoD 5220.22-M). The "Industrial

Security Regulation" (ISR) sets forth policies, practices, and procedures of the DISP used internally by the DoD to insure maximum uniformity and effectiveness in its application throughout industry.

The DoD Industrial Security Manual (ISM), a companion document to the ISR, contains detailed security requirements to be followed by U.S. contractors entrusted with safeguarding classified information. The ISM is made applicable to industry by management agreement, in concert with the DIS, to the terms of the Department of Defense Security Agreement (DD Form 441), and by direct reference in the "Military Security Requirements" clause in the contract.

The ISR and ISM are written in terms of the most common situation in which contractors have access to classified information in connection with performance of a classified contract; however, they are also applicable to the safeguarding of classified information in connection with all aspects of post-contract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract, such as classified information released pursuant to a User Agency program that a firm, organization, or individual participated in on a voluntary or grant basis. This includes foreign classified information that the U.S. Government is obliged to protect in the interest of national security.

The security policy under the DISP is approved only after coordination with the User Agencies. Proposed changes for policy improvement are initiated within the office of the DUSD(P), by the DIS, by the User Agencies, or at the suggestion of industry. Concerns of industry are usually expressed through the Council of Defense and Space Industry Associations (CODSIA). The CODSIA is given the opportunity to review and

comment on proposed changes to the ISM before approval and publication.

Although actual administration of the DISP is assigned to the Director, DIS, the responsibility for security cognizance for all contractors and industrial facilities under the DISP has been assigned to the DIS Deputy Director (Industrial Security). Security cognizance authority has, in turn, been delegated to Regional Directors of Industrial Security for all contractor facilities located within prescribed geographical boundaries. There are eight DIS Directors of Industrial Security located throughout the United States.

At present, the DISP includes nearly 14,000 cleared facilities with about 1,400,000 cleared contractor employees. Furthermore, it is estimated that private industry possesses about 16 million classified documents under the DISP. Worldwide, approximately 800 DIS personnel are assigned to Industrial Security Program related duties and responsibilities, of which approximately 200 of these are engaged in field inspection activities.

Under the DISP, the User Agencies may release classified information to contractors, but only after the management and personnel of the industrial facility have been investigated and a determination has been made that access to and custody of such information is consistent with the national security. An integral part of this determination is to ensure that cleared contractor facilities are sufficiently insulated from foreign ownership, control, and influence. Once cleared, contractor facilities are subject to periodic security inspections by industrial security representatives from the DIS Industrial Security Regional offices (cognizant security offices).

A contractor is not permitted to solicit his own security clearance. In order to be processed for a facility security clearance, the contractor must have an impending need for access to classified information. The prospective contractor must be sponsored by a Government contracting activity or a cleared contractor already engaged in classified contracts or programs who wishes to use the services of the prospective contractor in a capacity that requires access to classified information. This requirement is designed to ensure that investigative resources are not unnecessarily expended and that a facility is not cleared unless there is a valid need for classified access.

Staff personnel at each cognizant security office assist the Director of Industrial Security in administering the various aspects of the DISP. Such functions generally include:

- a. Processing facility security clearances for industrial facilities located within the region's geographical area and maintaining such clearances in a current status once granted.
- b. Evaluating factors of foreign ownership, control or influence that may be present in the facility.
- c. Processing conditions that have changed at the facility since it was initially granted a clearance.
- d. Responding to requests for verification of facility clearances and assessing the capabilities of the facility to safeguard classified information.
- e. Monitoring international aspects of the program, to include assisting in the arrangement for government-to-

government transmission channels for the movement of classified information or products.

f. Assuring quality and uniformity of all inspections and surveys conducted by the industrial security representatives in the field.

g. Processing all cases involving violations of security procedures and compromise of classified information.

h. Monitoring compliance with established automated data processing security requirements.

The U.S. Government representative who most directly interfaces with industry on industrial security matters is the industrial security representative, who is normally assigned at a DIS field office or resident office proximate to the contractor facility. There are about 200 of these individuals in more than 80 offices throughout the U.S. and Europe. The industrial security representative primarily is responsible for the following:

a. Provides orientation on the DISP to private industry.

b. Conducts surveys to ascertain a contractor's eligibility to have access to classified information.

c. Conducts recurring inspections to ascertain the contractor's adherence to the requirements of the ISM and his continuing ability to safeguard classified information.

d. Reviews and monitors the security aspects of all classified contracts and ensures that the contractor is provided adequate classification guidance.

e. Serves as the official representative of the cognizant security office/U.S. Government on all matters pertaining to industrial security.

f. Provides advice and assistance to the contractor.

g. Recommends invalidation or revocation of a contractor's facility security clearance in appropriate circumstances.

h. Conducts administrative inquiries into the loss, compromise, or suspected compromise of classified information

MAJOR DISP FIELD EXTENSIONS

Defense Industrial Security Clearance Office (DISCO)

An important adjunct to the DISP is a system for determining the eligibility of industrial personnel for access to classified defense information. This function is performed centrally by the DISCO located in Columbus, Ohio. The DISCO receives requests for personnel security clearances from DoD contractors and from contractors of other User Agencies; obtains Reports of Investigations (ROIs) from appropriate investigative agencies; evaluates personnel security request documentations and ROIs and issues clearances. The DISCO may reject requests for certain administrative reasons, but rejection that is based on derogatory information is not within the scope of the DISCO authority. Cases with significant derogatory information are referred to the Office of General Counsel, DoD, Directorate for Industrial Security Clearance Review Office (DISCR) for review and determination. The DISCO also processes overseas assignment notifications, assurances, and reciprocal clearances. The DISCO maintains a computerized records system (MODISCO) for the preservation and ready

accessibility of all industrial personnel and facility security clearances, maintains facility clearance records, and retains for the prescribed period the individual case folders pertaining to clearance actions. It also controls shipment to contractors of the blank forms required for initiation of personnel security clearance actions.

The Department of Defense considers the granting of a clearance to be a privilege, not a right. In order to be granted a security clearance, an individual must meet certain basic requirements such as the following:

- Attain minimum age
- Be employed by a cleared contractor
- Have a position that requires access to classified information
- Complete a personnel security questionnaire (PSQ) providing a detailed account of his personal history
- Must be relatively free of significant derogatory information
- Compliance with security regulations
- Must continue to be employed in a position requiring access to classified information

Defense Security Institute (DSI)

Established in 1972, the Defense Security Institute (DSI), located at Richmond, Virginia, offers specialized security training to eligible industry and Government personnel. These personnel are provided both with formal training and a forum in which to express recommendations for improvement of the DISP. In addition to providing DISP-oriented training, the DSI is tasked with presenting courses of instruction on the Defense Industrial Facilities Protection Program, the Personnel Security Investigations Program, and the Defense Information

Security Program. The DSI also develops training bulletins, correspondence courses and counterintelligence awareness briefings for use by DIS personnel and defense contractors. Every other year, DSI schedules an International Industrial Security Orientation Program to familiarize foreign industrial security officials with the DISP and to surface any problems with implementation of specific bilateral security agreements.

Offices of Industrial Security International (OISI)

The Office of Industrial Security International is located in Brussels, Belgium and Mannheim, West Germany. The OISI office performs the following functions:

- Serves as central points for maintaining personnel security clearance records issued on behalf of contractor personnel assigned outside of the U.S. Uses these records to process classified visit requests to U.S. Government, foreign government and North Atlantic Treaty Organization (NATO) activities when required and to confirm clearance data with these activities and contractors when appropriate.

- Processes requests for NATO Security Clearance Certificates and NATO Facility Security Clearance Certificates pursuant to DoD Directive 5210.60 and U.S. Security Authority for NATO (USSAN) Instructions 1-69 and 1-70. Maintains an index of such clearances and disseminates clearance verification of U.S. Government, foreign government and NATO activities upon request.

- Provides advice, guidance and assistance on industrial security matters to U.S. contractors and U.S. Government activities. Provides security briefings and assists in the processing of classified visit requests of cleared industrial representatives.

- Provides advice, guidance and assistance on industrial security matters to U.S., foreign and international organization officials. Maintains liaison with such officials on a recurring basis.

- Provides limited classified storage facilities to User Agencies or cleared U.S. contractors. Ensures that material that is not releasable to foreign governments or their citizens is safeguarded within a U.S. Government-controlled activity.

- Assists in the establishment of government-to-government transmission channels between the U.S. and foreign governments. Serves as a conduit for the designated U.S. Government Representative in processing classified material received from a foreign government.

- Conducts industrial security inspections of contractor facilities located overseas on U.S. Government controlled military installations.

In conclusion, the Deputy Under Secretary of Defense (Policy) (DUSD(P)), is the senior DoD official responsible for overall policy guidance and management oversight of the DISP. Staff representatives of the DUSD(P) arrange periodic visits to DIS activities to determine the effectiveness of the operations and adequacy of practices and procedures that are used in the administration of the DISP.

The DISP was functionally transferred from the Defense Logistics Agency to the Defense Investigative Service in October 1980. The DIS was established in 1972 to provide a single centrally directed service within the Department of Defense for conducting personnel security investigations. Today, it is a separate DoD agency headquartered in Washington, D.C.

APPENDIX II

**Memorandum of the Deputy Under Secretary of Defense
for Policy and Committee Charter**



POLICY

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

In reply refer to
I-16218/84ct
24 JAN 1984

MEMORANDUM FOR SECRETARY OF THE ARMY
SECRETARY OF THE NAVY
SECRETARY OF THE AIR FORCE
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: DoD Industrial Security Review Committee

Attached is a memorandum which describes the formation of subject Committee to analyze the effectiveness of current industrial security requirements and develop recommendations for Industrial Security Program improvement. Members of the Committee are as follows:

Daniel R. Foley, Office of the Inspector General, DoD,
Co-Chairman
John R. Hancock, Defense Investigative Service,
Co-Chairman
Kathleen A. Buck, Office of General Counsel, DoD,
Member
John E. Fields, Office of the Deputy Under Secretary of
Defense (Policy), Member
Alvin L. Madison, Office of the Inspector General, DoD
Member
Alfred W. Hazen, Defense Investigative Service,
Member

The Committee plans to conduct interviews of appropriate personnel within the Office of the Secretary of Defense, the Military Departments, and selected DoD components. Interviews will generally be focused in the areas of security, counterintelligence, law enforcement and procurement acquisition activities. Security clearances of Committee members will be passed separately, when required.

In order to facilitate the work of the committee, it is requested that each addressee identify a primary point of contact within your Department/Agency by February 1, 1984 and apprise Mr. Daniel Foley by telephone at 694-1247.

Richard G. Stilwell
Richard G. Stilwell
General, USA (Retired)
Deputy

Attachment



POLICY

THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

In reply refer to:
I-16218/83

06 DEC 1983

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE INVESTIGATIVE SERVICE

SUBJECT: DoD Industrial Security Review Committee

As you are aware, on October 24, 1983, I authorized the formation of a DoD panel to examine events associated with the arrest of James Durward Harper, Jr., for alleged espionage activity. The panel, under the general direction of the Director, Defense Investigative Service (DIS), with representation from my office, the Office of the Inspector General, and the Office of the General Counsel, was to study the modus operandi of Harper, Harper's wife, and the security posture of the DoD contractor from which the classified material was diverted. Within this context, the panel was to analyze the effectiveness of current industrial security requirements and develop recommendations for program improvement.

In light of the policy implications and to assist the panel with its responsibilities, I have decided to redesignate the panel as the DoD Industrial Security Review Committee and place it under my general auspices. Chairmanship will continue to be shared by the current Committee representatives from the Office of the Inspector General, DoD, and the Defense Investigative Service. Comments from industry and the DoD Components are encouraged although any such assistance from industry must be considered advisory in nature. This does not preclude Committee participation by a suitable industry representative on a selected basis, provided the Committee deems it essential, and that such an appointment is approved in accordance with applicable directives and instructions.

The importance of this review and its potential for enhancing the overall effectiveness of the Defense Industrial Security Program are evident. Accordingly, I ask that this effort be conducted objectively, and that ample time be devoted by each member to Committee business, which must be considered of the highest priority.

In full appreciation of the nature and scope of this review effort, I ask that the Committee's final report be completed and available for my review and consideration at the earliest possible date. In addition, beginning mid-January, I would appreciate a biweekly briefing concerning the Committee's progress.


Richard G. Stilwell
General, USA (Ret.)
Deputy

APPENDIX III

Memorandum of the Acting Secretary of the Air Force



DEPARTMENT OF THE AIR FORCE
WASHINGTON, D.C. 20330

1033 NOV 19 11 11 24

11 11 24

OFFICE OF THE SECRETARY

November 15, 1983

MEMORANDUM FOR THE SECRETARY OF DEFENSE

SUBJECT: Industrial Security - ACTION MEMORANDUM

The current espionage case (James Harper/Systems Control Inc) is the second case detected in a fairly short period in which Soviet Bloc intelligence has collected large amounts of sensitive information by penetrating a cleared defense contractor. In the other case (William Bell/Hughes Aircraft) the damage was extensive and serious, and it appears the same will prove true in the Harper case. Both cases involved facilities and persons cleared under the Defense Industrial Security Program.

The massive Soviet effort to collect US technology, classified and unclassified, is well documented. There is no reason to believe the cases we know of are isolated instances of successful espionage against cleared contractors. They are more likely just the tip of the iceberg. Our whole defense effort relies heavily on technological advantage. All of this technology is in the hands of the contractors who do our basic research and weapons development work, and the potential damage from successful espionage against these firms is unlimited.

We need to conduct an objective review of the Defense Industrial Security Program, and I recommend that the DOD Inspector General conduct such a review. I am sure that the Defense Investigative Service reviews its own efforts, and there have been some outside looks at parts of the Industrial Security Program in terms of economy and efficiency. However, to the best of my knowledge there has never been an outside, unbiased evaluation of the security effectiveness of the program. I recommend that this be the thrust of the DOD Inspector General review.

E. C. Aldridge, Jr.
Acting Secretary of the
Air Force



READY THEN

READY NOW

I-16218/83
49903

APPENDIX IV

Memorandum of the Secretary of Defense



THE SECRETARY OF DEFENSE

WASHINGTON, THE DISTRICT OF COLUMBIA

14 DEC 1983

MEMORANDUM FOR THE SECRETARY OF THE AIR FORCE

SUBJECT: Industrial Security

This is in response to your memorandum of November 15, 1983, expressing concern for the effectiveness of the Industrial Security Program as a result of recent espionage cases involving cleared contractors and their personnel.

I fully share your concern and agree that an objective review of the Defense Industrial Security Program (DISP) is indicated. In this regard, you will be pleased to know that on October 24, 1983, the Deputy Under Secretary of Defense for Policy (DUSD(P)) authorized the formation of a DoD Security Commission to examine events associated with the arrest of James Durward Harper, Jr. for alleged espionage activity and to review the security conditions present at the firm from which the classified material was diverted. Moreover, the Commission is charged to conduct a comprehensive evaluation of the effectiveness of the DISP, overall, and to make recommendations for general improvement. This Commission which is co-chaired by the Office of the Inspector General and the Defense Investigative Service, includes representation from ODUSD(P) and the Office of General Counsel, DoD.

The Commission has had meetings with the Federal Bureau of Investigation to review the modus operandi of Harper and his wife. However, for obvious reasons, until the Harper case comes to trial and receives disposition in court, the Commission is obligated to coordinate its activity with the FBI.

The Commission has researched the case of William Bell and Marian Zacharski which included reviewing trial transcripts and Bell's testimony before the Senate Permanent Subcommittee on Investigations.

I am confident that the Commission is sufficiently competent to comply with its given mandate and will conduct its evaluation of the DISP in an impartial and professional manner. The findings and recommendations of the Commission will be formally reported to the DUSD(P) for appropriate action. However, I have asked that the Commission determine whether further review by the Inspector General is necessary in order to evaluate the effectiveness of the program.

In a related and parallel action, the House Armed Services Investigations Subcommittee has announced it will likewise conduct an examination of the administration of the DISP by the Defense Investigative Service.

APPENDIX V

Committee Letter to Defense Contractors/Government Agencies



DEFENSE INVESTIGATIVE SERVICE

1900 Half Street, S.W.
Washington, D.C. 20324-1700

S A M P L E

December 1983

General Electric Co.
Easton Turnpike
Fairfield, CT 06431

Dear Facility Security Supervisor:

Within the Department of Defense, a Committee has been established to analyze the effectiveness of current industrial security requirements and develop recommendations for program improvement. Recent espionage cases reflect a need to examine current procedures and determine whether we can do a better job to protect classified and other sensitive technical information.

The importance of this review and its potential for enhancing the overall effectiveness of the Defense Industrial Security Program are evident. To assist the Committee in this review we welcome comments from industry and government with regard to any recommendations pertaining to procedural improvements in the program. These comments can address, but should not be limited to, topics such as the processing of personnel security clearances, classification management procedures, physical security requirements, or even the administration of the program by the Defense Investigative Service. In view of the timely nature of this Committee's work, it is requested that your comments be submitted within the next thirty days. They should be forwarded to:

Defense Investigative Service
Directorate for Industrial Security
ATTN: Mr. John R. Hancock (V0430)
1900 Half Street, S.W.
Washington, D.C. 20324

Thank you for your assistance in this matter.

JOHN R. HANCOCK
Chairman
Defense Industrial Security Review Committee



DEFENSE INVESTIGATIVE SERVICE
1900 Half Street, S.W.
Washington, D.C. 20324-1700

S A M P L E

December 1983

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR RESEARCH & ENGINEERING

SUBJECT: Defense Industrial Security Review Committee

Within the Department of Defense, a Committee has been established to analyze the effectiveness of current industrial security requirements and develop recommendations for program improvement. Recent espionage cases reflect a need to examine current procedures and determine whether we can do a better job to protect classified and other sensitive technical information.

