

February 1996

DEFENSE INDUSTRIAL SECURITY

Weaknesses in U.S. Security Arrangements With Foreign-Owned Defense Contractors





United States
General Accounting Office
Washington, D.C. 20548

**National Security and
International Affairs Division**

B-265628

February 20, 1996

The Honorable Floyd Spence
Chairman
The Honorable Ronald V. Dellums
Ranking Minority Member
Committee on National Security
House of Representatives

This is an unclassified version of a classified report issued to you in 1995. This report discusses security arrangements known as voting trusts, proxy agreements, and special security agreements that are used to protect sensitive information when foreign-owned U.S. defense contractors perform on classified Department of Defense contracts. Our review was in response to a request from the former Chairman and Ranking Minority Member, Subcommittee on Oversight and Investigation, House Committee on Armed Services. In chapter 4 of this report, we recommend improvements in trustee oversight of information security and additional controls to prevent potential trustee conflicts of interest.

We are sending copies of this report to the Chairman and Ranking Minority Member, Senate Committee on Armed Services, and the Secretary of Defense. Copies will also be made available to others upon request.

Please call me at (202) 512-4587 if you or your staff have any questions concerning this report. Other major contributors to this report are listed in appendix II.

A handwritten signature in black ink that reads 'David E. Cooper'. The signature is written in a cursive, flowing style.

David E. Cooper
Associate Director,
Defense Acquisition Issues

Executive Summary

Purpose

Since the mid-1980s, development, production, and marketing of weapon systems has been increasingly internationalized through government-sponsored cooperative development programs and various kinds of industrial linkages, including international subcontracting and teaming arrangements, joint ventures, and cross-border mergers and acquisitions. Foreign companies have acquired many U.S. defense companies and have legitimate business interests in them. The U.S. government allows such foreign investment as long as it is consistent with U.S. national security interests. Some foreign-owned U.S. companies are working on highly classified defense contracts, such as the B-2, the F-117, the F-22, and military satellite programs.

The Federal Bureau of Investigation and intelligence agencies have reported that foreign intelligence activities directed at U.S. critical technologies pose a significant threat to national security. According to these agencies, some close U.S. allies are actively trying to obtain U.S. defense technologies through unauthorized means. To reduce the national security risks of foreign control over companies working on sensitive classified contracts, the Department of Defense (DOD) requires controls known as voting trusts, proxy agreements, and special security agreements (SSA).

Concerned that a major U.S. defense contractor could be acquired by foreign interests, the former Chairman and Ranking Minority Member, Subcommittee on Oversight and Investigation, House Committee on Armed Services (now the House Committee on National Security) asked GAO to review voting trusts, proxy agreements, and SSAs. GAO reviewed the structure and implementation of the agreements intended to protect classified information from unauthorized disclosure to foreign interests and to reduce the risk that foreign control could adversely affect the companies' performance of classified contracts.

Background

The government has drafted the National Industrial Security Program Operating Manual (NISPOM) to replace the DOD Industrial Security Manual and various agencies' industrial security requirements. The section dealing with foreign ownership, control, or influence contains many provisions on voting trusts, proxy agreements, and SSAs that are similar to provisions in the DOD Industrial Security Regulation (ISR). The ISR will continue to apply in its current form until it is amended to reflect the NISPOM.

The ISR and NISPOM require a company to obtain a facility clearance before it can work on a classified DOD contract. To obtain a clearance, a U.S. defense contractor that is majority foreign-owned must first accept a voting trust, proxy agreement, or SSA to insulate it from its foreign owners. With one of these agreements in place, some foreign-owned U.S. defense contractors have access to some of the most highly classified information, such as Top Secret and Sensitive Compartmented Information.¹ The Defense Investigative Service (DIS) administers DOD's Industrial Security Program and is required to conduct compliance reviews of defense contractors operating under voting trusts, proxy agreements, and SSAs.

The agreements call for (1) installing one or more foreign owner-selected, DOD-approved, cleared U.S. citizens on the company's board of directors for management oversight and (2) limiting contact between the U.S. company and representatives of its foreign owners. The trustees, proxy holders, or SSA outside directors (collectively referred to as "trustees" in this report) are to represent DOD's interests by ensuring against unauthorized access to classified information and company actions that could adversely affect performance on classified contracts. Under the ISR and the NISPOM, voting trusts and proxy agreements must provide the trustees with complete freedom to act independently from the foreign owners, and trustees are to exercise responsibility and management prerogatives for the cleared U.S. companies. ISR and NISPOM requirements for SSAs are less specific and allow a higher potential for foreign control. Normally, SSA firms are not supposed to be cleared for Top Secret, Sensitive Compartmented Information, Special Access Programs, and certain other categories of classified information. The ISR and most implementing agreements were not intended or designed to protect unclassified export-controlled information.