The importance of this review and its potential for enhancing the overall effectiveness of the Defense Industrial Security Program are evident. To assist the Committee in this review we welcome comments from industry and government with regard to any recommendations pertaining to procedural improvements in the program. These comments can address, but should not be limited to, topics such as the processing of personnel security clearances, classification management procedures, physical security requirements, or even the administration of the program by the Defense Investigative Service. In view of the timely nature of this Committee's work, it is requested that your comments be submitted within the next thirty days. They should be forwarded to:

Defense Investigative Service
Directorate for Industrial Security
ATTN: Mr. John R. Hancock (V0430)
1900 Half Street, S.W.
Washington, D.C. 20324

Thank you for your assistance in this matter.

JOHN R. HANCOCK
Chairman
Defense Industrial Security Review Committee

APPENDIX VI

Administrative Inquiry - Systems Control, Inc. (SCI)



DEFENSE INVESTIGATIVE SERVICE

OFFICE OF THE REGIONAL DIRECTOR
BUILDING 31, ROOM 114
PRESIDIO OF SAN FRANCISCO, CA 94129

SAN FRANCISCO REGION (V5200)

January 30, 1984

IN REPLY
REFER TO

SUBJECT: Administrative Inquiry - Systems Control, Inc., (SCI),
1801 Page Mill Road, Palo Alto, California 95650

1. Authority: This inquiry was initiated by the Director, Defense Investigative Service in accordance with paragraph 5-102, Department of Defense Industrial Security Regulation (DOD 5220.22R). It was predicated upon disclosure through the filing of a criminal complaint, Docket No. CR-83-234-MISC, on 14 October 1983 before a United States Magistrate in the United States Courthouse by an agent of the Federal Bureau of Investigation (Attachment 1) stating in substance as follows: Beginning in May 1979, James Durward Harper, Jr., in concert with Ruby Louise Schuler, an employee of SCI had removed classified defense information from SCI, reproduced copies of the material, returned copies of the material removed from SCI to that company, and subsequently transported some of the reproduced copies of the classified defense material to Warsaw, Poland; places in Mexico; Vienna, Austria; and Geneva, Switzerland. Some of the reproduced material was turned over to the Polish Intelligence Service of the Polish People's Republic which in turn delivered the material to agents of the Union of Soviet Socialist Republics. Harper sold the material relating to the National Defense of the United States for a sum in excess of \$250,000.00. All this activity identified with Harper was in violation of Title 18, United States Code, Section 794(a)(c). The initiation of the inquiry was delayed at the verbal request of the Federal Bureau of Investigation and the United States Attorney for the Northern California District. This request was later confirmed in writing by the U.S. Attorney on 8 November 1983 (Attachment 2). Due to the ongoing Grand Jury proceedings and pre-trial activity by the U.S. Attorney this inquiry was restricted to establishing four things, (1) whether or not the failure to comply with the Industrial Security Program requirements at SCI contributed to the activities of Harper and Schuler, (2) positive identity of classified material known to have been compromised in this instance, (3) identity of classified material that may have been accessed by Schuler during the course of her employment with SCI that could have been removed from the facility but has not been identified by the Federal Bureau of Investigation and (4) identity of U.S. Government contractors and user agencies responsible for programs/contracts related to the compromised classified material. The inquiry was conducted at Systems Control Technology, Inc. (SCI), successor company to subject, at the same street address, during the period 14-20 December 1983, 4-5, 20 and 25 January 1984, by the writer, Mr. Rodger H. Raasch, Northwestern Region, and Mr. John Hancock, Headquarters, Defense Investigative Service.

2. Essential Facts:

a. Subject facility (SCI) was previously cleared Top Secret at its present location. Records in this office reflect that it was engaged in

classified contract work for the Ballistic Missile Defense Systems Command, Huntsville, Alabama; U.S. Air Force agencies at Wright-Patterson Air Force Base, Ohio; Naval Electronic Systems Command, Washington, D.C.; Office of Naval Research, Arlington, Virginia; and other U.S. Navy and U.S. Air Force contracting agencies. In 1980 facility began negotiations with representatives of the British Petroleum Company, Ltd., for sale of all interest in SCI to the British firm. Following completion of the negotiations and sale, SCI was cleared UK Reciprocal-Secret based upon its foreign ownership and the UK Secret clearance of the parent company. This occurred on 31 March 1981. Within the same period of time, the company determined that in order to effect a complete separation of the classified defense work from the influence of the foreign parent company, as required by the cognizant Industrial Security Office, it moved its classified work into other office areas in early 1981 and set up what is called a "spin-off" company known as Systems Control Technology, Inc. (SCT) with its own officers, directors, executive personnel, and stock held under a proxy agreement. Additional information concerning this process is contained in Attachment 3. In an undated letter received in Northwestern Region on 19 November 1981, Ballistic Missile Defense Command requested that SCT be cleared to the level of Top Secret. Facility had been issued a US Secret facility clearance on 11 December 1981 which was upgraded when a Top Secret facility clearance was issued on 13 January 1983 by the Northwestern Region, Defense Investigative Service.

b. Attachment 1 reflects that Harper and Schuler began the removal and reproduction of classified defense information from SCI sometime in May 1979. Our inquiry was concentrated in the time period when Schuler was initially cleared as an employee of SCI until the date of the termination of her clearance and subsequent termination of employment. Records of the Defense Industrial Security Clearance Office, Columbus, Ohio, reflect that Schuler was cleared to the Secret level on 8 September 1977 based on a National Agency Check. Her clearance was terminated on 21 August 1981 based upon the fact that she was not transferred to the new facility (SCT) from SCI but remained as an employee of SCI (Attachment 4). A check of the personnel file maintained on Schuler by SCI reflects that:

(1) She was employed at SCI in 1972 and became a secretary to Mr. Robert Larson in 1976. Evaluation reports and other administrative documents contained in the file revealed that Larson was her supervisor through her last day of work on 26 July 1982 when she was placed in a medical leave of absence and underwent extensive surgery, the cost of which was borne by the insurance carrier of the employer. Her date of death was listed as 22 June 1983. There was no documentation in the file which reflected that she was ever assigned to or worked for SCT. A copy of the death certificate in the file reflected that Schuler died from "cirrhosis, alcohol, a primary cause". "Alcoholism a secondary cause". A contributing cause was listed as an operation related to a la vien peritoneal venous shunt.

(2) Interviews with William Jones, E.C. Burrma, Kenneth M. Kessler, William Anton, all current employees of SCT, and formerly on the staff of SCI. They were acquainted with Schuler and all stated in substance that Schuler worked exclusively for Larson and did not type or work on classified material for which they were responsible. They were not aware of specific

classified material Schuler may have had access to but were in general agreement that she had access to everything stored in safe #26 in Larson's office and anything that passed through his office. They also expressed the opinion that Schuler's access was generally restricted to Ballistic Missile Defense System related material because that was Larson's primary area of expertise. None of these individuals had Schuler reproduce classified material for them. Anton recalled that he had her work on some unclassified slides for him at one time.

(3) Attachment 5 is a copy of the indictment dated December 9, 1983 filed by the United States Attorney in the United States Court for the Northern District of California. The indictment charges Harper with six violations of Title 18, U.S. Code, (1) conspiring to deliver National Defense information to aid a foreign government, (2) unlawfully obtaining National Defense information, (3) unlawful retention of National Defense information, (4) delivery of National Defense information, (5) income tax evasion, and (6) making a false income tax return. Beginning on page 10 of the indictment (Attachment 5), the classified material obtained by Harper and Schuler from SCI and reproduced is listed. A total of 61 classified documents are identified. However, a review of facility document control records reflects that the document listed on line 18, page 14 of the indictment (Attachment 5) titled, "Clarification/Questions and Answers for Contract RFQDASGO-80-Q-0225", is in actuality an enclosure to the document listed on line 10 of page 13 of the indictment (Attachment 5). This document is fully identified in Attachment 6, Classified Document Accountability Record (DA Form 3964) on file in SCT and in the Document Control Card numbered 80-248 in Attachment 8.

(4) Attachment 7 is a copy of each of the control cards fully identifying documents which were reproduced by Schuler and Harper, the copies having been subsequently turned over to the agents of the Polish People's Republic and the Union of Soviet Socialist Republics. The documents listed in Attachment 7 are listed on pages 15, 16, 17 and 18 of the indictment (Attachment 5). Interviews with Special Agent Power and the prosecuting assistant, U.S. Attorney John C. Gibbons, who are handling the Harper case, reveal that Power and Gibbons are reasonably sure that Harper was being truthful when he stated that the documents identified in Attachment 5, pages 15, 16, 17 and 18, and fully identified in Attachment 7, are all of the documents Harper turned over to foreign agents.

(5) Attachment 8 contains a compendium of classified Document Control Cards obtained from the facility which fully identifies the documents listed in pages 19, 20 and 21 of the indictment (Attachment 5) that were recovered from Harper by the Federal Bureau of Investigation. Interviews with Special Agent Power and Assistant U.S. Attorney Gibbons reveal that they are reasonably sure that this is all of the material reproduced by Harper and Schuler but not turned over to foreign agents.

(6) During the course of examining SCT Classified Document Control records, efforts were made to further identify the document listed on line 15, page 14 of the indictment (Attachment 5), "Proceedings of 1981 Western Regional Technical Symposium", classified Secret. A Document Control Card for document 81-001, received at the facility on 5 January 1981, bears the only

title similar to that listed in the indictment. Facility still had their copy of this document. The date of the document and the title indicates that it may not be the same. However, it is possible the person making up this list for the indictment did not accurately record the actual date and title. Because the copy in the possession of the U.S. Attorney is in evidence, no effort was made by this office to make a comparison. The Federal Bureau of Investigation was notified and the facility was requested to secure the document pending pick up by an agent of the FBI. This is an unresolved question, but is documented because until it is resolved, this is a document in a field of interest not associated with other documents taken by Schuler and Harper. Attachment 9 is a copy of the control card for document 81-001, possibly the same document listed in line 15, page 14 of the indictment (Attachment 5).

(7) Attachment 10 is a compendium of documents identified during the inquiry as material previously in possession of Robert Larson and William Anton which was subsequently destroyed. According to Mr. Anton, the listed documents would have been in Larson's and Anton's possession and that Schuler would also have had access to them. The documents identified under Control Number 80-234 through 80-239, received 13 November 1980 by SCI, from BMD Systems Command (Attachment 11), appear to be as critical as other material and predates some of the material reproduced by Schuler and Harper. Further inquiry into this matter with the Federal Bureau of Investigation following Harper's trial scheduled for April 1984 should be pursued.

(8) Examination of reproduction records on file at SCT for the period 1977 through 1982 reflected that only two documents listed in the indictment (Attachment 5) had been officially reproduced by the company (SCT) for internal use. Records did not reflect Schuler as the requester or reproducer. The copies of these reproduction requests are contained in Attachment 12, documents are identified as 79-220 and 80-050. Examination of destruction certificates revealed that copy 1 of each document was properly documented on destruction certificates. Copy 2 of each document is in the possession of the Federal Bureau of Investigation/US Attorney as evidence. An interview with Debra Graham, nee Whitfield, identified as Whitfield in Attachment 12, revealed that she was in charge of classified reproduction both for SCI and SCT during the period covered by this inquiry. Graham remembered Schuler and believed that during the period Schuler may have delivered and picked up classified jobs from the reproduction section. However, she is not certain of this. Graham was not sure of any of her comments regarding her work activities and appeared frightened. She also appeared to be telling the truth. When advised that Schuler's name did not appear on any of the reproduction requests on file, Graham stated that she does not recall Schuler ever asking her to reproduce anything, either officially or unofficially. She stated that she would only do reproduction based on a reproduction request signed off by classified document control personnel. Graham reiterated that Schuler could have picked up classified material for someone else in her (Schuler's) work area. Interview with Special Agent Power revealed that he is reasonably sure that classified material reproduced by Schuler and Harper was not accomplished on the premises of SCI but that it was done on a reproduction machine purchased by Harper for that purpose.

(10) Special Agent Power and Assistant U.S. Attorney Gibbons both related during interviews that Harper and Schuler kept good records of the classified material they reproduced and that Harper was very cooperative in telling them where and when Harper transferred material to foreign agents and where to locate the material Harper had in his possession. The FBI checked all unclassified material taken from SCI that Harper had in his possession and found no material marked as classified. The FBI requested assistance of cleared, knowledgeable personnel of SCT to assist in the examination. Mr. Kenneth Kessler, SCI employee, assisted in the unclassified review and stated during interview that the unclassified material was of little if any value to foreign agents.

3. Conclusions:

a. A thorough inspection of SCT was conducted during the period 14-20 December 1983. Most of the procedures in effect regarding control of classified material, destruction of the material, and other related activities were the same as those followed by SCI during the period of interest of the inquiry. Control of access to the facility during nonworking hours by employees was nonexistent. Any employee could enter the facility at night or weekends and holidays and bring visitors with them. While a security weakness, there is nothing in current regulations or requirements to cover this area. According to Special Agent Power, Schuler, among other employees, was observed in the facility on weekends and holidays. On at least one occasion Harper was observed in the facility in the company of Schuler. None of the deficiencies observed during the inspection or noted in the previous inspections contributed to the compromise of classified material noted herein. A compliance inspection of the SCT was conducted on January 25, 1984. Corrective action by the facility is adequate.

b. According to information developed by the FBI and agreed to by the U.S. Attorney, Schuler removed classified material from SCI clandestinely; she and Harper reproduced the material outside the facility and returned the originals to SCI clandestinely.

c. There is nothing in the current Industrial Security Program to preclude a cleared person, in possession of classified material or with knowledge to the combination of a classified material storage container, from removing the material clandestinely, reproduce it, and return the originals to the place from which removed undetected. Purses, briefcases, and other containers are not searched as a rule. Even if such searches took place, a person so inclined could still remove documents from a facility on their person.

d. Cleared facility personnel apprised the FBI, as well as their office, that Schuler was known as a heavy drinker. None considered her an "alcoholic" until they became aware of her illness in 1982 which led to her surgery and death. Had an adverse information report been filed in accordance with paragraph 6b(1) of the Industrial Security Manual, there is an extremely remote possibility a subsequent investigation might have revealed Schuler's and Harper's espionage activities.

e. It is concluded that the classified information identified in Attachments 5, 6, 7, 8, 9 and 11 have been compromised and classified information identified in Attachment 10 is presumed to be compromised. Classified material listed in Attachment 7 was turned over to foreign agents. Notwithstanding the cooperation of Harper with the FBI and U.S. Attorney's office, it cannot be factually determined that the information identified in Attachments 8, 9 and 10 as well as other information was not, in fact, turned over to other unauthorized persons, for example, William Bell Hugle, identified in Attachment 1, or his associates.

4. Corrective Action:

a. Schuler is deceased - no further action can be taken in her case.

b. Harper is in custody and will be tried under various sections of Title 18 of the U.S. Code.

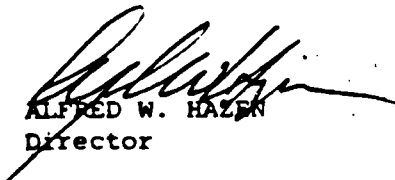
c. Management of SCT is fully aware of the impact of this case regarding the National Security. The security inspection completed 20 December 1983 highlighted security weaknesses of their security program and corrective action has been taken. It was recommended that the action be taken to centralize all classified material into one location under the control of the security officer. It was also recommended that the facility also develop better personnel access controls for weekends, holidays and after hour periods.

5. It is recommended that:

a. This be considered an interim report and that further interviews and material examinations will take place by this office as soon as we are certain that such activity will not interfere with the orderly prosecution of Harper. Additional inquiry will include inquiries based on information now in the court's evidence file, results of the Grand Jury testimony that can be obtained and interviews of key witnesses not interviewed during the inquiry for reasons previously cited.

b. Ballistic Missile Defense Systems Command be provided with a listing of material identified in Attachments 7, 8 and 9 with a summary of this inquiry.

c. The U.S. Air Force Electronic Systems Division, Hanscom Air Force Base, Massachusetts 01730, be advised that classified documents identified as 79-212 in Attachment 8 has been compromised; and that classified document 78-061 in Attachment 10 is presumed to have been compromised. These two documents were generated under Air Force Contract F 19628-78-C9992 by Lincoln Laboratories/MIT, P.O. Box 73, Lexington, Massachusetts 02171.


ALFRED W. HAZEN
Director

12 Attachments
(Listed on following page)

ATTACHMENTS NOT INCLUDED

12 Attachments

1. Criminal Complaint (Oct 14, 83)
2. U.S. Attorney's Ltr (Nov 8, 83)
3. DD Form 374 (Jul 20, 83)
4. DISCO Record (Ruby L. Harper)
5. Indictment (Dec 9, 83)
6. DA Form 3964 (Dec 5, 80)
7. Document Records (Passed to Poles)
8. Document Records (Recovered)
9. Document Control Record (81-001)
10. Document Records (Possibly Compromised)
11. DA Form 3964 (Oct 31, 81)
12. Reproduction Records (77-220/80-050)



DEFENSE INVESTIGATIVE SERVICE

OFFICE OF THE REGIONAL DIRECTOR
BUILDING 35 ROOM 114
PRESIDIO OF SAN FRANCISCO, CA 94129

SAN FRANCISCO REGION (V5200)

May 31, 1984

IN REPLY
REFER TO

SUBJECT: Administrative Inquiry - Systems Control, Inc., (SCI),
1801 Page Mill Road, Palo Alto, California 95650

1. Authority for conducting a supplemental inquiry is contained in report dated January 30, 1984, subject as above. This report contains supplemental information developed subsequent to completion of the January 30, 1984 report.