Results in Brief

The security arrangements GAO reviewed were not intended or designed to deny foreign owners the opportunity to pursue legitimate business with their U.S.-based companies working on classified contracts. Rather, they were designed to insulate these companies from undue foreign control and influence and to prevent foreign owners' access to classified information without a clearance and a need to know. Fifty-four companies operate under voting trusts, proxy agreements, and SSAs. GAO reviewed the controls established in 13 of these companies and a company operating under a unique security arrangement called a memorandum of agreement. The

¹Special Access Programs, Restricted Data, and Communications Security are also among the most highly classified categories of information that foreign-owned U.S. defense firms have access to on some DOD contracts.

structure and implementation of the agreements at most of the 14 companies GAO reviewed permitted some risk of foreign control, influence, and unauthorized access to classified data and technology. GAO did not determine whether unauthorized access to classified data or technology actually occurred. GAO observed the following:

- Thirty-six percent of SSA companies were granted exceptions to restrictions on their access to the most highly classified information.
- Visitation agreements permitted numerous visits, many occurring under contracts and export licenses for military and dual-use products, between the foreign owners and the U.S. defense contractor.
- Most trustees performed little oversight and, at four companies, some trustees appeared to have conflicts of interest.

Principal Findings

Through Exceptions, SSA Firms Gain Access to Otherwise Proscribed Data

The ISR and NISPOM allow each SSA to be tailored to the individual company, but SSAs have some common elements that allow foreign owners to exercise a high degree of control over the U.S. firms. For example, SSAs allow the foreign owner to have a representative (an “inside director,” often a foreign national) on the U.S. firm’s board of directors. Although inside directors do not hold a majority of votes on the board, their views about the company’s direction on certain defense contracts or product lines reflect those of the owners. In addition, unlike voting trusts and proxy agreements, most SSAs allow foreign owners to replace any member of the board of directors of the U.S. company for any reason. Under new boilerplate SSA language DOD provided to GAO, DIS will have to approve such a removal.

Because SSAs allow greater potential for foreign control than the voting trust and proxy agreement, SSA firms cannot work on Top Secret and other highly classified contracts, except when DOD determines it to be in the national interest. At the time of GAO’s review, at least 12 of the 33 SSA companies were working under exceptions to this restriction on at least 47 contracts that required access to Top Secret, Special Access, and other highly classified information.

A High Degree of Contact Occurs Under Visitation Agreements

To address the risk of foreign parent² firms' personnel gaining unauthorized access to classified information, the ISR requires each voting trust, proxy agreement, and SSA company to draw up a visitation agreement. Under the ISR, the visitation agreement is to generally restrict and limit visits between personnel of the U.S. defense contractor and its foreign parent firm, except for trustee-approved visits relating to regular day-to-day business operations pertaining to purely commercial products or services. DOD-approved visitation agreements that permitted a high number of visits pertaining to military and dual-use products and services. Often these visits occurred under approved export licenses for specific products and technologies. These licenses and a large number of contracts between the U.S. defense contractors and their foreign owners allowed considerable access to the U.S. facilities. In several cases, GAO observed hundreds of visits and long-term visits with personnel at technical and other levels of the companies.

A primary tool for trustees and DOD to monitor visitation by foreign owners' representatives is post-visit reporting. Post-visit reporting requires the individuals contacted by the foreign representatives to report the substance of the discussions that took place. With few exceptions, the contact reports GAO examined identified only the individuals involved and the title of the program they discussed, without providing any detailed information on technical discussions that may have occurred.

In 1993, DOD eliminated separate visitation agreements and included visitation controls in each voting trust, proxy agreement, and SSA. The new NISPOM does not address visitation control agreements or procedures. According to DOD, when the ISR is amended to reflect the NISPOM, it will retain a requirement for visitation approval procedures.

Little Trustee Oversight; Some Have Appearance of Conflicts of Interest

The foreign owner selects and DOD approves cleared U.S. citizens to be placed on the boards of directors of foreign-owned U.S. defense contractors to guard against undue foreign influence over company management and to ensure against unauthorized access to classified information. At a few of the 14 companies GAO reviewed, the trustees were more actively involved in company management and security oversight than at the other companies. At some companies, the trustees maintained their responsibility for approving all visits by representatives of the foreign

²The business arrangements between U.S. firms and their foreign owners may take a variety of forms, including a parent-subsidiary relationship. This report uses those terms in general way to indicate affiliation rather than as a description of the exact legal relationship between specific U.S. and foreign entities.

owners, as required in the visitation agreements. The more active trustees also interviewed a sample of technical staff who had been contacted by the foreign owners to determine the parameters of their discussions, questioned potentially adverse company business conditions caused by exclusive arrangements with the foreign parent, and attended business meetings at the company more often than quarterly. In most cases, however, the trustees delegated nearly all aspects of visitation oversight to the foreign-owned company's facility security officers, who generally lacked substantive knowledge of the company's business affairs or defense programs. Most trustees viewed their role as limited to ensuring that the company had policies designed to protect classified information and attending scheduled quarterly meetings at the company. These trustees did not actively check on the implementation of the security policies or remain engaged in company management issues. DOD security officials suggested that some trustees needed to take a more active oversight role.

GAO also found situations at four companies that had the appearance of conflicts of interest among some DOD-approved trustees. For example, at two companies under proxy agreements, DOD-approved trustees also held positions as chief executive officers at the foreign-owned companies. As proxy holders, these individuals were paid up to \$50,000 annually to protect DOD's security interests, while as chief executive officers they were paid over \$100,000 for exercising their fiduciary duty and loyalty to the foreign-owned firm. GAO observed other cases giving the appearance of conflicts of interest (see ch. 4).

Recommendations

GAO recognizes that some security vulnerabilities cannot be fully eliminated, nor would the costs and benefits warrant trying. Still, GAO's findings indicate some improvements to information security could reasonably be made at firms operating under voting trusts, proxy agreements, and SSAs. In chapter 4, GAO makes a number of recommendations to the Secretary of Defense that will improve trustee oversight of information security and recommends additional controls designed to prevent potential trustee conflicts of interest.

Agency Comments and GAO's Evaluation

In commenting on a draft of this report, DOD generally agreed with most of the report, but disagreed on some matters. For example, DOD agreed that visitation agreements give foreign owners a high degree of access to the facilities and personnel of foreign-owned U.S. defense contractors, but

stated that this access is consistent with applicable U.S. law and regulation. GAO believes such frequent contact, often at the technical and engineering levels, can increase the risk.

DOD indicated classified and export-controlled unclassified information is sufficiently protected at firms operating under SSAs. However, GAO points out that DOD established restrictions on SSA companies' access to certain levels of classified information since there is a higher degree of risk assumed under SSAs. Despite the risk of the foreign owners' control or dominance of the U.S. defense contractors' operations and management, 36 percent of SSA companies were granted exceptions to restrictions on their access to the most highly classified information.

While acknowledging that some trustees need to be more actively involved, DOD disagreed with GAO's statement that trustees at most of the companies reviewed did little to ensure that company management was not unduly influenced by the foreign owners or that the security controls were being properly implemented. As GAO noted, trustees at two firms reviewed were actively involved in company management and security oversight. However, GAO also reported that in the majority of the cases, the trustees saw their role as limited to ensuring that the company had policies to protect classified information, and their performance in this role was limited to attendance of four meetings a year. Following a 1993 survey of foreign-owned U.S. defense contractors, the Defense Intelligence Agency and DIS concluded that trustees that were the most successful in fulfilling their responsibilities were those that established procedures that allowed them to independently monitor and assess the implementation of the security agreements. They also concluded that trustees who primarily depended on management of the cleared facility to implement and monitor the security controls were less successful.

DOD stated that it generally agreed with the thrust of the recommendations in this report, but did not agree that the specific actions GAO recommended were necessary, given DOD's efforts to address the issues involved. DOD said it had addressed these issues by educating, advising, and encouraging the trustees to take corrective actions. However, DOD and GAO have both seen instances in which this encouragement has been rejected. Because of the risk to information with national security implications, GAO believes that requiring, rather than encouraging, the trustees to improve security at the cleared foreign-owned defense contractors would be more effective. Therefore, GAO continues to believe its recommendations are valid and

believes they should be implemented to reduce the security risks. (See app. I.)

Contents

Executive Summary		2
Chapter 1		12
Introduction		
	Government Required Security Controls	12
	Agreements Are Negotiated and Vary	15
	Agreements Were Not Designed to Protect Unclassified	15
	Export-Controlled Technologies	
	Fifty-Four Firms Operate Under Voting Trusts, Proxy	16
	Agreements, or SSAs	
	Objective, Scope, and Methodology	16
Chapter 2		20
Espionage Threat and		
Information at Risk		
	Information at Risk	20
	U.S. Intelligence Agencies Identified Economic Espionage Efforts	22
	of Certain Allies	
Chapter 3		27
Assessment of		
Control Structures		
	Higher Degree of Risk With SSA Structure	27
	Visitation Agreements Give Foreign Owners a High Degree of	30
	Access	
	Conclusions	33
Chapter 4		34
Assessment of		
Control		
Implementation		
	Little Involvement by Trustees in Security or Company	34
	Management Oversight	
	Foreign Owners Acted in Capacities Beyond That of Beneficiary	37
	in Proxy Firms	
	Some Foreign-Owned Firms Are Financially Dependent on	38
	Foreign Owners	
	Some Trustees Have Appearance of Conflicts of Interest	38
	DIS Inspections Did Not Focus on Foreign Ownership Issues	40
	Recommendations	41
	Agency Comments and Our Evaluation	43
Appendixes		
	Appendix I: Comments From the Department of Defense	44
	Appendix II: Major Contributors to This Report	72
Tables		
	Table 1.1: Ownership and Agreement of Companies Reviewed by	17
	GAO	

Abbreviations

CEO	Chief Executive Officer
CIA	Central Intelligence Agency
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FOCI	foreign ownership, control, or influence
FSO	facility security officer
ISR	Industrial Security Regulation
MOA	memorandum of agreement
NISPOM	National Industrial Security Program Operating Manual
SCA	security control agreement
SSA	special security agreement

Introduction

In the last decade, weapon systems have increasingly been developed, produced, and marketed internationally through government-sponsored cooperative development programs and a variety of industry linkages. These linkages include international subcontracting, joint ventures, teaming arrangements, and cross-border mergers and acquisitions. Also, the Department of Defense (DOD) and other agencies have shared certain highly classified information with allied governments. U.S. government policy allows foreign investment as long as it is consistent with national security interests. Foreign companies from many countries have acquired numerous U.S. defense companies and have legitimate business interests in them. Some of these foreign-owned companies are working on highly classified defense contracts, such as the B-2, the F-117, the F-22, and military satellite programs.