2. Essential Facts:

a. Attachment 1 is an unsigned copy of a Personnel Security Questionnaire (DD Form 48) dated July 1, 1961 regarding James Durward Harper, Jr., identified in the previous report. The form reflects that he was employed by several firms currently cleared under the Defense Industrial Security Program and believed to have been cleared in the past. The firms known to be currently cleared and cleared during the time Harper reflects he was employed by them were contacted to determine if they by chance had a formal record of clearance for Harper. The following results were obtained:

(1) Aerojet General Corporation (Aerojet Gen Eng Corp), employment 3/55 to 11/55. A source checked available records for all Aerojet General facilities in the Azusa and California area and could find no record of Harper.

(2) Lenkurt Electric Co., later known as GTE Lenkurt, San Carlos, California. Employment 12/55 to 6/57. Regional files reflect this firm closed its operation November 27, 1983 and transmitted all files to GTE Network Systems (Automatic Electric, Inc., 400 North Wolf Road, North Lake, Illinois 60164).

(3) Federal Electric Corp., Anchorage, Alaska. Employment 7/57 to 7/58. Mr. Frank Addonizio, Manager, Security and Safety, Federal Electric Corporation, 621 Industrial Avenue, Paramus, New Jersey 07652 states that his company has an old employee card containing the following information:

(a) James Durward Harper, SSN 570-43-3474

(b) Address: Box 714, Belmont, California
Forwarding Address: 323 Woodrow St., Daly City, California

(c) Dates of Employment: 18 July 1957 to 9 June 1958

(d) Reason for Leaving: Resigned because of difficulty in adapting to isolated living conditions. Card is annotated further: "Reemployment not recommended".

(e) Clearance: Cleared Interim Secret 28 August 1957
Cleared Final Secret 29 October 1957

(f) Attended high school in California and junior college
in San Mateo, California

(g) Classified as: Technical Aid

(h) Work Place: Anchorage, Alaska

(i) In another section of the PSQ Harper reflected he was
cleared by the U.S. Air Force for work on "White Alice" sites in Anchorage,
Alaska. No dates were given but it is believed this is the same as the
employment by Federal Electric in Alaska.

(4) Osborne Electronics Company, 712 Hawthorne, Portland, Oregon.
Employment 7/60 to present (1961). It was established that the company is
now known as OECO, Inc. Region files reflect that the company was initially
cleared circa 1952. In 1962, as OECO, Inc. it was cleared to the level of
Secret. A check with the Security Officer of the company, Jarold A. Krafve,
revealed that the company could not locate records pertaining to Harper or
a clearance record reflecting that he was cleared. There are personnel
working for the company who remember Harper and confirmed that he worked
there. Their recollection was triggered by newspaper articles concerning
Harper and Ruby Louise Harper (Schuler). Further inquiry was not considered
worthwhile.

b. Records of the California State Department of Motor Vehicles reflect
that Ruby Louise Schuler, identified in the previous report, was arrested
August 16, 1979 in Cupertino, California for violation of Section 23102, DVC
(Driving While Intoxicated). She was convicted for the violation, Sunnyvale
Judicial District Court, Santa Clara, California, Docket Number E 79004,
Court Number 43477, sentence not reflected indicating no time served in jail.

c. Personnel of Systems Control Technology, Inc., (SCT) at the request
of this office, examined control cards, records of receipt, actual documents
existant and other records in an effort to establish if any of the classified
material listed in the previous report was identified with any contract
number and/or user agencies not identified in the previous report. The
company reported that they made an exhaustive search but could not identify
any additional contract numbers or agencies. This tends to confirm a
similar search made earlier by personnel of this office.

d. Special Agent Powers, Federal Bureau of Investigation, compared the
copy of the document in the courts possession with the one described in
Attachment 9 of the previous report, Attachment 2 of this report, which is
in possession of the facility and determined that the documents are
different in dates and content and are not the same.

e. Attachment 3 is a copy of a resume prepared by James D. Harper and
submitted to various contractors in the San Francisco Bay Area just prior
to his arrest on espionage charges in October 1983. The resume updates his

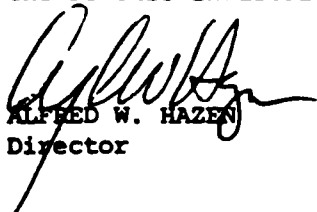
alleged employment with that listed in Attachment 1. Attachment 4 is the results of our local checks in an effort to establish clearance information regarding Harper.

f. On Monday, May 14, 1984, a Federal Judge of the U.S. District Court sentenced Harper to life in prison with a recommendation that he not be paroled. The U.S. Attorney, San Francisco and the Federal Bureau of Investigation continue to pursue the case against Huggle, et al.

3. Recommendation: It is recommended that:

a. The proponent agency for the document identified in Attachment 2 hereto be advised that instant document is not the same as the one found in Harper's possession.

b. In the absence of any further new involvement with subject company, Systems Control Technology, Inc., Harper or other persons involved with the Defense Industrial Security Program, this case is considered closed.


ALFRED W. HAZEN
Director

4 Attachments

1. Personnel Security Questionnaire
2. Document Control Record (81-001)
3. James D. Harper Resume
4. Results of Checks of Facilities
Identified in Atch 3 for Security
Clearances of Harper

Appendix VII
Committee Questionnaire to DIS Personnel



POLICY

OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

2 8 FEB 1984

Dear Security Professional:

As a professional employee of DIS with Defense Industrial Security Program (DISP) related responsibility, your assistance is needed to enhance the depth and scope of an on-going review of the DISP.

By way of background, in October of last year, General Richard G. Stilwell, USA (Ret.), the Deputy Under Secretary of Defense for Policy, established a committee to analyze the effectiveness of current industrial security policies, practices and procedures and to develop recommendations for program improvement. The committee has been formally designated as the DoD Industrial Security Review Committee and is directly responsible to General Stilwell in fulfillment of its charge. The need to establish the committee resulted from areas of known and suspected program weaknesses and from several recent cases of espionage involving cleared industrial personnel working with various hostile foreign intelligence service representatives.

As a participant in the program, you can appreciate fully the importance of the review and its potential for enhancing the overall effectiveness of the DISP. Accordingly, General Stilwell considers committee business to be of the highest priority. This effort has also attracted substantial Congressional interest.

The committee is comprised of representatives of the Office of the Deputy Under Secretary of Defense (Policy), the Office of the General Counsel, DoD, the Office of the Inspector General, DoD, and the Defense Investigative Service. The committee has already conducted extensive interviews with representatives of selected DoD and non DoD activities at various locations throughout the country. As a person with direct involvement in making the system work as efficiently and effectively as possible, the committee considers your individual contribution vital to the success of this endeavor.

In this connection, we have developed a questionnaire (attached) to assist us with soliciting and analyzing certain information determined pertinent to our review. In most instances, the questionnaire provides for both checklist and narrative type responses, the latter of which enables you to explain the basis of your multiple choice selection. Your narrative response is, therefore, of significantly greater importance to the committee than your multiple choice response. We encourage you to take the additional time required to furnish us with the more meaningful information.

To reduce our administrative burden we ask that the senior official in each office be responsible for the reproduction of this letter along with the required number of questionnaires for distribution to intended recipients. It is absolutely essential that ample time be set aside to complete the questionnaire, that it be accomplished in private, and that you return it anonymously in a DoD franked envelope to the following address:

Mr. Daniel R. Foley
Deputy Assistant Inspector General
Department of Defense
Suite No. 431
1600 Wilson Blvd
Arlington, Virginia 22209

The ultimate success or failure of our review effort relies heavily on the individual contribution of persons such as yourself. We urge you to seize upon this unique opportunity to be heard free of bureaucratic entanglement. We eagerly await your comments on this most important matter. We have every reason to believe that your contribution will serve as a principal catalyst in the formulation of meaningful recommendations to bring about near-term program improvement. We would appreciate receipt of the completed questionnaire by March 30, 1984.

Sincerely,


Dan Foley
Co-Chairman


John Hancock
Co-Chairman

Enclosures

INDUSTRIAL SECURITY PROGRAM REVIEW COMMITTEE

SUMMARY OF RESPONSES TO QUESTIONNAIRE

<u># of</u> <u>Resp.</u>	<u>%</u>		1. My present position is:
69	40.8	___	IS Rep (any grade)
20	11.8	___	Field Office Chief
35	20.7	___	Regional HQ Professional Staff
6	3.6	___	DOSI/Regional Director
6	3.6	___	DSI Professional Staff
27	16.0	___	DISCO Professional Staff
1	.6	___	OISI Professional Staff
5	2.9	___	DIS HQ Professional Staff
<u>1</u>	<u>-</u>		Not indicated
170	100%		

2. My educational attainment to date:

14	8.3	___	High school or equivalent
42	25.0	___	Some college
22	13.1	___	Community college degree (2 year curriculum)
63	37.5	___	Bachelors degree
25	14.9	___	Masters degree
2	1.2	___	Doctorate
<u>2</u>	<u>-</u>		No Response
170	100%		

<u># of</u> <u>Resp.</u>	<u>%</u>		3. Years of direct experience in the Defense Industrial Security Program (DISP).
26	15.5	___	Less than 2
35	20.8	___	2-4
26	15.5	___	5-7
19	11.3	___	8-10
27	16.1	___	11-15
35	20.8	___	16 or more
<u>2</u>	<u>-</u>		No Response
170	100%		

<u># of</u> <u>Resp.</u>	<u>%</u>		4. I consider the overall effectiveness of the Defense Investigative Service (DIS) industrial security inspections to be:
52	31.5	___	Significantly effective
76	46.1	___	Moderately effective
18	10.9	___	Marginally effective
19	11.5	___	Don't know
<u>5</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

With respect to the overall effectiveness of the DIS inspection program, the comments reflected a consensus that the program is effective. The opinions on the degree of effectiveness varied with the experience of the inspector and the attitude and training of defense contractor personnel. The presence of IS representatives has the impact of alerting the corporate management to security problems. To be effective, the IS representative must approach the inspection as a challenge and question the employees. Some comments did reflect concern that the representative did not have sufficient authority to take action when major violations were observed. An inexperienced IS representative workforce creates problems in running an effective inspection program and conducting in-depth inspections. Some of the comments cited the reluctance to suspend or revoke clearances and the emphasis on administrative inspections. It was suggested that additional training should be provided to IS representatives. Unannounced inspections were referred to in some comments as a positive change.

of
Resp. % 5. I rate my Agency's ability to attract and recruit
qualified people:

12	7.4	_____	Extremely high
73	45.1	_____	Fully satisfactory
65	40.1	_____	Extremely low
12	7.4	_____	No opinion
<u>8</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

Comments indicated that DIS has taken steps to improve recruitment of qualified personnel and to implement a program of upward mobility. Most respondents cited a need to continue an upward mobility program to retain "motivated" people. A consistent theme of the comments was frustration regarding the length of time it takes to hire an individual. Some comments expressed concern that qualified individuals with experience were being passed over for individuals with college degrees but no experience. Numerous individuals complained about low salaries for entry level positions in high cost areas and the high turnover rate because of higher salaries with industry.

of
Resp. % 6. Confidence in receiving DIS management support of
my professional decisions and recommendations is
considered:

44	26.7	_____	Extremely high confidence (at the Region level)
94	56.9	_____	Usually confident
27	16.4	_____	Extremely low confidence
<u>5</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

The respondents generally believed that IS representatives received support for the decisions made. While this view was repeatedly expressed at the field office level there were mixed views on the confidence question the further down the respondent was in the DIS chain of command.

# of Resp.	%		7. My agreement with DIS HQ or higher authority decisions:
---------------	---	--	---

8	4.9	_____	Always agree
140	85.3	_____	Usually agree
16	9.8	_____	Usually disagree
-	-	_____	Never agree
6	-		No Response
<u>170</u>	<u>100%</u>		

Summary of respondents' comments:

Most of the respondents generally agreed with decisions made at the headquarters level. Some of the respondents did point out, however, that it is difficult for individuals in the field to attempt to second guess certain decisions since they do not have all the facts.

# of Resp.	%		8. I rate my formal (Defense Security Institute) DISP training as:
---------------	---	--	---

38	23.0	_____	Excellent
68	41.3	_____	Fully Sufficient
36	21.8	_____	Less than sufficient
1	0.6	_____	Unsatisfactory
22	13.3	_____	Have not attended the Defense Security Institute
5	-		No Response
<u>170</u>	<u>100%</u>		

Summary of respondents' comments:

The training program at DSI generally received sufficient ratings. Additional training was needed in ADP security and the "real world" situation that an inspector confronts in a contractor facility. Advanced courses were suggested for individuals who do have experience.

of
Resp. % **9. DIS relationship with military departments and user agencies appears to be:**

21	12.6	_____	Excellent
75	44.9	_____	Cordial
13	7.8	_____	Adversarial
8	4.8	_____	Misdirected
5	2.9	_____	Poor
27	16.2	_____	Don't know
18	10.8	_____	Other (please specify)
<u>3</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

The comments on the relationship with user agencies, including the military services were mixed. Some comments described the relationship as basically cordial and professional and others called it adversarial.

of
Resp. % **10. Overall effectiveness of Industrial Security Program in detecting and preventing the compromise of classified information:**

71	42.0	_____	Significant
58	34.3	_____	Marginal
9	5.3	_____	No appreciable impact
31	18.4	_____	Don't know
<u>1</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

The DISP in many of the comments is considered to be effective in training individuals but not necessarily stopping all compromises of classified information. Ultimately the human reliability element plays a very important role in any security program. Some compromises would simply be impossible to detect.

# of Resp.	%	
		11. My perception of higher HQ's emphasis and direction regarding inspections is toward enhanced:

22	13.0	_____ Quality
30	17.8	_____ Quantity
84	49.7	_____ Quality & quantity
5	2.9	_____ Unaware of any particular emphasis
17	10.1	_____ No opinion
11	6.5	_____ Other (please specify)
<u>1</u>	<u>-</u>	No Response
170	100%	

Summary of respondents' comments:

Most of the respondents stated that great emphasis was placed on the quality and quantity of inspections. Some individuals stated that the program had to meet certain goals in order to handle the volume of requests.

# of Resp.	%	
		12. The length of my formal on-the-job training was:

7	4.3	_____ Too long
107	65.2	_____ About right
34	20.7	_____ Too short
16	9.8	_____ No opinion
<u>6</u>	<u>-</u>	No Response
170	100%	

Summary of respondents' comments:

Most of the respondents who provided a narrative comment on this question believed that formal, on-the-job training (OJT) was essential to the proper development of an industrial security professional. A prevalent statement among those making positive comments on their OJT was that they have seen marked improvements in this area over the past several years. There was a lack of consensus, however, on what constitutes an optimum amount of OJT, with opinions ranging from several months to two years. A significant number of individuals

stated that they regard OJT as a continuous process and no matter how many years of experience they may have, they are still learning.

Many of the negative comments seemed to reflect particular problems or shortcomings in individual offices or with specific supervisors. The most common reasons offered by the respondents for being dissatisfied with their OJT was that, due to a high turnover of personnel, either the individuals providing the OJT were inexperienced themselves or an untrained individual was pressed into assuming an immediate workload because of a backlog.

<u># of</u> <u>Resp.</u>	<u>%</u>	
		13. As a general rule, I consider the technical expertise and program knowledge of contractor industrial security personnel to be:
5	3.2	_____ Outstanding
74	47.7	_____ Fully adequate
65	42.0	_____ Less than adequate
4	2.6	_____ Unsatisfactory
7	4.5	_____ No opinion
<u>15</u>	<u>-</u>	_____ No Response
170	100%	

Summary of respondents' comments:

The majority of the respondents differentiated between contractors with large security programs and those with small ones. They respected the expertise and program knowledge of personnel who represented large contractors and who could genuinely be referred to as full-time security professionals. They were dissatisfied with the representatives of the smaller firms, who had more responsibilities than just security. Most of the respondents felt that these individuals either did not have enough time to devote to security or they were not at an appropriately responsible level within the company and thus had no authority. There were numerous comments that attributed improvements in the area of contractor knowledge and expertise to the education and training effort of DIS, especially the courses offered by the Defense Security Institute.

# of Resp.	%	
62	40.5	_____ No
91	59.5	_____ Yes
<u>17</u>	<u>-</u>	No Response
170	100%	

Summary of respondents' comments:

Most of the comments acknowledging counterproductive aspects of the DISP centered around the utilization of resources. With so much to do, there appeared to be a consensus that attention to priorities was poor. The most frequently cited example was the requirement to periodically inspect selected uncleared locations where cleared personnel are employed or physically located. Many respondents questioned the value of spending so much time on such efforts, especially when the apparent returns are minimal. Related comments questioned the wisdom of inspecting access elsewhere and dormant facilities every nine months. Many respondents regarded this as an "overkill". Another frequent comment on the counterproductive aspects of the DISP addressed the subject of Standard Practice Procedures. All the comments seriously questioned their value, especially at small facilities. The following comment sums up many of the sentiments expressed: "A burdensome task that yields few or no benefits. The employees don't read them, they ask the security people. The security people don't read them, they read the ISM or call us. Also, the time spent reading and writing are completely disproportionate to its importance." Other examples which were cited as being counterproductive included unannounced inspections, OPSEC, Carve-outs and contractor granted Confidential clearances.

# of Resp.	%	
134	78.8	_____ Agree
5	3.0	_____ Disagree
<u>31</u>	<u>18.2</u>	_____ Don't know
170	100%	

15. It has been suggested that one of the more serious problems in the DISP is the reluctance of the Directorate of Industrial Security Clearance Review (DISCR) to deny or revoke a personnel security clearance in instances when any reasonable person could be expected to conclude that issuance or continuance would not be clearly consistent with the national interest.