Recognizing that undue foreign control or influence over management or operations of companies working on sensitive classified contracts could compromise classified information or impede the performance of classified contracts, DOD requires that foreign-owned U.S. firms operate under control structures known as voting trusts, proxy agreements, and special security agreements (SSA). Each of these agreements requires that the foreign owners select and DOD approve cleared U.S. citizens¹ to be placed on the board of directors of the foreign-owned company to represent DOD's interests by ensuring against (1) foreign access to classified information without a clearance and a need to know and (2) company actions that could adversely affect performance on classified contracts.

Government Required Security Controls

In February 1995, the government issued the National Industrial Security Program Operating Manual (NISPOM) to replace the DOD Industrial Security Manual and various agencies' industrial security requirements. The NISPOM's section dealing with foreign ownership, control, or influence (FOCI) contains many provisions on voting trusts, proxy agreements, and SSAs similar to those in the DOD Industrial Security Regulation (ISR). The ISR will continue to apply in its current form until it is amended to reflect the NISPOM.

Both the ISR and NISPOM require a company to obtain a facility clearance before it can work on a classified DOD contract and prescribe procedures for defense contractors to protect classified information entrusted to

¹Voting trustees, proxy holders, and outside directors under SSAs are collectively referred to as "trustees" in this report.

them. DOD's policy provides that a firm is ineligible for a facility clearance if it is under FOCI. However, such a firm may be eligible for a facility clearance if actions are taken to effectively negate or reduce associated risks to an acceptable level. When the firm is majority foreign-owned, the control structures used to negate or reduce such risks include voting trusts, proxy agreements, and SSAS.

The Defense Investigative Service (DIS) administers the DOD Industrial Security Program and is required to conduct compliance reviews of defense contractors operating under voting trusts, proxy agreements, and SSAS. This oversight function requires a DIS security inspection of the cleared facility every 6 months and an annual FOCI review meeting between DIS and the trustees of the foreign-owned firm. These reviews are aimed at ensuring compliance with special controls, practices, and procedures established to insulate the facility from foreign interests.

Voting Trusts

Under a voting trust agreement, the foreign owners transfer legal title to the stock of the foreign-owned U.S. company to U.S. citizen trustees. Under the ISR and NISPOM, voting trusts must provide trustees with complete freedom to exercise all prerogatives of ownership and act independently from the foreign owners. Under the ISR and NISPOM, five actions may require prior approval by the foreign owner:

- the sale or disposal of the corporation's assets or a substantial part thereof;
- pledges, mortgages, or other encumbrances on the capital stock of the cleared company;
- corporate mergers, consolidations, or reorganization;
- the dissolution of the corporation; or
- the filing of a bankruptcy petition.

Under the ISR, the trustees were to act independently without consultation with, interference by, or influence from the foreign owners, but the NISPOM allows for consultation between the trustees and foreign owners.

Proxy Agreement

The proxy agreement is essentially the same as the voting trust, with the exception of who holds title to the stock. Under the voting trust, the title to the stock is transferred to the trustees. Under the proxy agreement, the owners retain title to the stock, but the voting rights of the stock are transferred to the DOD-approved proxy holders by a proxy agreement. The

powers and responsibilities of the proxy holders are the same as those of the trustees under a voting trust. From a security or control perspective, we saw no difference between the voting trust and the proxy agreement. DOD and company officials stated that from the companies' perspective, the difference between these two agreements is largely a tax issue.

Special Security Agreement

The third type of control structure for majority foreign-owned firms is the SSA. Unlike a voting trust or proxy agreement, the SSA allows representatives of the foreign owner to be on the U.S. contractor's board of directors. This representative, known as an inside director, does not need a DOD security clearance and can be a foreign national. In contrast, outside directors are U.S. citizens and must be approved by and obtain security clearances from DOD. Under DOD policy, outside directors are to ensure that classified information is protected from unauthorized or inadvertent access by the foreign owners and that the U.S. company's ability to perform on classified contracts is not adversely affected by foreign influence over strategic decision-making.

Because SSAs allow the foreign owners a higher potential for control over the U.S. defense contractor than proxies or voting trusts, firms operating under SSAs are generally prohibited from accessing highly classified information such as Top Secret and Sensitive Compartmented Information. However, DOD can grant exceptions to this prohibition and can award contracts at these highly classified levels if it determines it is in the national interest.

Visitation Agreement

The ISR required a visitation agreement for each voting trust, proxy agreement, or SSA. This agreement was signed by

- the foreign owners,
- the foreign-owned U.S. firm,
- the trustees, and
- DOD.

The visitation agreement was to identify the representatives of the foreign owners allowed to visit the cleared U.S. firm, the purposes for which they were allowed to visit, the advance approval that was necessary, and the identity of the approval authority. In 1993, DOD eliminated visitation agreements as separate documents and incorporated visitation control procedures as a section of each voting trust, proxy agreement, and SSA.

Agreements Are Negotiated and Vary

Voting trust agreements, proxy agreements, SSAs, and their attendant visitation agreements are negotiated between the foreign-owned company and DOD. Although DOD has boilerplate language that can be adopted, according to a DOD official, many cases have unique circumstances that call for flexible application of the ISR provisions. DOD's flexible approach leads to negotiations that can result in company-specific agreements containing provisions that provide stronger or weaker controls. Generally, the foreign owners negotiate to secure the least restrictive agreements possible.

DOD has approved more lenient visitation agreements and procedures over time. A DOD official explained that DOD's flexible approach to FOCI arrangements and the resulting negotiations have probably caused the visitation controls to become relaxed. Each negotiated visitation agreement that relaxed controls became the starting point for subsequent negotiations on new agreements as the foreign-owned companies' lawyers would point to the last visitation agreement as precedent. We recognize the need to tailor the agreements to specific company circumstances and to permit international defense work, but the lack of a baseline set of controls in the agreements made DIS inspections very difficult, according to DIS inspectors.

Agreements Were Not Designed to Protect Unclassified Export-Controlled Technologies

Almost all the foreign-owned U.S. firms we reviewed possessed unclassified information and technologies that are export-controlled by the Departments of State and Commerce. DOD deemed some of these technologies to be militarily critical, such as carbon/carbon material manufacturing technology and flight control systems technology. Many classified defense contracts involve classified applications of unclassified export-controlled items and technologies. The ISR and most agreements were not designed to protect unclassified export-controlled information. As such, DIS does not review the protection of unclassified export-controlled technology during its inspections of cleared contractors. In fact, the U.S. government has no established means to monitor compliance with and ensure enforcement of federal regulations regarding the transfer of export-controlled technical information. In light of what is known about the technology acquisition and diversion intentions of certain allies (see ch. 2) and the high degree of contact with foreign interests at foreign-owned U.S. defense contractors (see ch. 3), enforcement of export control regulations is important. The new NISPOM reflects this concern and requires trustees in future voting trusts, proxy

agreements, and SSAs to take necessary steps to ensure the company complies with U.S. export control laws.

Fifty-Four Firms Operate Under Voting Trusts, Proxy Agreements, or SSAs

As of August 1994, 54 foreign-owned U.S. defense contractors were operating under voting trusts, proxy agreements, or SSAs. Six of these companies operate under voting trusts, 15 under proxy agreements, and 33 under SSAs. These 54 firms held a total of 657 classified contracts, valued at \$5.4 billion. The largest firm operating under these agreements (as measured by the value of the classified contracts it held) is a computer services company that operates under a proxy agreement and held classified contracts valued at \$2.5 billion. The foreign owners of the 54 firms are from Australia, Austria, Canada, Denmark, France, Germany, Israel, Japan, the Netherlands, Sweden, Switzerland, and the United Kingdom. Currently, three of the companies are wholly or partially owned by foreign governments.

Objective, Scope, and Methodology

Our review was conducted at the request of the former Chairman and Ranking Minority Member, Subcommittee on Oversight and Investigation, House Committee on Armed Services (now the House Committee on National Security). Our objective was to assess the structure of voting trusts, proxy agreements, and SSAs and their implementation in the prevention of unauthorized disclosure of classified and export-controlled information to foreign interests. We did not attempt to determine whether unauthorized access to classified or export-controlled data/technology actually occurred. Rather, we examined the controls established in the ISR, the draft NISPOM, and the agreements' structures and the way they were implemented at each of 14 companies we selected to review.

We discussed security issues involving foreign-owned defense contractors and information security with officials from the Office of the Deputy Assistant Secretary of Defense (Counterintelligence, Security Countermeasures and Spectrum Management); DIS; and information security officials from the Air Force, the Army, and the Navy. We also discussed the performance of Special Access and Sensitive Compartmented contracts by foreign-owned companies with an official from the office of the Assistant Deputy Under Secretary of Defense (Security Policy). To obtain information on the threat of foreign espionage against U.S. defense industries, we interviewed officials and reviewed documents from the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), and Federal Bureau of Investigation (FBI).

In selecting the 14 companies for our judgmental sample, we included 5 companies² that were wholly or partially owned by foreign governments. We selected the nine additional foreign-owned firms on the basis of (1) the sensitivity of the information they held, (2) agreement types, (3) country of origin, and (4) geographic location. One company we reviewed operated under a voting trust, five operated under proxy agreements, and six operated under SSAs. In addition, one firm transitioned from an SSA to a proxy agreement during our review, and we found that another firm operated under a different control structure, a memorandum of agreement (MOA). Table 1.1 shows the countries of ownership and agreement type of the companies we reviewed.