Summary of respondents' comments:

Respondents consistently expressed dissatisfaction with the DISCR. Representative sample comments include: "DISCR appears to be more concerned with the technicalities of whether or not they can defend a clearance denial decision if it is appealed, as opposed to the judicious use of common sense in order to protect the national interest;" and "I felt that DISCR places too much emphasis on legal sufficiency in cases referred by DISCO"; as well as "DISCR decisions are obviously based on the legal viewpoint of the case, as opposed to the national security viewpoint." Some respondents defended DISCR. Most of these stated that you could not measure DISCR's effectiveness strictly by the number of clearances denied or revoked. Several comments attributed the inability to deny or revoke clearances to the superficiality of the personnel security investigation conducted.

<u># of</u> <u>Resp.</u>	<u>%</u>		16. Individual initiative and flexibility in conducting security inspections and other aspects of the DISP are:
84	53.2	_____	Encouraged
19	12.0	_____	Discouraged
55	34.8	_____	Not specifically encouraged or discouraged
<u>12</u> <u>170</u>	<u>-</u> <u>100%</u>		No Response

Summary of respondents' comments:

Most of the respondents to the question were favorable in their comments. Many referred to the desire to achieve quality inspections and recognized that this cannot be accomplished in "cookie-cutter fashion." The over-riding sentiment can be summed up in this quote: "Individual flexibility is encouraged within the framework of the standard policy guidance. The main objective is for consistency in inspection criteria." The prevailing theme of the negative comments was the perception that quantity took precedence over quality and that a check-list approach to conducting inspections was emphasized.

<u># of Resp.</u>	<u>%</u>		17. I consider the technical (program) knowledge of my immediate supervisor to be:
102	61.1	_____	Excellent
41	24.6	_____	Good
14	8.3	_____	Average
9	5.4	_____	Poor
1	0.6	_____	Unsatisfactory
<u>3</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

The overwhelming majority of the respondents felt the technical knowledge of their supervisors to be good to excellent. "The most competent individual in the program I have met" and "My boss is a professional -all the way" are representative of the of positive comments. Most of the negative comments appeared to deal with the supervisor's management style as opposed to his or her technical expertise. Some of the negative aspects cited were that the supervisor "sees everything as black or white," or "lacks common sense" or "flexibility." Some respondents believed that the supervisor did not keep up with changes and was not current in his or her technical knowledge.

<u># of Resp.</u>	<u>%</u>		18. Contractors who demonstrate an inability or unwillingness to properly administer or comply with Industrial Security Program requirements and obligations are justly dealt with.
67	40.4	_____	Agree
73	43.9	_____	Disagree
26	15.7	_____	Don't know
<u>4</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

The consensus among those individuals providing positive narrative comments to this question was that a tremendous improvement has

recently been seen in this area. "Unfortunately, this was not the case a few years ago". The overriding theme throughout the negative comments is that there is perceived to be a double standard for large and small defense contractors. "If they are medium or small size, they are (justly dealt with). The giants get away with too much" was typical of the many comments made along this line. Politics was perceived by many to be the decisive factor in how any particular contractor was dealt with. Many of the respondents, however, attributed these politics not only to DIS, but to the User Agencies as well.

of
Resp. %

19. On a numerical scale, please rank the following security disciplines in accordance with your relative expertise in each (no. 1 being your strongest area of expertise, no. 2 your second strongest area of expertise, etc.):

<u>RANKING</u>	1	2	3	4	5	6	7	8	9	NR
___ International programs	8	10	13	10	2	19	24	55	4	25
___ FOCI	8	13	9	18	23	24	36	11	2	26
___ ADP	11	16	21	15	24	18	11	29	3	22
___ Personnel security	73	35	25	7	11	2	2	2	-	13
___ Physical security	34	43	26	19	10	9	8	2	1	18
___ COMSEC	8	8	11	22	22	30	32	9	2	26
___ Information security	44	29	29	15	15	8	8	4	-	18
___ Classification management	12	18	15	31	22	20	9	16	3	24
___ Other (please specify)	8	7	2	2	2	-	-	-	4	145

Summary of respondents' comments:

By far, the majority of the comments reflected the obvious; i.e. the more you are exposed to a given area, the most expertise you will develop. The common theme in the narrative comments, however, addressed the issue of training. Many individuals felt they should be experts in all areas, yet also felt that they were not provided adequate training in those areas where they received limited exposure. International and COMSEC were the disciplines given as the most common examples.

# of Resp.	%	20. DIS personnel promotional policies and practices are considered:
14	8.3	_____ Outstanding
70	41.4	_____ Fully satisfactory
67	39.6	_____ Poor
18	10.7	_____ Don't know
<u>1</u>	<u>-</u>	No Response
170	100%	

Summary of respondents' comments:

The respondents generally complimented the promotional opportunities within DIS, but questioned the agency's promotional policies and practices. The respondents also expressed general dissatisfaction with many of the promotions to higher level positions, especially those involving supervisory positions in the field. One respondent commented "opportunities for promotion are excellent. If anything, people are moved too quickly and sometimes placed in staff positions (at Region and Headquarters) too soon and with little or no field experience." Another respondent stated that the foregoing problem was most prominent in the Washington, D.C. and Los Angeles areas, where the high cost of living and opportunity for industry jobs have a significantly greater impact. Several respondents complained about the excessive length of time needed to fill positions, disagreed with the degree of emphasis on a college education, and expressed concern with prejudicial factors entering into the selection process. Examples included "it takes too long for Division to approve promotions, which should have been made at Region level. Disagree with need for college degree." "Most promotions are written to fit a particular person, not a wide spectrum of all employees." "Getting trainees on board is still too slow. The DIS must anticipate needs. It takes nine months to a year before we can use a trainee." "Outsiders, lacking experience, are given promotions over deserving employees." "When a person can serve 17 years as a GS-4 and have been a very effective worker but not receive a promotion there is something wrong (DISCO)." "I have seen personnel promoted to positions for which they were not fully qualified nor had sufficient field experience." "At least from the Industrial Security side, it is common knowledge that there is much favoritism and manipulation in the promotion process. The usual promotion practices and hiring practices are subverted so that outsiders are hired and promoted ahead of longtime employees." "Too much emphasis on who you know and whether you are willing to move." "While its a common complaint everywhere, I have never seen an organization base its placement and promotion decisions on politics more than DIS. The selection process is too

centralized and managed from too high up." "It was dictatorial prior to the (appointment) of the current Director of DIS. Higher grade selection is still somewhat too rigorously controlled." "There is nothing resembling a merit promotion program in this agency. Every personnel action, be it promotion or lateral assignment, is subjective. Employees are completely at the mercy of a select few at the headquarters level. The practice of 'blackballing' is common throughout the program and at all levels." "In a number of instances, 'games' have been played in order to select and promote specific individuals. One individual under my direct supervision was promoted without my full knowledge, understanding and concurrence."

<u># of</u> <u>Resp.</u>	<u>%</u>	21. From my perspective, the DISP is administered and managed:
14	8.3	_____ Exceptionally well
76	45.0	_____ Reasonably well
34	20.1	_____ In a fully satisfactory manner
31	18.3	_____ Somewhat poorly
4	2.4	_____ Exceptionally poorly
10	5.9	_____ Don't know
<u>1</u> 170	<u>-</u> 100%	No Response

Summary of respondents' comments:

Representative responses included the following comments: "In all fairness, it is a tremendous job. From the Director of DIS down to the lowest grade employee, it takes dedication and teamwork." "If the Postal Department could do as much with as little we'd still be buying nickel postage stamps. Quality of management is probably the biggest overall improvement in DIS in recent years." "I have seen an appreciable upgrading of the program since leaving DLA." "Program manager concept works well. Claims of micromanagement have some merit, but leadership seems open-minded and receptive to field views." "There is room for improvement in the administration of the DISP. However, my perception is that the DISP is administered and managed with a reasonable degree of efficiency." "Reasonably well and improving. Mr. O'Brien is a very capable and progressive administrator." "Under Mr. O'Brien everybody does seem to try harder." "I have worked in several User Agencies during my career; and from my experience, I appreciate, maybe more than others, how well DIS is managed." "Emphasis in DIS is on form not substance -larger contractors are OK; smaller ones vary widely. Workload prevents us from spending enough time at facilities to ensure the DISP's success."

"In DIS it appears the investigative side is given preferential treatment over the industrial side." "The program has little power over uncooperative companies. Too much concern with quantity rather than quality. Too few dollars to adequately accomplish DIS mission." "There does not seem to be a true concern for the individual. Poor working conditions and insufficient resources are all I have seen since joining the DISP in November of 1981. Decision makers are too easily influenced by higher authority or people in high places to do things that are contrary to the DISP standards." "Exceptionally poor. The program is running despite management. DIS is oriented toward AIA, ASIS, NCMS, and CODSIA -also, Pentagon Corner articles which are prepared by the HQ staff along with the speeches that top management presents. The organization exists at the pleasure of and to make TJO'B look good." "DIS tends to over manage." "There are too many policy and procedure variances from Region to Region." "Overall program management is a shambles. Control is far too centralized, with Regions exerting little influence in the program direction. Furthermore, those making the decisions are neither competent nor honest. This is the crux of the low morale which exists at all levels, including the Headquarters." "We flit from one crises to another. Direction from HQ DIS is erratic and frequently contradictory. People who have no idea of what the program is about are sitting in judgement on field actions and making decisions that have far reaching impact. Tons of data gets collected at HQ, but no one knows how to analyze it. We survive in spite of it."

# of Resp.	%	
		22. My immediate supervisor attempts to exert undue influence on me to alter my position on actions assigned to me for my independent judgement and analysis, e.g., DD Form 696 inspection results; administration inquiry findings, adjudicative determinations, etc.

7	4.5	_____ Frequently occurs
26	16.7	_____ Sometimes occurs
107	68.5	_____ Never occurs
16	10.3	_____ No opinion
<u>14</u>	<u>-</u>	No Response
170	100%	

Summary of respondents' comments:

Positive comments outnumbered negative comments by a ratio of about 3 to 1. Representative examples included the following: "I personally feel my professional opinions and judgements are respected by my supervisor." "Discussions occur, but undue influence doesn't

exist." "The Regional Director and his staff have been very supportive of my findings and recommendations." "My current supervisor has enough expertise not to feel challenged or inadequate when told how I feel. My experience has been that supervisors will always challenge decisions based on information they have failed to acquire." "I get field support, not destructive criticism." "My immediate supervisor very seldom nonconcurs with my decisions. He permits independent judgement and analysis." "No such influence ever." "Any influence exerted would only be in a positive, enlightening and educational manner." "A change is requested only after a discussion of the matter and it is usually done with the concurrence of both parties." "Sometimes politics enter the picture. For example, too much attention is given to the number of deficiencies, unsatisfactory ratings, number of inspections, etc., in other Regions." "Honesty and frankness are never appreciated. I find most managers are afraid to be characterized as 'uncooperative' if they follow their own judgement instead of what they anticipate HQ expects. It is dulling to managerial initiative and the agency is paying dear price. The easy way out is the solution to most problems."

# of Resp.	%		23. Treatment and opportunities afforded Series 080 and Series 1810 personnel of DIS are considered relatively equal.
45	28.3	___	Agree
62	39.0	___	Disagree
52	32.7	___	Don't know
11	-		No Response
170	100%		

Summary of respondents' comments:

The consensus is that Series 1810 investigative personnel have an advantage over Series 080 personnel for promotional opportunities within the DIS. Typical comments were: "I am told that according to the civilian personnel manual, experience in 1810 is qualifying experience for 080 but the reverse is not true. This obviously gives 1810 personnel unequal advantage in lateral transfers and job opportunities in DIS." "1810 personnel are being assigned to DISCO but the reverse is practically nonexistent. It is a one sided program without merit." "It is all too evident that investigator personnel can just about call whatever shots that they want, and get them." "Having been on both sides of the house, I can see that Industrial Security is still considered the 'step child' in many instances. However, I do feel promotional opportunities are much greater in the 080 Series." "Most IS Reps feel 1810's are given preference for promotions to responsible HQ and Regional Director positions." "I have been an 1810 and 080 at DIS. I know they are not treated

equally. Investigative side is treated better. Cars are taken home or parked near home and most of higher management are promoted from the investigative side." "Responsibilities of 1810 personnel are less demanding and duties require less expertise and responsibility than 080 Series. As it is now Regional staff personnel positions are being filled by 1810 people with very little or no DISP experience. These people haven't even attended the basic Industrial Security course for IS Reps. The irony here is these inexperienced people receive GS-12 grades and have never conducted a 696 inspection or seen a closed area. You don't get this experience from reading regulations and manuals." "I think that there is a perceived feeling among DISCO GS-9 and GS-11 Series 080 that the Series 1810 personnel were brought to DISCO as GS-11 adjudicators. This limits promotional opportunities for a number of GS-080-9 personnel already in DISCO and there are some bitter people as a result." "It would appear that more publicity, recognition, and awards are given to the 1810 Series rather than the 080 Series.

of
Resp. % 24. In general, I consider Owner, Officer, Director,
Executive Personnel (OODEP) support and appreciation
of the Industrial Security Program to be:

15	9.2	_____	Extremely high
93	57.1	_____	Moderately high
29	17.8	_____	Moderately low
9	5.5	_____	Extremely low
17	10.4	_____	Don't know
<u>7</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

Representative examples of both positive and negative responses were: "Most OODEPS have an appreciation of our program." "Usually, the higher the OODEP, the more support and cooperation we get." "The exit briefing process with top management has been instrumental in getting support from OODEPS. There is still a need for total support and efforts are continuing within the DIS to get the maximum." "Support varies depending on facility involvement with classified contracts and dollar income versus unclassified contracts and dollar income." "Most management officials appreciate the importance of the program and give it good support." "Reception of recommendations, advice and assistance has been generally excellent. Recurring

inspections support that premise. Management support of its security personnel at our large facilities has been found to be outstanding." "The key is to get the attention of OODEPS. If you do that in the right way you have a supporter for life." "Most of the problems in the cleared facilities occur because the security personnel are not backed by management. Making money is the name of the game and security is overhead." "We are too often perceived as a necessary evil to be tolerated only to the least extent possible. Very few OODEPS embrace the 'partnership' concept." "Management is motivated by profit, not patriotism. Since no contractor was ever debarred for security violations, management support is not high. Of course, if you or I ask them, they'll tell you the opposite. But talk to an employee sometime - one who's been told to get the job out and security rules be damned." "Most average size companies consider security as a necessary evil, with the Security Officer wearing many, many other hats. Security is then usually placed as a low priority." "Varies, large facilities with large military contracts reflects high OODEP support; small facilities at times lacks total OODEP support."

# of Resp.	%		25. Industrial Security policies and procedures, as prescribed by the ISM and ISR, are generally sufficient to serve intended purpose.
---------------	---	--	--

126	75.4	___	Agree
32	19.2	___	Disagree
5	3.0	___	Don't know
4	2.4	___	No opinion
3	-		No Response
<u>170</u>	<u>100%</u>		

Summary of respondents' comments:

Responses regarding the adequacy of current policies and procedures were generally favorable. Representative comments were: "Realizing that there is no way to insure against compromise 100 percent, I think the requirements are adequate to prevent such occurrences - if followed." "Generally, guidelines are concise and describe fully action to be taken in each situation by the contractor." "We have a lot of good procedures and policies. If we can ever get them fully implemented (security education of people, both in industry and government) we would be in excellent shape." "The ISM and ISR are fairly detailed and explicit. It does seem to take a great deal of time to get changes made." "I think it is time for a complete new indexing and reorganization of both publications. I think that over the years we have added on to both publications. Perhaps it is now time to break the whole thing apart and rewrite them

with the customer in mind." "Adequate, yes, for the purpose of helping honest people meet our minimum requirements. It is a cost effective program for that. However, we need to do more if the program ever hopes to effectively curb espionage of the Boyce, Bell and Harper variety. The same is true if we expect to see the number of carve outs diminish or hope to have additional oversight responsibilities." "I agree, although from time to time one finds something in either the ISR or ISM that is incongruent and if time permitted should be written up for a decision. But with the work load as it is, one never has the time." "Simplify the ISM; clarify DIS mission. Empower your employees to implement your policy." "Too many policies are given verbally that are never addressed in the ISM/ISR." "Too much emphasis on administrative matters which do not contribute to protection of classified material." "Although there has been some recent progress in updating the publications much of the information in the manuals is not updated until long after it is obsolete. Some changes have taken several years to appear in the manuals. But an even greater deficiency is the large number of policy letters that are never incorporated into the manuals." "Don't worry if industry wants a requirement changed or eliminated -DIS will oblige." "Program is good if applied judiciously by well trained and experienced personnel. Due to shortage of personnel and inexperienced personnel, gaps occur in accomplishing the intended purpose."

of
Resp. % 26. The Industrial Security inspection frequency
(interval between inspections) is:

3	1.8	_____	Too frequent
97	58.8	_____	About right
40	24.2	_____	Too infrequent
25	15.2	_____	No opinion
5	-		No Response
170	100%		

Summary of respondents' comments:

In regard to adequacy of the existing inspection schedule, the comments were generally favorable. A representative sampling of the comments suggesting inspection scheduling changes follows: "Why should we inspect excluded parents. Except when considerable changes are noted, why not have a letter from the cognizant security office sent out on an annual basis?" "We know the level of expertise at our facilities and should be allowed flexibility in scheduling." "Believe a 'dormant' facility should be on an 18 month (close-out) cycle. An access elsewhere on a 12 month cycle. A category A thru O facility on a 9 month cycle. A Top Secret possessor on a 6 month cycle." "Facilities possessing Top Secret material should be inspected once

each 3 months." "Top Secret possession should be 3 months." "All others should be on a 6 month cycle." "About right, except that category A and B facilities may warrant, an increase, i.e., 4 months." "Too infrequent. A schedule which dictates a 6 month inspection for a facility with one person, one container and one Secret document, and a 9 month inspection for a facility with 100 people, 10 containers and 1000 Confidential documents may suggest some rethinking." "More frequent inspections are necessary in order to realize a significant impact." "The correct answer would probably be both too frequent and too infrequent. Too infrequent for more involved facilities, and too frequent for dormant, access elsewhere, and less involved facilities." "All inspections should either be on a 5 month or annual basis. Let's get rid of the 9 month interval." "We need to be more visible in those 5 percent of our cleared facilities that have 95 percent of all the classified material in industry." "Has anyone ever thought about inspecting a facility by involvement and track record as opposed to level of possession?" "Inspection frequencies should act as a guidance or reference point only. Most field personnel are aware that a number of their assigned facilities have excellent security officers/staff, and yearly inspection would be adequate; while other facilities should be inspected three or four times per year due to security postures or type of classified material in their possession."

of
Resp. %

27. Hostile intelligence threat information concerning cleared contractor facilities is to the best of my knowledge:

52	31.3	_____	Routinely made available (to DIS personnel)
66	39.8	_____	Sometimes made available (to DIS personnel)
20	12.0	_____	Never made available (to DIS personnel)
3	1.8	_____	Not sure what hostile intelligence threat information is
25	15.1	_____	Not in a position to know
4	-		No Response
<u>170</u>	<u>100%</u>		

Summary of respondents' comments:

Respondents furnished conflicting comments regarding receipt of threat information. Generally speaking, they indicated that threat data was now being furnished, that such information should be more readily available, or that such information is not now being furnished but should be. Representative examples of comments received are as follows: "I have been told that hostile threat information has been made available to DIS personnel but I have never been privy to such information." "DISCO receives briefings periodically from the FBI and

DIS HQ." "Security Awareness Bulletins are routinely provided." "Special classroom training has been provided." "Always receive latest information." "DSI does an excellent job in this regard." "At least weekly we receive some material in this area from our E&T specialist." "Should be routinely made available when such information is known." "The FBI has visited our cleared contractors and given their briefing on the hostile threat. Contractors receive the Security Awareness Bulletin from DSI, but newspaper articles that are repeated are not much help. Most people have already read the original articles." "We are constantly receiving newsletters and bulletins expressing the realities of hostile intelligence." "Specific hostile threat intelligence information on DISP facilities is never made known to DIS by FBI, DoD, etc." "Unless a system is formalized, we can't expect much more." "More emphasis is required on this subject. Hostile intelligence penetration should not be taken lightly and never assumed to be dormant." "We have received some information through the security awareness circulars; however, they are unclassified and therefore I consider them to be of limited value. The DIA has several publications, one of which is classified at the Secret level which could be made available to DISCO personnel. On the whole, we are poorly informed on the subject." "Never made available (to DIS personnel). Never saw it at my level." "Sometimes this information is too elaborate, wordy and redundant, without providing real insight to the threat. After all, the DISP is a passive counterintelligence program." "Only made available when specific espionage cases have received publicity." "I cannot remember, in my seven years, a threat estimate being given to me by DIS. "This is never disseminated to the field level. If only we received real intelligence briefings (as NIS and MI receive) we could emphasize the importance of the DISP to contractors." "There seems to be a lack of coordination between the intelligence community and DIS, i.e., reluctance to share what they have with me."

of
Resp. % 28. I consider the overall effectiveness of
contractor self-inspections to be:

14	8.6	_____	Significantly effective
83	50.6	_____	Marginally effective
33	20.1	_____	No appreciable effect
34	20.7	_____	Don't know
6	-		No Response
<u>170</u>	<u>100%</u>		

Summary of respondents' comments:

"The quality of self-inspections is suspect, but on occasion it does bring a situation to light sooner than waiting for the Gov. inspection." "Total waste of time." "The Government's 'good faith' in having contractors do a self inspection and not report any deficiencies lets them just tell us 'yes, we did it' and the date done." "We find too many deficiencies that should have been found by management." "Requirement is a paper tiger. No teeth." "I personally have not encountered a contractor who has admitted to a serious deficiency uncovered during a self-inspection." "Generally, the larger the facility, the more effective their program, especially large professionally staffed facilities. Self-inspections at these facilities are often times conducted better than the DISP inspections." "I doubt, in many instances, the contractor actually goes out and conducts a thorough 'hands-on' inspection. I wouldn't be surprised if some just go down the checklist (from their desks) and check off blocks."

<u># of</u> <u>Resp.</u>	<u>%</u>	
		29. Do you think too great an emphasis is currently placed on the administrative "checklist" approach to the conduct of industrial security inspections?
43	26.1	___ Yes
87	52.7	___ No
35	21.2	___ Don't know
5	-	No Response
<u>170</u>	<u>100%</u>	

Summary of respondents' comments:

"A checklist is a helpful tool in the inspection if it doesn't become a square filling exercise by the reviewer." "Everyone needs a 'tickler system' to assist them to ensure adequate coverage." "A checklist is only a guide to keeping organized notes." "Emphasis is away from checklists." "Checklists hinder independent thinking." "Checklists are an insult to one's intelligence and displays a lack of confidence in an employee's competence." "A checklist is necessary for a majority of IS Reps since most IS Reps lack either the experience or the training to perform a quality in-depth inspection without a checklist." "There is an over emphasis on meeting the administrative requirements of the program, rather than the practical requirements. Mandatory coverage during the inspection, mandatory paragraph sequence and content in the inspection report, and stale letters to management reflect adversely on the entire agency." "Even a checklist like the old form would be better than the report we now submit." "In the short time I have been here most inspections seemed like exercises in shuffling paper work." "More time should be spent

talking with the cleared people on the floor." "There seems to be more emphasis given to reviewing the administrative elements rather than interviewing employees."

# of Resp.	%	
		30. As you may know, category "A" facilities are involved with some of our most sensitive programs and projects and they represent our largest and most complex contractor operations. A certain number of facilities of a lessor category also perform work on our nation's most sensitive programs and projects. In this connection, would you favor or consider it justifiable from a security oversight and assistance standpoint to physically locate an I.S. Rep at such facilities on a full or substantially full-time basis?
68	49.9	_____ Yes
70	42.2	_____ No
28	16.9	_____ Don't know
4	-	No Response
<u>170</u>	<u>100%</u>	

Summary of respondents' comments:

Following is an illustrative sample of comments to this question: "Based on experience at a contractor facility with a QC Rep in residence--it could be effective." "Could give consultant advice on a timely basis. Would most definitely be a plus." "It should assist the contractor immensley in reducing violations, training, recruitment and enhancing the overall effectiveness of the facility security program." "I have advocated this idea for 10 years." "I am currently a one-man R.A. at a 20,000 person, 100% Defense contractor. This is extremely productive for me and the contractor's security staff." "The sheer size of many category 'A's' means that many areas are not inspected for several cycles or years..." "Suggest a 1-2 year trial with 15-20 largest contractors." "Certain facilities are involved in more classified activity than a hundred or more smaller facilities." "With the increased emphasis on in-depth inspections a lot of time is spent sending teams, often TDY, to these facilities." "Two weeks every year is insufficient to fully understand a company's security program."

"Contractors would resent such a move." "This could be viewed as threatening or doubting a contractor's integrity and could adversely affect the teamwork concept being pushed by HQs." "Familiarity breeds contempt." "Too close a relationship would develop." "DIS is to 'police' industry not 'please' industry." "We have enough problems without having our reps going to bed with the contractors." "We should not lose our outside auditor image." "The responsibility is

the contractors." "It may create a 'watch dog' effect..." "DIS would have to share in the blame for deficiencies noted."

of
Resp. %

31. Considering the universe of work and the existing assets to perform it, the current practice of conducting a complete inspection each time may be unproductive and unnecessarily time-consuming under certain circumstances. Accordingly, do you think local DIS management and I.S. Reps should routinely have the prerogative to concentrate, skip altogether, or significantly curtail coverage of DD Form 696 alpha code areas when circumstances warrant?

110	65.9	_____	Yes
39	23.4	_____	No
18	10.7	_____	Don't know
<u>3</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

Following is an illustrative sample of comments to this question. "Team chief should have the option of putting resources where the problems are not be forced to fill all squares." "We should concentrate on problem areas, windows of vulnerability and critical issues." "Regional management is responsible for getting the DISP job done and delegates portions of the job to the ISR. If we have the professional staff we should have, I see no reasons why a competent ISR through coordination with management should not be able to decide when coverage of 696 Alpha code areas should be skipped, curtailed, etc." "Such a prerogative would merely enhance the professionalism of the organization." "By testing the system using a small sampling it doesn't take long to determine if the system is working." "If you don't think this is going on now you are dreaming." "I would rather see an in-depth inspection of one sample of an Alpha code category, rather than the current practice of lightly inspecting the universe of that category." "It would be more beneficial to rotate areas of concentration during inspection. IS Reps should be encouraged and taught to concentrate on a hands-on approach, interviewing employees, spending time on the floor rather than spending a lot of time checking records." "Not to keen on 'skip altogether.' Some facilities could accuse us of being subjective if they are always inspected but the facility next door is 'given a break.'"

"Take the time to do a quality, in-depth inspection--no more, no less--in order to prevent problems, not go around them or create more." "Who decides what on what basis? The lazy or the ambitious IS Rep?" "You are inviting trouble." "This would be an invaluable tool in distorting the monthly management statistics." "Absolutely not. All areas must be covered regardless of facility size."

# of Resp.	%		32. Do you think the DISP would be strengthened if DIS maintained closer liaison with the counterintelligence community at both the national and local levels?
126	75.0	_____	Yes
11	6.5	_____	No
31	18.5	_____	Don't know
<u>2</u>	<u>-</u>		No Response
170	100%		

Summary of respondents' comments:

Though most respondents favored this concept, the following quotes further amplify their position. "Most of our people (DIS) don't know a thing about intelligence collection." "DIS should have its own aggressive CI capability to assist the FBI." "This would not only strengthen the DISP but lend greater credibility to our day to day presence in a contractor facility." "I believe there are unique threats to each geographical area that cleared personnel should be aware of." "Close liaison with the counterintelligence community would provide the IS Rep with information useful in developing 'customized' approaches to the inspection of certain facilities." "We have to know what the threat is before we can react to it." "Our local FBI counterintelligence people seem to have little knowledge of what we do, and of the DISP. They would have to cooperate with us and I can't see them doing that." "We are rarely filled in on this aspect of security." "I have heard more about 'threats' from my facilities than from DIS ... I sometimes find this lack of information a handicap." "Identification of problem areas becomes more difficult when one doesn't know what he's looking for."

"This is an area best left to FBI, NIS, etc. We don't have the time or expertise to make any contributions here." "We primarily check administrative procedures and personnel security awareness at cleared contractor facilities. I don't see what an on-going liaison would benefit the DISP or national security." We should do our thing and let the other agencies do theirs."

"I strongly urge consideration of establishing a CI element within DIS HQs. If properly staffed with knowledgeable persons, who also have investigative and industrial security experience, the proper tickets and liaison with the intel community can be fostered and maintained. I would suggest moving the 3-person security awareness Div from DSI to DIS HQS where it can be put to better use and productivity."

<u># of</u> <u>Resp.</u>	<u>%</u>		33. Should there be greater emphasis on furnishing contractor employees with counterintelligence threat information during the conduct of DI 696 security inspections?
106	63.9	_____	Yes
32	19.3	_____	No
28	16.8	_____	Don't know
<u>4</u> 170	<u>-</u> 100%		No Response

Summary of respondents' comments:

Most respondents said yes, however, the "Security Awareness Bulletin" (currently received by contractors) was cited as the principal source of counterintelligence knowledge. Counterintelligence training of DIS personnel was considered a vital requirement. One IS representative stated, "It can't hurt. Of course, we have to be informed of it first." Others wrote, "This is where our first line of defense must begin to prevent the loss or compromise of our classified information. This information would be invaluable in the facilities' education program." "Many employees are not aware of the counterintelligence threat and activity that takes place. When they are told during the inspection they express complete surprise. It would also help these individuals to be aware and report any such actions." "They don't want generalized crap; they want specifics. If we can get them, we would boost our credibility and the impact of our inspections." "I believe the contractor employees would take their security-related duties and responsibilities more seriously if they had a better understanding of the threat. Concurrently with providing the threat information, they could also be briefed in the proper ways of responding to unauthorized attempts to obtain information from them and how and to whom to report any security problems." "Why wait for a 696 inspection? Do it now if a facility is affected." "Many contractor employees think the hostile intelligence threat is exaggerated or fictitious." "I think that DIS should furnish more, but not during a 696 because the atmosphere during a 696 is not as conducive to such briefings as during non-696 periods."

Others wrote, "Let them read the security newsletter like we do." "There is already enough to do during a 696 inspection."

of
Resp. #

34. As you undoubtedly know, literally millions of dollars are expended each year on the Industrial Personnel Security Clearance Program. Notwithstanding this fact, only .04 of one percent of contractor employees had a security clearance denied or revoked during calendar year 1982. Understandably, significant criticism has been levied on a program which costs so much and provides such questionable results. Many security experts allege that the problem lies with an adjudicative system which is excessively lenient and investigative scoping criteria which is misdirected. If you agree that improvement is needed, so indicate below and identify the aspects you consider weak or ineffective as well as your suggestions or recommendations for improvement.

Summary of respondents' comments:

The security clearance process, i.e., investigative scoping and adjudicative process, is too lenient. Too much emphasis is placed on completing personnel security investigations rapidly in accordance with the scoping guide which stifles investigative ingenuity. Investigators lack sufficient training and conduct interviews with a check-off list of questions. The lack of policy on what constitutes grounds for revocation or denial of clearance handicaps the adjudicative process. A large case backlog at DISCO results in more lenient adjudicative guidelines. Adjudicators accommodate perceived permissiveness in society for many character defects such as financial irresponsibility, drug abuse and alcoholism. Adjudicators should be less concerned with legal sufficiency and more concerned with culling out those persons whose access to classified material is not clearly consistent with the national interest. Adjudicators must be willing to defend revocations or denials in court if necessary. They will lose some but must have courage. Adjudicators should have more formal training. Individuals who have used marijuana regularly and cocaine intermittently in the past year should not be granted a clearance just because they sign a form indicating they will not abuse drugs in the future--they sign this form to protect their job. This process is a farce. Low statistics for clearance denials and revocations may be attributed to the premise that persons with questionable backgrounds are deterred from applying for positions which require a clearance.

of
Resp. 8

35. I consider the weakest link of the DISP to be
(please identify and briefly explain your response):

Summary of Respondents' Comments

The preponderance of respondents felt that the personnel clearance system (DISCO, PIC, DISCR) was a DISP weakness. DISCR was reluctant to deny or revoke a personnel security clearance that could reasonably be expected to be clearly inconsistent with the national interest. "Too many people are given clearances without just cause-- as are too many facilities." Many respondents also felt that DIS did not exert enough authority over contractors. "There appears to be too many political implications between contractors and the DIS." "When a contractor has repeat deficiencies that show the contractor does not care, or the corrective action is inadequate and no response to the letter of requirements, very little action is taken by DIS." Respondents said that another weakness was reporting requirements for adverse information. "There is not enough authority to ensure facilities report this information nor to obtain access to facilities personnel records in many cases to discover the information."

Respondents to this question also thought a weak link of the DISP was "people who are not knowledgeable in the security requirements of their job and of the hostile intelligence threat in general." They believed that "problems in the DISP occur because people make mistakes."

Other respondents commented on "the rather casual attitude taken by user agencies and the freedom they seem to adopt in releasing classified information to contractors," problems with allowing DoD components to carve DIS out of the inspection of special access programs, the inadequacy of the communication link between user agencies, contractors and the DISP, and the shortage of manpower to do inspections.

Many respondents saw weaknesses as being the lack of professional training of DISP personnel "beyond the initial training stage, the policy of numbers in terms of inspections vice quality, lack of security training, unannounced inspections, a lack of cohesive policy, and an understanding of classification management."

of
Resp. §

36. I consider the strongest aspect of the DISP to be (please identify and briefly explain your response):

Summary of Respondents' Comments

Respondents believed that the strongest aspect of the DISP to be "the dedication and knowledge of personnel within the DISP." "The conscientious and hard-working IS Reps who do their best to keep contractors operating properly, and who present to industry an honest and professional image of a government employee." Other respondents felt that "the cooperation between the I.S. Rep, his facility security personnel and the user agencies (although most of the time the user agency is the lesser of the three in regard to seeing the importance of security regulations)" was a strong aspect of the DISP. Other strong aspects were cited as being unannounced facility inspections, inspection subjects and criteria, education of contractors by the Defense Security Institute, the Defense Industrial Security Clearance Office, document handling, storage and control procedures, and the "threat of an unsatisfactory rating to keep irresponsible DISP participants in line." The Industrial Security Manual and "some new innovations and changes that are beginning to be seen" were also cited by questionnaire respondents as strong aspects of the DISP.

of
Resp. §

37. The most dissatisfying aspect of or my present position or duties is (please identify and briefly explain your response):

Summary of Respondents' Comments

Many respondents to the questionnaire indicated that they were not really dissatisfied with any aspect of their present position. Those areas where some respondents expressed dissatisfaction concerned unproductive administrative paperwork and needless reports and procedures, too large a span of supervision, inadequate personnel resources (support and inspectors) to perform workload, poor working conditions, defective supervision, and "management's lack of involvement with the program." Other respondents said that occasionally they were discouraged over the "lack of enforcement," and, "The realization that it is almost entirely up to the contractor whether the DISP succeeds or fails and there isn't an awful lot I can do about problem contractors (where compromise can't be demonstrated)." Personnel policies (awards, recruiting practices and procedures, promotion opportunities, low grade structures, performance evaluations) were also indicated by questionnaire respondents as not being strong aspects of the DISP.

of
Resp. %

38. The most satisfying aspect of my present position or duties is (please identify and briefly explain your response):

Summary of Respondents' Comments

The majority of the respondents to the questionnaire said that the most satisfying aspect of their present position was a "sincere feeling that "I'm contributing to national security." Other satisfying aspects were cited as "having the opportunity to help facilities get cleared and assisting security personnel with their problems, helping a contractor interpret and apply the ISM, working with good people who are professional and dedicated, and the fact that the efforts of DIS, as well as contractors, result in strengthened security programs and a more secure America."

of
Resp. %

39. If I could change one policy or practice concerning either the DIS or the DISP it would be (please identify and explain your response):

Summary of Respondents' Comments

One policy or practice respondents wanted to change concerned the administration of resources by the DIS Headquarters level. Also, included were: "the insatiable desire" for statistics, encouraging "1810s to crosstrain in industrial security," making unsatisfactory ratings stick for at least a month or two, need for progressive management, automating manual jobs, revamping hiring practices, and increasing the journeyman grade of the ISR from GS-11 to GS-12."