Table 1.1: Ownership and Agreement of Companies Reviewed by GAO

Country of foreign ownership	Agreement type
United Kingdom	SSA
United Kingdom	SSA
Switzerland	SSA to proxy
Sweden	Proxy
France	Proxy
United Kingdom	Proxy
France	Proxy
United Kingdom	SSA
Netherlands	Voting trust
United Kingdom	SSA
France, Germany, and Italy	MOA
France	SSA
United Kingdom	Proxy
United Kingdom	SSA

This judgmental sample reflects the distribution of agreement type and country of ownership of the 54 companies operating under voting trusts, proxy agreements, and SSAs. However, due to the small size of our sample and the nonrandom nature of its selection, the results of our review cannot be projected to the universe of all companies operating under these agreements.

We were initially told that an aerospace company operated under an SSA, and selected the company for our sample based on foreign government ownership of companies that are its partial owners. We subsequently

²Two of these five companies no longer operate under SSAs. One of them was sold to American interests, and the other no longer performs on classified contracts.

learned that the company operated under a unique arrangement—an MOA . Because of the foreign government ownership component and the sensitivity of the information accessed by this aerospace company, we retained the company in our sample. When we present statistics in our report on the number of companies operating under voting trusts, proxy agreements, and SSAs and the number of contracts they hold and the contracts' value, this company is not included in those numbers.³ However, we include the company in the discussions of control structures and their implementation (see chs. 3 and 4). In those instances, we specifically refer to the MOA.

We compared the agreements of the 14 companies to each other and to boilerplate agreements provided by DIS. We also examined the agreements' provisions to determine if they met the requirements of the ISR, the regulation in force at the time. We examined the visitation approval procedures and standard practice procedures manuals at the companies we reviewed to determine how the companies controlled foreign visitors and their access to the cleared facilities. We also interviewed company management, security personnel, and the company trustees to determine how they implemented the agreements. To assess implementation of the agreements, we reviewed annual company implementation reports, board of directors minutes, defense security committee minutes, visitation logs, international telephone bills, and various internal company correspondence and memorandums. To assess trustee involvement, we interviewed trustees and reviewed visitation approvals, as well as trustee meeting minutes, which showed the frequency of meetings, individuals' attendance records, and topics of discussion. We also discussed each company's implementation of the agreements and its information security programs with the cognizant DIS regional management and inspectors and reviewed their inspection reports.

Access Limitation

During our review, we had limited access to certain information. Foreign-owned contractors were working on various contracts and programs classified as Special Access Programs or Sensitive Compartmented Information. We were told by an official from the Office of the Assistant Deputy Under Secretary of Defense (Security Policy) that in some instances, it is not possible to acknowledge the existence of such contracts to individuals who are not specifically cleared for the program.

³At the time of our review, the aerospace company operating under an MOA held 10 classified contracts valued at approximately \$1.0 billion.

As a result, we may not know of all foreign-owned firms involved in highly classified work.

DOD provided written comments on a draft of this report. The complete text of those comments and our response is presented in appendix I. We performed our review from August 1992 through February 1995 in accordance with generally accepted government auditing standards.

Espionage Threat and Information at Risk

Some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means. Through its National Security Threat List program, the FBI National Security Division has determined that foreign intelligence activities directed at U.S. critical technologies pose a significant threat to national security. As we testified before the House Committee on the Judiciary in April 1992, sophisticated methods are used in espionage against U.S. companies.¹ Unfortunately, the companies targeted by foreign intelligence agencies may not know—and may never know—that they have been targeted or compromised.

The Joint Security Commission was formed in 1993 at the request of the Secretary of Defense and the Director of Central Intelligence to develop new approaches to security. The Commission examined (1) policies and procedures regarding foreign ownership or control of industrial firms performing classified contracts and (2) the national disclosure of classified information to permit export and coproduction of classified weapon systems. In its February 1994 report, the Commission wrote the following:

“The risk in each of these situations is that foreign entities will exploit the relationship in ways that do not serve our overall national goals of preserving our technological advantages and curtailing proliferation. These goals generally include keeping certain nations from obtaining the technical capabilities to develop and produce advanced weapon systems and from acquiring the ability to counter advanced US weapon systems. In cases where U.S. national interests require the sharing of some of our capabilities with foreign governments, security safeguards must ensure that foreign disclosures do not go beyond their authorized scope. Safeguards must also be tailored to new proliferation threats and applied effectively to the authorization of foreign investment in classified defense industry and the granting of access by foreign representatives to our classified facilities and information.”

Contractors owned by companies and governments of these same allied countries are working on classified DOD contracts under the protection of voting trusts, proxy agreements, and SSAs. These companies perform on DOD contracts developing, producing, and maintaining very sensitive military systems, and some of them have access to the most sensitive categories of U.S. classified information.