Other respondents wanted "to strengthen the adjudication process in an attempt to reform the program's credibility to the high standard it once enjoyed" and making individual clearances harder to get. "Standardize the criterion and interpretation of criterion between DISCO and DISCR." Many respondents sought organizational realignments between DIS Headquarters, field offices and resident agent offices and the "revamping of procedures in the DISM 31-4," "less TDY," and "placing the promotion program out in the open." "I've seen too much favortism in the promotional structure."

Respondents also wanted: DIS to be "delegated cognizance over carve-outs," more formal training of DIS industrial security managers and representatives, change the undesirable locations of "COG offices and field offices," better "FOCI" policy, "closer control of temporary help suppliers," elimination of unannounced inspections, uniform interpretation of the ISM by region offices, use of overtime as opposed to compensatory time, improved employee morale, less rigid inspection cycles which "detract from the over-all effectiveness of the program, and speedier recruitment practices to fill vacant positions."

of
Resp. %

40. We would gratefully appreciate any additional comments, observations, criticism, or recommendations you may have to offer concerning the DIS and/or the DISP.

Summary of Respondents Comments

Overall, the majority of respondents believed the DISP to be a valuable program. Respondents additional comments, observations, criticisms and recommendations focused on the need for: training ISR's and ISS's, the Director taking time on field trips to meet subordinate staff members and explain the importance of the Industrial Security Program, "a simpler written ISM," without continual references to other paragraphs, upgrading Directors of Industrial Security in each region to grade GS-15, more awards, Industrial Security Representatives to participate in the Region decision-making process, upgrading the journeyman level for industrial security personnel to GS-12, and the need for improved morale.

Respondents felt that DIS needs more publicity--some agencies do not know who we are or what we are. Concerning the DISP, in some cases, we softshoe the contractor. That is, "no matter how seriously deficient a contractor may be found very seldom are they rated unsatisfactory, and then only with the concurrence of the Director of Industrial Security or higher."

Other respondents felt that: DISCR should be more prompt in authorizing or denying clearances; Regions should improve telephone etiquette; an industrial security law was needed; and "a rethinking was needed of our philosophy about clearing parent or grandparent companies." "It's a lot of work for facilities and people who will never have a clearance."

Other comments made by questionnaire respondents concerned taking a hard look at present "FOCI factors concerning cleared contractors," the need to more fully or more clearly address in the ISM ramifications of interim clearances on a facility, and the need for policy on the International Program. "International policy should be coordinated and included in the ISM and ISR in more detail that presently exists."

Respondents saw a need to "require local agency checks, credit checks, and a NAC" for a Secret clearance, develop a "profile of a person who might end up helping a hostile intelligence service," come down hard on security violations, and the need for more Industrial Security Representatives to carry out the DISP for the betterment of the country.

Other respondents to the questionnaire stated that one problem is that the military and user agencies do not have the same security requirements as the DISP and they tell contractors that "they don't have to follow the ISM." And that "there is a consensus among field personnel that the Region headquarters will not support the IS Rep but tends to lean over backwards for industry security officers in the 'club.'"

APPENDIX VIII

The Case of James Harper and Ruby Louise Schuler

(Prepared by the Defense Security Institute)

The Case of James Harper and Ruby Louise Schuler

On May 14, 1984, James Durward Harper was sentenced to life in prison, with a recommendation that he never be paroled. He had pleaded guilty in April to selling classified documents to the Polish Intelligence Service. The material, classified up to Secret, pertained to survivability of the Minuteman missile system and to U.S. defenses against attack by ballistic missiles.

Harper was a self-employed electronics engineer in Mountain View, California. He first became involved with the Poles in 1975 when a business associate, William Bell Hugle, introduced him to Polish agents seeking U.S. electronics technology. Harper was at that time running a small firm which made and marketed the world's first digital stop-watches. He sold technological information to the Poles for several thousand dollars. Harper did not hold a security clearance and had no direct access to classified information.

But in May 1979 Harper began what appears to have been a sort of "business-romance" with a woman named Ruby Louise Schuler. She held a Secret clearance as Executive Secretary to the President of Systems Control, Incorporated (SCI), in Palo Alto, California, a Defense contractor doing research for the U.S. Army Ballistic Missile Defense Advance Technology Center, Huntsville, Alabama. Schuler agreed to provide documents to be copied and sold. Harper contacted Hugle who, in return for a share of the proceeds, arranged a meeting with Polish Intelligence in Warsaw.

Harper conducted a total of a dozen meetings with Polish agents in Warsaw, Vienna and various locations in Mexico between July 1979 and November 1981. He received approximately

\$250,000 for documents whose loss has been rated by Army experts as "beyond calculation."

Harper and Schuler were married in October 1980. She died in June 1983 from complications of cirrhosis of the liver.

James Harper was ultimately arrested in October 1983, partly on the basis of information from a source within the Polish Intelligence Service. But his apprehension was also partly due to his own futile efforts to negotiate immunity and a double-agent role for himself through anonymous contacts with the Central Intelligence Agency and the Federal Bureau of Investigation (FBI). Shortly after his arrest, numerous classified documents were recovered from a safe deposit box in his name in a bank in Tijuana, Mexico.

The case against Harper has now been completed with his sentencing and incarceration. But certain aspects of the investigations remain active. This account is based primarily upon court papers pertaining to the prosecution of Harper, especially affidavits and testimony by the FBI investigators. It is also drawn upon a follow-on inspection of the cleared facility by the Defense Investigative Service.

The most detailed account of Harper's activities was provided by prosecution testimony at a presentencing hearing on April 16, 1984. This hearing did not receive extensive coverage in the press, although more limited information available at the time of Harper's arrest last October was widely reported.

Accompanied by his friend, Mr. Hugle, James Harper sat down on July 17, 1979 in Warsaw across the table from Zdzislaw Przychodzien, known publicly as an official of Polish Ministry of Machine Industry but in fact a lieutenant colonel in the

Polish Intelligence Service and head of an intelligence section of "Wydzial" using the Ministry as cover for collection operations against the West. Przychodzien was fluent in English, having been assigned to the U.S. in the 1970's with the Polish Commercial Office in New York.

Harper described the materials now accessible to him through Louise Schuler at Systems Control, including classified documents pertaining to U.S. strategic forces and ballistic missile defenses. And he provided reproduced excerpts of ten documents. (Enroute to Warsaw he had placed copies of the full documents in a safe deposit box at the Citibank in Paris.)

Przychodzien was very interested in the material. He promised generous payment, although he demurred at the American's initial asking price of \$1 million. Also discussed at this July meeting was other materials available to Harper including computer data base tapes obtainable through his contacts in Silicon Valley.

Harper and Hugle agreed to meet with Przychodzien again in Vienna the following October. On that occasion, Harper delivered full-text copies of the ten documents which Przychodzien had previewed earlier. He also provided excerpts of additional documents. But a disagreement arose over the matter of payment which caused the meeting break-up. Harper was unsure of his position with Przychodzien. It appeared that the Poles were not as interested in the classified Defense documents from SCI as he had originally thought, so, upon his return to California, he buried them in an out-of-the-way location in the San Joaquin River delta near Stockton--just for safe-keeping in case a buyer could later be found.

At this point, Harper wanted nothing further to do with Hugle, but he was able to reestablish contact with Przychodzien

through a friend in Switzerland, and he returned to Warsaw in May 1980 with the Silicon Valley data base tapes and without any classified documents. But it was the classified ballistic missile material that Przzychodzien really wanted. The intelligence officer paid \$10,000 for the ten documents delivered at the meeting in Vienna and urged Harper to come back with all of the Defense documents he could get his hands on.

So Harper went back to the delta, dug up his "stash" and transported the additional documents to Warsaw (via Vienna and Geneva) the following month (June 1980). Harper later estimated that this second delivery of classified reports weighed about 100 pounds. The documents were somewhat the worse for their seven-month interment on the banks of the San Joaquin River. But Przzychodzien's people worked through the night of June 5 to separate the matted pages and restore the materials to decipherable condition.

On June 6, the documents were brought to the Soviet Embassy where a team of 20 KGB experts, flown in specially from Moscow, declared them to be genuine and extremely valuable. Harper was paid \$100,000 on this occasion. A month later Przzychodzien and his unit received a commendation for their efforts, directly from KGB Chairman Yuri Andropov.

Harper next returned to Warsaw in September 1980, this time bringing along a document register for the safe in his wife's office, i.e., an inventory of all documents in the SCI president's security container. The Poles selected several items for purchase and Harper delivered them during visits to Warsaw in October and November 1980, receiving \$20,000 in payment.

During the November meeting with Przychodzien, Harper was instructed to meet next time in Mexico City with a Polish agent whom he knew only as "Jacques."

The first meeting with Jacques took place as agreed at the cashier cage of the Museum of Anthropology on December 14, 1980. Harper brought no documents, treating the occasion as a dry run to establish contact and "get the feel of the city." Jacques paid him \$10,000 anyway, and at the next encounter in the same city two months later Harper brought nine Secret documents and received \$60,000.

Following one more transaction with Jacques (eight classified documents and excerpts for 30 more, in return for \$50,000), Harper told the agent in September 1981 that he was dissatisfied with the payments he was receiving. He brought no documents to the September meeting in Guadalajara, and received no payment, although Jacques had brought along \$30,000 for the 30 documents previewed last time in extract. It was agreed that Harper would go back to Warsaw to work out his complaints with Przychodzien directly.

This was in fact the end of Harper's active dealings with the Poles. He made a trip to Warsaw in November 1981 and spoke with Przychodzien, but he remained dissatisfied with the payments offered and no further contacts ensued. Before going to Warsaw, Harper had driven with Louise to Tijuana and placed his remaining collection of classified documents in a safe deposit box where they remained until retrieved by the FBI, with Harper's cooperation, following his arrest.

These were, in fact, the last documents available to Harper, since Louise lost her clearance in August 1981, not due to any suspicion of her activities, but rather due to acquisition of her company by a foreign firm. Under an

arrangement approved by the DoD, SCI's Defense contracts have been retained by a "spin-off" company insulated from the parent by a stock proxy agreement. The facility clearance for this subsidiary was later upgraded from Secret to Top Secret. But Ruby Schuler remained an employee of the original SCI organization, now under British ownership, and her Secret clearance was administratively terminated as a result.

She died June 1983 of cirrhosis of the liver. Her death certificate lists "alcoholism" as a "secondary cause" of death.

In September 1981, at the time he was becoming increasingly unhappy about his exchanges with the Poles, Harper contacted attorney William Dougherty requesting that Dougherty act as go-between in negotiations with the CIA and FBI. Harper wanted to arrange immunity from prosecution in exchange for information on his activities and services as a double agent. While concealing his identity from the lawyer, he provided detailed written and tape-recorded accounts of his espionage activities through Dougherty to the Government. This continued for two years until Harper's ultimate arrest, although the Government showed no willingness to agree to his terms.

Investigators succeeded in positively identifying him in March 1983. He was immediately placed under surveillance at his home in Mountain View, California, where he was at that time living with Louise. Wiretaps were also authorized and installed on their telephone. Investigators were able to learn the location of a storage locker where Harper kept records of his activities. They also learned he was planning overseas travel and was again in contact with the Swiss friend who had arranged earlier meetings with Przychodzien.

He was arrested on October 15, 1983, forestalling any chance that he would turn over his remaining documents.

One lesson of this case is unmistakable confirmation of the intimate ties between Warsaw Pact intelligence services and the Soviet KGB. It is clear not only that the Polish Intelligence Service works closely with the KGB, but that they in fact work for the KGB. When Harper brought his main installment of documents to Warsaw in June 1980, the Poles spent the night putting the pages in order, but once collated, the materials were immediately turned over to the Soviets for evaluation and analysis.

Harper has stated to the FBI that the tasking presented him by the Polish agents was derived from a "master shopping list" provided by the Soviets. And this has been confirmed by the Polish intelligence officer who served as a source in breaking the Harper case. The source has confirmed that Polish agents respond directly to detailed tasking from the KGB, with military collection as a top priority.

The Polish source was aware of Harper's activities, although he did not know Harper's identity. Przychodzien had told him of the initial meetings with an American, fitting Harper's description, who had access to ballistic missile information. And he even recalled seeing a phone message from Hugle written on Przychodzien's desk calendar at the time of those first meetings in October 1979. This inside information confirmed the authenticity of Harper's accounts once his anonymous statements began coming in.

Information so far available does not reveal any major security deficiencies at SCI which can be identified as contributing directly to Harper's and Schuler's activities. She apparently removed the documents from the facility to be reproduced at home on a paper copier which Harper had bought for the purpose. As in most facilities, governmental or

industrial, there were no searches at the exits to prevent removal of classified material.

Schuler was noted in the facility during evenings and weekends. On at least one occasion Harper was with her. But this was not a violation since he was escorted -- by Schuler! Unexplained off-hours activity has often been highlighted as a possible indication of espionage, and this is another case in point.

As a result of the case, the company has centralized its classified document storage at one location under direct control of the security officer (something which would obviously not be possible for a larger facility), and they have implemented tighter personnel access controls for nonworking hours.

There are some indicators that certain adverse information regarding Louise Schuler was known to co-workers and company officials and was not reported. She was, first of all, an alcoholic and ultimately died of complications from that disorder. Quotations in the press indicate that co-workers were aware that she carried vodka in her purse and drank on the job. An inquiry into that issue might have revealed some indication of her illicit activities, or possibly exerted some deterrent effect.

In addition, a former official of the company, also a cleared individual, had a close involvement with Louise during much of the period in question, and he was aware not only of her drinking, but also of her unexplained income. She does not seem to have flaunted her ill-gotten gains in a public sort of way, and most co-workers would have had no occasion to notice anything out of the ordinary. But the company executive was with her on at least one occasion when she placed a large stack

of \$100 bills in a safe deposit box at a local bank. He did not report this either at the time or when later interviewed by the FBI. His security clearance (he is now with another cleared company) has been suspended pending resolution of his possible involvement in the case.

APPENDIX IX

The Case of William Bell and Marian Zacharski
(Prepared by the Defense Security Institute)

The Case of William Bell and Marian Zacharski

Marian Zacharski arrived in Los Angeles from Poland in late 1976. He was assigned as West Coast Branch Manager for the Polish American Machinery Company (POLAMCO), a U.S. incorporated firm serving as marketing arm for the Polish trade agency, Metal Export.

But machinery was not Zacharski's only business. He was also covertly assigned by the Polish Intelligence Service to spot and recruit agents within California's aerospace industry. And he was for a time highly successful in both of his occupations. By early 1981 (at the age of 29), he has been appointed president of POLAMCO, and he had recruited at least one agent with access to important classified weapons information and technology.

Thereafter, Zacharski's fortunes took a turn for the worse, and by the end of 1981, he was serving a life sentence for espionage against the United States -- but not before doing both a lot of good for Polish exports and a lot of harm to U.S. national security.

William Bell was Zacharski's agent. He was born in Seattle, Washington, on May 14, 1920. He was employed as an engineer with Hughes Aircraft Company and met the Polish businessman in 1977 at the Cross Creek Apartments in Playa del Ray where both were residents. The two shared an interest in tennis as well as a common concern with the aerospace industry, where Zacharski sold much of his industrial equipment.

After almost a year of purely social and recreational contacts, Zacharski began to ask Bell for unclassified literature from work. Then he asked for "interesting" material and received first Confidential, then Secret documents to look

over. He paid Bell lavishly for his minimal "consulting" work. And when Zacharski proposed that Bell, for additional thousands of dollars, photograph classified documents and carry them to Europe to meet other Polish representatives, Bell was ready to go along. Soon he felt "over his head" and too committed to back out. William Bell is now in prison, serving an eight-year sentence.

Zacharski's recruitment approach was a standard one. It should be as familiar and, hence, as ineffective as attempts to sell shares in the Brooklyn Bridge. But Bell's susceptibility was not the result of tender years, or slim experience or lack of education, training or intelligence. He was 57 years old when he met Zacharski, with 25 years in defense work, a B.S. in applied physics from UCLA and two overseas tours with his company.

Bell had been briefed on the threat of hostile intelligence services, but he did not recognize the classic approach when he encountered it in real life. He did not believe that it could actually be happening to him, that this amiable Polish tennis buff (who reminded him of his estranged older son) could possibly be anything other than what he appeared to be.

Marian Zacharski was arrested for espionage in June 1981 and went to trial in October. He was convicted largely on the basis of William Bell's testimony against him, and Bell's lighter sentence was based in part upon consideration of his cooperation with the government in the final stages of the investigation and the trial. This account of the Bell/Zacharski espionage case is based primarily upon the transcript of Zacharski's trial. It also draws upon Bell's testimony in May 1982 before the Senate Permanent Subcommittee on Investigations.

In the fall of 1977, when he was first introduced to Marian Zacharski at the swimming pool of the Cross Creek Apartments, William Bell had recently returned to Los Angeles from an assignment in Brussels as Manager of European Operations for the Radar Systems Group, Hughes International Corporation. He was now a Project Manager in the Advanced Systems Division, Radar Systems Group at the main Hughes facility in Los Angeles.