Information at Risk

Contracts requiring access to classified information at the levels shown in table 2.1 have been awarded to foreign-owned U.S. defense contractors.

¹Economic Espionage: The Threat to U.S. Industry (GAO/T-OSI-92-6, Apr. 29, 1992).

Table 2.1: Levels of Classified Information

Acronym	Classification
C	CONFIDENTIAL: Information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.
S	SECRET: Information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to national security.
TS	TOP SECRET: Information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.
SAP	SPECIAL ACCESS PROGRAM: Program imposing “need-to-know” or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information.
WNINTEL	WARNING NOTICE - INTELLIGENCE SOURCES AND METHODS INVOLVED
SCI	SENSITIVE COMPARTMENTED INFORMATION: Information bearing special controls indicating restricted handling within present and future intelligence collection programs and their end products.
RD	RESTRICTED DATA: Information concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy.
FRD	FORMERLY RESTRICTED DATA: Information removed from the Restricted Data category upon joint determination by the Department of Energy and DOD. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.
CNWDI	CRITICAL NUCLEAR WEAPON DESIGN INFORMATION: Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device.
COMSEC	COMMUNICATIONS SECURITY: Information concerning protective measures taken to deny unauthorized persons information derived from telecommunications related to national security and to ensure the authenticity of such communication.
NOFORN	NOT RELEASABLE TO FOREIGN NATIONALS

The following are examples of some sensitive contract work being performed by the 14 foreign-owned U.S. companies we reviewed:

- development of computer software for planning target selection and aircraft routes in the event of a nuclear war (a Top Secret contract);
- maintenance of DOD’s Worldwide Military Command and Control System ((WWMCCS) - the contract was classified TS, SCI, and COMSEC because of the information the computer-driven communications system contains);
- production of signal intelligence gathering radio receivers for the U.S. Navy;
- production of command destruct receivers for military missiles and National Aeronautics and Space Administration rockets (to destroy a rocket that goes off course);
- production of carbon/carbon composite Trident D-5 missile heat shields; and
- production of the flight controls for the B-2, the F-117, and the F-22.

Some of the contracts these foreign-owned U.S. companies are working on are Special Access Programs. Due to the special access requirements of these contracts, the contractors could not tell us what type of work they were doing, what military system the work was for, or even the identity of the DOD customer.

Some of the contracts performed by companies we examined involve less sensitive technologies. For example, one company we visited had contracts requiring access to classified information because it cast valves for naval nuclear propulsion systems, and it needed classified test parameters for the valves. Another firm operating under an SSA is required to have a Secret-level clearance because it installs alarm systems in buildings that hold classified information.

In addition to classified information, most of the 14 foreign-owned companies we reviewed possessed unclassified technical information and hardware items that are export-controlled by the State or Commerce Departments. DOD deemed many of these technologies to be militarily critical.

U.S. Intelligence Agencies Identified Economic Espionage Efforts of Certain Allies

Reports and briefings provided during 1993 by U.S. intelligence agencies showed a continuing economic espionage threat from certain U.S. allies.² Eight of the 54 companies operating under voting trusts, proxy agreements, and SSAs and working on classified contracts are owned by interests from one of these countries. The following are intelligence agency threat assessments and examples illustrating this espionage.

Country A

According to a U.S. intelligence agency, the government of Country A conducts the most aggressive espionage operation against the United States of any U.S. ally. Classified military information and sensitive military technologies are high-priority targets for the intelligence agencies of this country. Country A seeks this information for three reasons: (1) to help the technological development of its own defense industrial base, (2) to sell or trade the information with other countries for economic reasons, and (3) to sell or trade the information with other countries to

²“Economic espionage” was defined in a 1994 U.S. government interagency report as “government-sponsored or coordinated intelligence activity designed to unlawfully and covertly obtain classified data and/or sensitive policy or proprietary information from a U.S. Government agency or company, potentially having the effect of enhancing a foreign country’s economic competitiveness and damaging U.S. economic security.”

develop political alliances and alternative sources of arms. According to a classified 1994 report produced by a U.S. government interagency working group on U.S. critical technology companies,³ Country A routinely resorts to state-sponsored espionage using covert collection techniques to obtain sensitive U.S. economic information and technology. Agents of Country A collect a variety of classified and proprietary information through observation, elicitation, and theft.

The following are intelligence agency examples of Country A information collection efforts:

- An espionage operation run by the intelligence organization responsible for collecting scientific and technologic information for Country A paid a U.S. government employee to obtain U.S. classified military intelligence documents.
- Several citizens of Country A were caught in the United States stealing sensitive technology used in manufacturing artillery gun tubes.
- Agents of Country A allegedly stole design plans for a classified reconnaissance system from a U.S. company and gave them to a defense contractor from Country A.
- A company from Country A is suspected of surreptitiously monitoring a DOD telecommunications system to obtain classified information for Country A intelligence.
- Citizens of Country A were investigated for allegations of passing advanced aerospace design technology to unauthorized scientists and researchers.
- Country A is suspected of targeting U.S. avionics, missile telemetry and testing data, and aircraft communication systems for intelligence operations.
- It has been determined that Country A targeted specialized software that is used to store data in friendly aircraft warning systems.
- Country A has targeted information on advanced materials and coatings for collection. A Country A government agency allegedly obtained information regarding a chemical finish used on missile reentry vehicles from a U.S. person.