Bell held a Secret security clearance and was responsible, as he later testified, for "development and promotion of the radar fire control product line of tank vehicles." He had been with Hughes since graduation from UCLA in 1952, employed entirely at the Los Angeles facility except for two European assignments (in mid-1960's and from 1974 to 1976).

In his Senate testimony, Bell stated that these overseas assignments had been "financial nightmares" for him, "although they are touted as glamorous and lucrative." Upon his return in 1976, he recalled, he was "pursued by four separate Internal Revenue Service offices for back taxes on disallowed deductions primarily arising out of my overseas assignments." The year of 1976 was in fact a low point in Bell's life for a number of reasons. He was divorced from his wife after 29 years of marriage ("in an extended proceeding") and was faced with alimony payments of \$200 per week. His accumulated debts forced him to file bankruptcy in July 1976. During the previous year, Bell's family had suffered a tragic loss when his 19 year old son died in a camping accident in Mexico.

In addition to financial hardship, divorce and personal tragedy, Bell also later recalled feeling "like an outsider" upon his return to the Los Angeles plant. "I returned from Europe to find a younger group at Hughes and I (was) shunted off to a quiet back room." But regardless of any

disappointment with his assignment, Bell was in fact given major responsibilities for development of advanced weapons systems -- a fact which Marian Zacharski was quick to learn.

When he met Zacharski in 1977, Bell was attempting to make a new start. He had remarried ("to a young Belgian citizen," formerly his secretary overseas) and had taken up residence with her and her six year old son at the Cross Creek Apartments. He was making a gradual financial recovery (although alimony, taxes and debts still put a strain on his \$35,000 income). And he found comfort in the companionship of a close friend:

"Zacharski and his wife moved into the apartment complex and I began to play tennis (with him) on a daily basis. He slowly became my best friend. He was about the age of my oldest son who had been close to his mother and quite distant from me since our divorce."

Marian "made friends easily," Bell recalled. The two couples socialized frequently, both by themselves and with an informal "little United Nations," a social group at the complex consisting of couples one or both of whom were foreign nationals. And the two men found common professional interests as well. Zacharski was a skilled and successful salesman of industrial equipment and the California aerospace industry was one of his principal sales targets. He naturally discussed the aerospace business with his tennis partner and in about mid-1978, he asked Bell for help in making contacts at Hughes and other companies in the field.

Bell gave Zacharski's name to a purchasing manager at Hughes and also contacted people at Lockheed and Northrop. And for this, Zacharski paid him approximately \$5,000. At the

trial, the cross-examining attorney wondered why Bell had not been suspicious of such generosity. He had been, he claimed, though evidently only temporarily. "To receive four or five thousand dollars for doing practically nothing made me very suspicious."

Q: It also made you very glad, did it not, Mr. Bell?

A: It sure did. I needed the money.

Bell and Zacharski discussed the possibility that Bell might be permanently retained by POLAMCO as a "consulting engineer" and sales advisor, although the terms of the arrangement were left studiously indefinite ("I was working, in a way, and talked about working as a consultant for POLAMCO..."). Bell began again around mid-1978, to provide printed material from the office, to help Zacharski keep abreast of sales opportunities. It started out (with) simple things," Bell later told the grand jury, "like the Hughes News," the company newspaper.

Then came documents of more technical substance. He brought Zacharski copies of the Hughes "Vector," a technically-oriented publicity sheet on company programs. Zacharski had specifically requested these openly-published materials. But then Bell began to volunteer materials in response to Zacharski's general expressions of interests. "I could tell from our conversatons that they were things that he would like to see." "We would be talking about it at the tennis court -- unclassified documents in the beginning."

During the summer of 1978, he provided Marian with several documents "related to items that were machined." These were unclassified, at least for the most part, but "there was possibly one Confidential I'm not certain." Bell has

never been sure of exactly when he first showed Zacharski a Confidential document -- or just which or how many such documents he had compromised.

He may also have been uncertain in his grasp of security requirements for the handling of Confidential material, as indicated by this courtroom exchange between Bell and prosecutor Robert Brewer:

Q: Would that (taking documents home) be a violaton of ... security policy?

A: Not a Confidential document no. You can bring confidential documents home. You cannot bring secret documents home.

The Secret documents which Bell compromised can be more reliably identified since the company maintained accountability records for them (not required by the Industrial Security Manual for Confidential). Bell determined that his first transfer of Secret material occurred in October or November of 1978 when he lent Zacharski (at the tennis court) Copy No. 8 of the "Proposal for a Covert All-Weather Gun System, Executive Summary, Volume I." Bell was the author of this material. He wanted Zacharski to understand his role at Hughes and he wanted to impress him with his work. "I was proud of it," he said of the Executive Summary, "and I gave it to him." Later, Bell turned over an unclassified document on the same subject and stamped it Secret "to make it look more important."

The Covert All-Weather Gun System ("CAWGS") was the primary development project under Bell's technical management at that time. It envisioned the application to tanks of the Low Probability of Intercept Radar ("LPIR") or "quiet radar." LPIR utilizes a disguised radar signal which is difficult for

enemy targets to identify as radar; they are thus prevented from taking evasive action or using the radar signal for directing return fire. The CAWG, subsequently redesignated the Dual Purpose Weapon System or "DPWS" (to be used against both aircraft and other tanks), was Bell's main responsibility throughout his relationship with Zacharski. It was, according to trial testimony, the principal program compromised by his espionage activities.

It was announced in mid-1978 that the Cross Creek Apartments would be converted to condominiums. Bell and his wife wanted to remain, but he was worried that he could not make the down payment required to purchase his unit. His friend Zacharski said he might be able to help. And in February 1979, he provided Bell with \$12,000 in two payments handed over in envelopes at the door of Bell's apartment. They were speedy and uncomplicated transactions, as Bell later testified: "Q: Did you say anything to him? A: 'Thanks.'"

He used the money for the condominium payment and for back taxes. He assumed that the money was from POLAMCO's "marketing" fund. And he credited Marian's good will with inspiring this generosity. "I thought we were good friends and I knew he would like me to stay in the apartment complex. I wanted the condominium and I accepted the money."

Bell still thought it was in connection with "consulting" activities when Zacharski suggested, in the summer of 1979, that he travel to Europe to meet certain unidentified Polish representatives ("whom I thought would be POLAMCO people"). He was asked to photograph documents from work and bring the film with him to the meeting in Innsbruck, Austria. Marian had earlier given Bell a Canon movie camera, which turned out to have a frame-by-frame capability ideal for photographing

documents. He provided a tripod and special film and instructed Bell in using the camera in his bedroom.

William Bell departed on the first of four overseas "missions" on November 26, 1979. Marian gave him about \$2500 for expenses, although Bell's wife was an airline flight attendant and his trans-Atlantic fare was \$18. On the morning of November 30, he went to a predesignated restaurant in Innsbruck and was met by a man who introduced himself as "Paul" and asked "are you a friend of Marian's?" -- the agreed upon recognition signal. The two left the restaurant and entered a car driven by another man (name not recalled) and drove to the outskirts of Innsbruck.

Bell handed over his film and the three men discussed Bell's work, the types of information he should attempt to collect and the need for secrecy and security. At one point Bell was shown a picture of his wife and son. "He (Paul) told me that I had a lovely family. Then he said that our security depended upon each other and that if anybody got out of line that he'd take care of them." The Poles did not dwell on the point, but Bell clearly perceived an "implied threat" in Paul's words. Before leaving Innsbruck, he received \$7,000 and agreed to another meeting in the same city in May 1980.

When he returned to Los Angeles, Bell received an additional list of desired collection targets from Zacharski. On this and other occasions he was surprised at Zacharski's highly specific knowledge of system designations and even particular document numbers.

Q: And did you ever ask Mr. Zacharski where he obtained those numbers?

A: Yes.

Q: What did he say, if anything?

A: He didn't answer me. He just smiled.

By now, at the end of 1979, Bell could no longer maintain the illusion that he was involved in a (more or less) innocent consulting arrangement with POLAMCO. It was clear, as he testified, that he was "conducting espionage" for "agents or offices of the Polish Intelligence Service." And Zacharski himself dropped any such pretense after that time. He made no more requests for assistance in promoting machine tools.

Bell took three more trips to Europe, meeting with one or both of the Polish operatives at Innsbruck in May 1980, at Linz (Austria) in October 1980 and at Geneva in April 1981. Prior to each meeting, he photographed several documents with the movie camera in his apartment (when his wife was away). At the Innsbruck meetings, he provided film of unclassified and Confidential documents. At Linz and Geneva, he turned over copies of Secret material related to the DPWS and LPIR systems. He continued to receive substantial payments, in bills and in gold, from both Zacharski and the handlers overseas.

After Geneva, Bell's next meeting with the Poles was to be in Mexico City. He was uneasy about transacting his business there, he testified, in part because "Mexico City is where a spy was caught, I don't recall his name." The name, of course, was Daulton Lee, accomplice of TRW spy Christopher Boyce. But Bell was relieved of the necessity of following Lee's footsteps to Mexico. He was called to Hughes security on June 23, 1981 to be questioned by the FBI. At the trial, Special Agent James Reid recalled the crucial point of the interrogation as follows:

(Reid): I showed Mr. Bell a translation of a Polish newspaper article which indicated an individual who had been assigned to the U.N. in New York had defected to the United States Government. I then explained to Mr. Bell that this individual had in fact defected, and that he had been providing the FBI with information concerning activities of the Polish Intelligence Service in this country.

Q: What if anything did Mr. Bell say?

A: Mr. Bell asked, "Did he mention me?" And then without waiting for an answer, he said, "this is very serious. I would like to talk to an attorney."

(Reid told Bell that he could talk with a government attorney or make a telephone call to an attorney of his own.)

Q: And after you said that, what happened?

A: Well, at that point Mr. Bell physically slumped in his chair and he said, "I did it. I do not need an attorney."

Bell signed a confession and agreed to cooperate in the further investigation of Zacharski. On June 28, he was fitted with a hidden recording device when he met with Marian on the apartment grounds to discuss further payments and certain sensitive programs at Hughes which Zacharski was interested in targeting. Zacharski was arrested shortly thereafter.

The Lessons

The Bell case, like any other espionage case, has its unique and peculiar elements. But it is, by and large, a "text-book" case which confirms many of the long-standing precepts of counterintelligence, as well as patterns derived from recent espionage cases.

Financial gain was Bell's primary motivaton. This is typical of most recent cases, and his testimony was quite clear on the point. Politics or ideology did not play a part:

Q: You are not, in other words, a secret Polish patriot?

A: No I am not.

The motivation was primarily mercenary. "Mr. Zacharski had found a fool that needed money. I had a weak spot. He took advantage of me." Bell also cited the veiled threats from "Paul." This played some part in his thinking and discouraged him from pulling out once he was involved, but "the motive was always money." ("Q: Was it worth it? A: No, absolutely not.")

Financial difficulties and other personal problems were an important cause of Bell's susceptibility to recruitment. From his trial testimony, it appears that Bell faced the kind of difficulties which everyone encounters at some time during life, although the coincidence of several misfortunes in quick succession clearly contributed to an imbalance in judgment. Withdrawl of clearances in cases like this might generally be considered both cruel and unusual. But certainly whatever positive assistance or counselling an organization might provide to employees in trouble, combined with an active

program of defensive security training, will help to ensure that a person like Bell is not so choice a target for a person like Zacharski.

Job dissatisfaction or some element of grudge against the company or the U.S. government have figured as predisposing elements in several recent cases (Boyce, Kampiles, Edwin Moore, etc.). Bell's remarks display some signs of disgruntlement with Hughes. The European assignments were not as "glamorous and lucrative" as they were "touted" to be; he felt like an "outsider" among the younger personnel at the Los Angeles plant -- and so forth. But here again Bell's difficulties were of a rather ordinary sort, providing no obvious warning of an employee who was ready to take desperate measures.

Several attempts have been made in recent years to draw up a behavioral profile of the typical spy, to identify the patterns of activity which are characteristic of espionage in progress. Bell's is presumably one of the cases which underlies this analysis and his activities do in fact lend credence to several of the major espionage indicators. Early reporting of suspicious behavior may help to halt an espionage operation before irreparable damage is done.

Unexplained affluence is well known as a possible tip-off to ongoing espionage and certainly Bell received a substantial increase in income from his illicit activities. His estimates of the total amount varied widely, from \$470,000 to \$170,000. Payments specifically cited during the trial were totalled to between \$101,000 and \$103,000.

Bell spent or invested most of the money, although some of the gold remained unconverted at the time of his arrest and was confiscated by the government. His testimony indicates that he was relatively conservative in his use of the funds, and even

the luxury items cited -- a "red Cadillac," a \$2000 necklace for his wife and a brief vacation to Rio de Janeiro --would not necessarily appear extravagant for a family with an income of \$52,000 (in 1980, \$40,000, his wife, \$12,000). Much has been made in press coverage regarding the "young stewardess" angle in the case, but there is no indication that Bell's second wife either contributed to his financial setbacks or drove him to seek new income in support of an inflated lifestyle. (And she was not in fact an airline flight attendant when she met and married him but entered training in January 1979.)

Bell's windfall earnings were directed not to high living but primarily to hastening his recovery from bankruptcy. His was a case not so much of unexplained affluence as of unexpected solvency. Any major alteration in financial circumstances may be of significance when personnel with access to classified information are involved.

Attempts to gain unauthorized access to classified information (e.g., beyond legitimate need to know) are often characteristic of diligent spies, but Bell seems to have avoided this pitfall. He was apparently a cautious (or lazy) agent and did not seek out information beyond his assigned projects. The major compromises confirmed at the trial (LPIR, DPWS) fall within the scope of his primary duties as a project manager.

Removal of classified material from the facility is a more or less inevitable accompaniment to spying, and certainly Bell took some risks in this regard. When he carried documents home to be photographed, he was vulnerable to detection since Hughes had a policy of random searches at the plant exits. Either Bell was lucky in his timing or he was somehow able to anticipate the searches. In any case, he was never caught in the act.

Foreign travel, on a regular basis and without sufficient explanation, is another "tell-tale sign" displayed by Bell and one which evidently contributed to his detection. His trips to Europe were partially legitimized by company business and family visits. But testimony (by Bell himself and by a Hughes security official) indicates that his overseas travel -- and, on one occasion, incomplete reporting of his itinerary -- was a factor which helped to place him under suspicion.

So Bell confirms, to some degree, certain of the behavioral patterns associated with previous cases of this kind. Financial difficulties and job-related dissatisfaction can predispose an individual to espionage. Unexplained income, unauthorized removal of documents and unexplained foreign travel may be indicators that espionage activity is underway. But the case also confirms the difficulty of applying this sort of preventive counterintelligence to real-world situations, without the benefit of "20/20 hindsight." The real "ounce of prevention" would have involved measures to forestall Bell's recruitment in the first place. And there is good reason to think that this could have been done -- with the infusion of a little more awareness.

This presupposes that Bell was genuinely unaware, during the initial stages, of what Zacharski was up to. A more cynical view might suppose that he knew exactly what was happening all along and complied with Zacharski's wishes, from the beginning, with his eyes wide open. But those who investigated and prosecuted Bell are inclined to accept his account of the evolution of the case. And Bell has testified that, when he returned to the state-side facility from Brussels, he assumed that his worries were over where hostile intelligence activities were concerned. "When you are sent to Europe," he told the Senate Subcommittee, "you are told to

expect attempts by foreign spies, but whoever would expect it to happen here at home?"

He received the required briefings and signed the required forms upon rejoining the Los Angeles organization, but apparently treated them as a matter of insignificant routine. A "Security Briefing and Termination Statement" was introduced in evidence at the trial, and he acknowledged having seen it: "I recall signing the normal form you signed when you hire into the company.... There are many forms you sign and I am sure that was one of them."

"Whoever would expect it to happen here at home?" It was in this innocent frame of mind that Bell initially made the acquaintance of the Polish machinery salesman and then agreed (in fact eagerly sought) to serve as a consultant for POLAMCO, an arrangement which included providing inside information on his company. The delusion persisted right up to his first overseas visit:

Even as I went to Innsbruck, Austria, I was rationalizing and kidding myself that the persons I would meet were representatives of POLAMCO, that this was just the kind of industrial espionage that goes on all the time.

After his return from Innsbruck, Bell knew exactly what he was doing and exactly what had been done to him. Why he did not extricate himself at that point is a complex psychological question involving a confluence of material inducements, Zacharski's personal magnetism and "Paul's" implicit menace. For whatever reason, Bell now felt genuinely trapped. He told the Senators after his conviction: "There is little left of my life now but I feel I am freer in prison than I was with Zacharski."

Clearly, there was more to this entrapment than simple monetary temptation. And we must not take too literally Bell's own statement that he was "a fool that needed money." A fool he may have been and he was certainly hungry for cash. But too much stress on Bell's foolishness can lead us to ignore Zacharski's skill. Preoccupation with financial motives, moreover, can obscure the fact that many months of cultivation preceded the first mention of money between Zacharski and Bell. We must not ignore the subtle but powerful psychological influences which reinforced the material incentives once offered and laid the groundwork for Bell's receptivity, by creating a willingness to regard Zacharski's offers as well-intentioned, as motivated by friendship and good will.

Bell's recruitment was the result (not necessarily the only result) of a carefully planned and orchestrated intelligence operation. As the focal point for this operation, Zacharski was provided with the best possible cover for his activities, a cloak of propriety calculated to inspire the least possible suspicion. To begin with, his nationality was in his favor. As a citizen of an Eastern European country, he would not present the same threatening image as a Soviet national -- although there can be no doubt that the information he collected was to be shared with Poland's Warsaw Pact ally. (It might be recalled in this connection that during the year Zacharski arrived, 1976, a Presidential candidate had come very close to declaring Poland a member of the free world!)

In addition, he was provided with a commercial rather than a diplomatic position. He was employed, in effect, by the Polish government, but as a salesman of industrial equipment he assumed an image which was less official and hence, again, less threatening. In addition, he was exempt from travel restrictions imposed upon diplomats from communist countries and had more flexibility of movement and greater access to U.S.

industrial facilities and personnel. Of course, commercial status carried with it a certain disadvantage: no diplomatic immunity. Zacharski is no doubt now hoping to be exchanged for someone imprisoned in the Soviet bloc, but there have been no indications that a swap is contemplated.

Once fitted with suitable camouflage, Zacharski was introduced into a promising hunting ground, the technology-rich area of Los Angeles, California. He moved into an apartment complex where many executives and engineers of aerospace companies were residents. And he set to work.

Having met William Bell, as he must have met many others in similar professional positions, and having decided to proceed with cultivation, Zacharski worked with extreme caution and practiced subtlety. He was a skilled salesman and master persuader and well equipped for his task.

Bell testified that they first met in Autumn 1977. He could recall no requests of any kind from Zacharski until mid-1978. So Zacharski spent the better part of an entire year simply making friends with his prospect, insinuating himself into his personal life, meeting and befriending his family, assessing his character traits (and flaws), learning his likes and dislikes (and sharing them), discerning his weaknesses and above all his needs.

Only after many months of this did he begin seeking active assistance from Bell and overtly feeding his desire for money. Cornelius G. Sullivan, a former counterintelligence agent with the FBI, testified at the trial that this is a crucial "dividing line" in the process of developing an agent, the boundary between a simple social relationship and one involving overt exchange. This "barrier" is typically overcome, he said,

by first requesting unclassified and seemingly innocent items -
- and this of course is the approach which Zacharski adopted.

There is also a second dividing line -- between providing innocent, public materials and handing over restricted, sensitive and/or classified items. Zacharski used the "consulting" process to bridge the barrier between legal successful strategy. It was so effective in fact that Bell apparently volunteered the first transfers of classified material on his own initiative.

Offering the prospect of a consulting arrangement, as a prelude to espionage, proved successful in this case for a number of reasons. The promise of additional income appealed to Bell's financial hunger, of course. And it must also have appealed to his entirely normal professional vanity to be asked to lend his technical expertise and the benefit of his contacts in the industry. Because the arrangement was obviously improper to a degree, it introduced a surreptitious element into the Zacharski/Bell relationship and helped to ease Bell toward a fully clandestine role as a full-fledged spy. (Bell explained his additional income to his wife as coming from work for a Swiss aircraft firm. He asked her to be discreet about the arrangement, stating that Hughes would not approve of his consulting for a competitive firm.)

Perhaps above all the consulting arrangement permitted Zacharski to deceive Bell, and Bell to deceive himself, into regarding the initial compromises of national security information as a venial sort of "industrial espionage." "Within the avionics industry," Bell told the Senate Subcommittee, "It is a common practice for all companies to obtain the secrets of their competitors by the same techniques Zacharski used with me."

He thought of POLAMCO as "an American company." They had offered him a job which would be "the solution to all my problems." And providing them with inside information from Hughes would only be adhering to the common practices of the industry, as he interpreted them:

An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to security classification....

Whether or not Bell accurately describes a common practice, he certainly does reflect a common attitude -- "Everybody's Doing It." Zacharski exploited this attitude and used the consulting ploy to ease Bell almost imperceptibly into his initial ventures in the illegal exchange of information. After that, Bell felt that it was too late to back out, and it was indeed too late to prevent some damage to the national security, since some damage had already been done.

APPENDIX X

The Case of Christopher John Boyce
(Prepared by the Defense Security Institute)

The Case of Christopher John Boyce

Christopher Boyce's case involves a program outside the Defense Industrial Security Program and thus only a brief synopsis is provided.

Christopher Boyce was an employee of TRW, Incorporated, in Redondo Beach, California. From 1975 to 1977 he worked as a security clerk in a "black vault" operated at the facility in conjunction with a CIA contract.

Boyce eventually entered into a scheme with his boyhood friend, Daulton Lee, whereby Boyce would remove classified documents from the vault, photograph them, and Lee, in turn, would sell them to the Soviets at their embassy in Mexico City. Eventually, Lee was taken into custody for acting suspicious outside the Soviet Embassy. Mexican authorities discovered clasified material in Lee's possession. Lee, in turn, implicated Boyce.

Ironically, Boyce had already resigned his position at TRW and, at the behest of his Soviet mentors, planned to go back to college and eventually obtain a sensitive government job. Presumably, he would then continue his espionage activities on behalf of the Soviet Union.

Boyce and Lee were arrested by the FBI in January 1977 and charged with selling secrets to Soviet Agents. Both eventually were convicted with Lee being sentenced to life and Boyce being sentenced to 40 years in prison. Incidentally, Boyce escaped from Federal prison in January 1980 and was not recaptured until November 1981.

Appendix I
DIS Categorization System

Appendix I
DIS Categorization System

Category A. The Category A facility is normally a large and complex operation which is involved in most aspects of the DISP. It usually employs several hundred cleared personnel, is performing on numerous contracts, and possesses several thousand classified documents located at dozens of classified control stations throughout the plant. Offsite locations, classified ADP systems and graphic arts activities are usually involved. The Category A facility requires a Team Inspection.

Category B. The Category B facility is described in much the same manner as the Category A facility, except that its universe of classified documents, cleared employees, classified control stations, ADP systems, etc., will be somewhat less than the Category A facility thus resulting in a lower point evaluation. Based on classified involvement and supervisory determination, the Category B facility may require a Team or Individual effort.

Category C. The Category C facility is only moderately involved in classified activities. It normally has only a few classified contracts and considerably less cleared personnel and classified holdings than Category A and B facilities. Except in unusual circumstances, the inspections of a Category C facility is an individual effort.

Category D. The Category D facility has only limited classified involvement. It will normally have only one or two security containers, a relatively small volume of classified items and only a few cleared employees. The inspection effort for a Category D facility requires only one individual.

Category E. Category E is reserved exclusively for those facilities performing in the DISP on an ACCESS ELSEWHERE basis. Guard and Janitorial facilities are included as well as other active DISP facilities without approved classified storage capability.

Category F. Category F is reserved exclusively for DORMANT facilities. A facility is DORMANT when it is not possessing classified material/information and when no employee/official is currently having access to classified information

DIS Categorization Point Factoring Criteria

Number of Cleared Employees

1 - 35 = 3 (points)
36 - 500 = 5
500 + = 10

Accountable Items

1 - 50 = 5
51 - 500 = 7
501 - 3200 = 12
3200 + = 15

Non Accountable Items

1 - 50 = 3
51 - 500 = 6
501 - 3200 = 7
3200 + = 8

Controlled Areas

Closed: 3 pts each
Restricted: 1 pt each

Approved ADP Systems

DP: 3 pts each
WP: 1 pt each
Other: 2 pts each

After Hours/Varied Shift
5 pts

Approved off Sites
3 pts each

COMSEC
Each Account : 3 pts

Approved Supplemental Controls
Badge = 2
Guards = 2
Alarms = 2

Government to Government Since
Last Inspection
5 pts maximum

Special
Top Secret = 3
New Carve Out = 2
NATO/CNWDI/WNINTEL = 2

Current Visit Letters
5 pts maximum

Classified Contracts
1-10 = 5
10 + = 10

Totals: Over 115 pts = A
71 to 115 pt = B
46 to 70 pts = C
45 or less pts = D
All Access Elsewhere = E
Dormants = F (except graphic arts
and commercial carriers)

APPENDIX XII
COMPILATION OF PERSONNEL CONTACTED
DURING THE COMMITTEE STUDY

COMPILATION OF PERSONNEL CONTACTED
DURING THE COMMITTEE STUDY

OFFICE OF THE SECRETARY OF DEFENSE

Maynard C. Anderson, Director, Security Plans and Programs,
Office of The Deputy Under Secretary of Defense for Policy
(ODUSD(P))

Robert S. Brady, Chief Department Counsel, Directorate of
Industrial Security Review (DISCR)

Terry Crites, Staff Assistant to Director, DISCR

John J. Delaney, Chairman, Screening Board, DISCR

John F. Donnelly, Director, Counterintelligence and
Investigative Programs, ODUSD/P

William Fedor, Deputy Director (Personnel Security), ODUSD/P

Rita Friga, Industrial Specialist, Office of Industrial Base
Assessment

James A. Hall, Screening Board, Panel #1 Leader, DISCR

James H. Kordes, Director, Office of Industrial Base Assessment

John J. Meehan, Directorate of Security Plans and Programs,
Deputy Director (Industrial Security), ODUSD/P

Rowland A. Morrow, Former Director, Counterintelligence and
Investigative Programs, ODUSD/P

Peter Nelson, Security Specialist (Personnel Security), ODUSD/P

Robert Sabatini, Office of the Assistant Inspector General for
Auditing, (Consolidated CRYPTO Programs, National Security
Agency, Fort Meade)

L. Britt Snider, Principal Director, Counterintelligence and
Security Policy, ODUSD/P

Henry Winkler, Office of the Assistant Inspector General for
Auditing, (Consolidated CRYPTO Programs, National Security
Agency, Fort Meade)

DEPARTMENT OF ARMY

Don Brenno, Special Agent 902nd MI Group

Major Frank Chapuran, Technical Analysis Directorate, Ballistic Missile Defense Systems Command (BMDATC), Huntsville, Alabama

Charles K. Fendley, BMDATC-T, Huntsville, Alabama

Brigadier General Eugene Fox, Commander, BMDATC, Huntsville, Alabama

Elmer F. Hargis, Chief, Intelligence and Security Division, BMDATC, Huntsville, Alabama

Bill Johnson, Security Specialist, BMDTAC

Art Nichols, Deputy Division Chief, Operations Security Support Division, U.S. Army Intelligence and Security Command

Zane Phillips, Chief, Acquisitions Management Division, BMDTAC

Colonel Donald P. Press, Director of Counterintelligence, Assistant Chief of Staff, Intelligence

Lieutenant Colonel Joseph H. Saul, Chief, Operations Security Support Division, U.S. Army Intelligence and Security Command

Paige Stagner, Security Specialist, BMDTAC

Robert Teetz, Security Specialist, BMDTAC

Edward Vaughn, Security Specialist, BMDTAC

DEPARTMENT OF NAVY

Bob Allen, Director, Security Policy

Vincent H. DeVito, Assistant Special Security Officer, Chief of Naval Material

Captain Earl L. DeWispelaere, Assistant for Special Programs (OP-090J)

Evan G. Highley, Jr., Navy Support Systems Command

Charles A. Partridge, Navy Regional Contracting Center, Washington, D.C.

Victor J. Palmucci, Assistant Director for Counterintelligence, Naval Investigative Service Headquarters

William J. Stryker, Special Agent, Naval Investigative Service
Resident Agency, Washington, D.C.

William J. Thomas, Special Agent, Naval Investigative Service
Resident Agency, Washington, D.C.

DEPARTMENT OF AIR FORCE

Doyle Edwards, Air Force Office of Security Police, Kirtland
Air Force Base, New Mexico

Frankie J. Farris, Security Specialist, Air Force Contract
Management Division, Kirtland Air Force Base, New Mexico

Colonel Harry D. Gerber, Vice Commander, Air Force Contract
Management Division, Kirtland Air Force Base, New Mexico

Lieutenant Colonel Jerry Hoffman, Assistant Director of
Counterintelligence, Headquarters, Air Force Office of Special
Investigations

Colonel David K. Holman, Chief of Staff, Air Force Contract
Management Division, Kirtland Air Force Base, New Mexico

Lieutenant Colonel Tom Jensen, Counterintelligence Directorate,
Headquarters, Air Force Office of Special Investigations

John A. Jones, Chief of Security, Air Force Contract Management
Division, Air Force Systems Command

Colonel Jed Klingensmith, Commander, Air Force Plant
Representative Office (AFPROO), Hughes Aircraft, Los Angeles,
California

Colonel Richard F. Law, Director of Counterintelligence,
Headquarters Air Force Office of Special Investigations

George Paseur, Director of Information Security, Headquarters,
Air Force Office of Security Police, Kirtland Air Force Base,
New Mexico

Captain Kevin Petterson, Counterintelligence Directorate,
Headquarters, Air Force Office of Special Investigations

Cyndi C. Smink, Information Security Program Manager, Foreign
Disclosure Policy Officer, AFPRO Westinghouse, Baltimore,
Maryland

Brigadier General Donald J. Stukel, Commander, Air Force
Contract Management Division, Kirtland Air Force Base, New
Mexico

Colonel Richard H. Troyer, Air Force Research and Development
Quality Liaison Officer, Pentagon, Washington, D.C.

Virginia L. Valdez, Security Specialist, Air Force Contract
Management Division, Kirtland Air Force Base, New Mexico

DEPARTMENT OF ENERGY

Tom Blankenship, Chief, Security Operations Branch

A. Barry Dalinsky, Deputy Director Division of Security

Vincent McClelland, Physical Protection Branch

John Miller, Chief, Personnel Security Branch

Ernest E. Wagner, Chief, Administrative Review Section

CENTRAL INTELLIGENCE AGENCY

Seven representatives interviewed

FEDERAL BUREAU OF INVESTIGATION (FBI)

Don K. Pettus, Section Chief, CI-2, FBI Headquarters

Joseph C. Johnson, Assistant Section Chief, CI-2

Robert Opfer, Unit Chief, CI-2

NATIONAL SECURITY AGENCY

Robert Louis Benson, Chief, Management and Policy Staff, Office
of Security

John E. Dooley, Chief, Clearance Division

A. Kenneth Hanus, Chief, Industrial and Field Security

Phillip T. Pease, Director of Security

David H. Schachnovsky, Chief, Industrial Security Branch

DEFENSE INVESTIGATIVE SERVICE

Richard H. Anderson, Industrial Security Specialist

Michael L. Craig, Director of Industrial Security,
Pacific Region

Geraldine Crane, Director, Defense Industrial Security Clearance Office (DISCO)

Daniel J. Dinan, Deputy Director (Industrial Security)

Robert C. Fisher, Industrial Security Specialist

John N. Held, Regional Director, Mid-Atlantic Region

William C. Henry, Director of Industrial Security, New England Region

John G. Hoffman, Industrial Security Specialist

Everett S. Johnson, Jr., Industrial Security Specialist

Norman E. Johnson, Chief, San Francisco Industrial Security Field Office

Donald M. Kelleher, Director of Industrial Security, Capital Region

Lloyd M. Kelley, Director of Industrial Security, Southwestern Region

Donna Kimbler, Industrial Security Representative

James P. Linn, Defense Security Institute

Gordon W. Matheson, Industrial Security Representative

Donald M. McAlister, Director of Industrial Security, Mid-Western Region

Francis J. Mullan, Director of Industrial Security, Northwestern Region

Rae E. Nehls, Assistant Deputy Director (Industrial Security)

Thomas J. O'Brien, Director, Defense Investigative Service

Rodger H. Raasch, Chief, Santa Clara Industrial Security FO

Lothar K. Schulz, Industrial Security Representative

Robert G. Schwalls, Director of Industrial Security, Mid-Atlantic Region

Joseph L. Seidl, Industrial Security Specialist

William E. Stemple, Industrial Security Specialist

Joan J. Turner, Director of Industrial Security, Southeastern Region

William J. White, Industrial Security Representative

Richard F. Williams, Chief, Industrial Security Programs Division

DEFENSE TECHNICAL INFORMATION CENTER

Patricial M. Gaynor, Director of Document Services

Charles E. Gould, Deputy Director of Document Services

Ellen V. McCauley, Director of Special Projects

Robert B. Rice, Command Security Officer

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Carolyn Chewing, Program Management Office

William L. DeWeese, Director, Administrative Services Office

Jannis G. Goodwyn, Director, Program Management Office

Kaye Polzone, Special Security Officer, Administrative Office

**ATTENDEES AT DoD INDUSTRIAL SECURITY REVIEW COMMITTEE SEMINAR
AT STANFORD RESEARCH INSTITUTE, JANUARY 11, 1984**

Ray C. Averill, Manager, Plant Protection, Lockheed Missiles and Space Company

George C. Bessey, Manager, Security, ESL, Incorporated

John W. Browne, General Manager, Stanford Telecommunications, Incorporated

Bill R. Dixon, Manager, Security, Raychem Corporation

Maxine G. Eberz, Manager, Security, Argosystems, Incorporated

Clark G. Fiester, Vice President and General Manager, Sylvania Systems Group

Linda G. Fitzpatrick, Industrial Relations Manager, Raytheon Company

Phillip R. Gohr, Manager, Security, Watkins Johnson Company

Donald L. Jacobs, President, ESL, Incorporated

Julius C. Layson, Chief, Security Administration, The Boeing Company

Herbert D. Lechner, Vice President, Systems and Administration, SRI International

James W. Maneggie, Director, Security Services, Applied Technology

Janice E. Martin, Security Officer, Integrated Systems, Incorporated

Lloyd E. Martin, Chief Security Manager, Probe Systems, Incorporated

Richard M. Niemi, Manager, Security, Ford Aerospace

Richard L. Olinger, Manager, Government Security, Lockheed Missiles and Space Company

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

William H. Pretto, Manager, Security, Sylvania Systems Group

Lloyd C. Schuknecht, Director, Security Services, SRI International

Lynda L. Simon, Security Officer, Stanford Telecommunications, Incorporated

Audrey J. Smith, Corporate Security Officer, Systems Control Technology

George C. Stalker, Manager, Security, Argosystems, Incorporated

Harry W. Wilson, Vice President, Employee Relations, Applied Technology

Aerospace Industries Association of America, Incorporated,
(Industrial Security Committee) Spring Meeting--Tucson,
Arizona, May 7-9, 1984. Eighty-five representatives from
Government and private industry attended during which the
Committee made a presentation followed by a floor discussion
period.