Country B

According to intelligence agencies, in the 1960s, the government of Country B began an aggressive and massive espionage effort against the United States. The 1994 interagency report on U.S. critical technology

³Report on U.S. Critical Technology Companies, Report to Congress on Foreign Acquisition of and Espionage Activities Against U.S. Critical Technology Companies (1994).

companies pointed out that recent international developments have increased foreign intelligence collection efforts against U.S. economic interests. The lessening of East-West tensions in the late 1980s and early 1990s enabled Country B intelligence services to allocate greater resources to collect sensitive U.S. economic information and technology.

Methods used by Country B are updated versions of classic Cold War recruitment and technical operations. The Country B government organization that conducts these activities does not target U.S. national defense information such as war plans, but rather seeks U.S. technology. The motivation for these activities is the health of Country B's defense industrial base. Country B considers it vital to its national security to be self-sufficient in manufacturing arms. Since domestic consumption will not support its defense industries, Country B must export arms. Country B seeks U.S. defense technologies to incorporate into domestically produced systems. By stealing the technology from the United States, Country B can have cutting-edge weapon systems without the cost of research and development. The cutting-edge technologies not only provide superior weapon systems for Country B's own use, but also make these products more marketable for exports. It is believed that Country B espionage efforts against the U.S. defense industries will continue and may increase. Country B needs the cutting-edge technologies to compete with U.S. systems in the international arms market.

The following are intelligence agency examples of Country B information collection efforts:

- In the late 1980s, Country B's intelligence agency recruited agents at the European offices of three U.S. computer and electronics firms. The agents apparently were stealing unusually sensitive technical information for a struggling Country B company. This Country B company also owns a U.S. company operating under a proxy agreement and performing contracts for DOD classified as TS, SAP, SCI, and COMSEC.
- Country B companies and government officials have been investigated for suspected efforts to acquire advanced abrasive technology and stealth-related coatings.
- Country B representatives have been investigated for targeting software that performs high-speed, real-time computational analysis that can be used in a missile attack system.
- Information was obtained that Country B targeted a number of U.S. defense companies and their missile and satellite technologies for

espionage efforts. Companies of Country B have made efforts, some successful, to acquire targeted companies.

Country C

The motivation for Country C industrial espionage against the United States is much like that of Country B: Country C wants cutting-edge technologies to incorporate into weapon systems it produces. The technology would give Country C armed forces a quality weapon and would increase the weapon's export market potential. The Country C government intelligence organization has assisted Country C industry in obtaining defense technologies, but not as actively as Country B intelligence has for its industry. One example of Country C government assistance occurred in the late 1980s, when a Country C firm wanted to enter Strategic Defense Initiative work. At that time, the Country C intelligence organization assisted this firm in obtaining applicable technology.

Country D

The Country D government has no official foreign intelligence service. Private Country D companies are the intelligence gatherers. They have more of a presence throughout the world than the Country D government. However, according to the 1994 interagency report, the Country D government obtains much of the economic intelligence that Country D private-sector firms operating abroad collect for their own purposes. This occasionally includes classified foreign government documents and corporate proprietary data. Country D employees have been quite successful in developing and exploiting Americans who have access to classified and proprietary information.

The following are examples of information collection efforts of Country D:

- Firms from Country D have been investigated for targeting advanced propulsion technologies, from slush-hydrogen fuel to torpedo target motors, and attempting to export these items through intermediaries and specialty shipping companies in violation of export restrictions.
- Individuals from Country D have been investigated for allegedly passing advanced aerospace design technology to unauthorized scientists and researchers.
- Electronics firms from Country D directed information-gathering efforts at competing U.S. firms in order to increase the market share of Country D in the semiconductor field.

Country E

Intelligence community officials stated that they did not have indications that the intelligence service of Country E has targeted the United States or its defense industry for espionage efforts. However, according to the 1994 interagency report, in 1991 the intelligence service of this country was considering moving toward what it called “semi-overt” collection of foreign economic intelligence. At that time, Country E’s intelligence service reportedly planned to increase the number of its senior officers in Washington to improve its semi-overt collection—probably referring to more intense elicitation from government and business contacts.

The main counterintelligence concern cited by one intelligence agency regarding Country E is not that its government may be targeting the United States with espionage efforts, but that any technology that does find its way into Country E will probably be diverted to countries to which the United States would not sell its defense technologies. The defense industry of this country is of particular concern in this regard.

It was reported that information diversions from Country E have serious implications for U.S. national security. Large-scale losses of technology were discovered in the early 1990s. Primary responsibility for industrial security resides in a small staff of the government of Country E. It was reported that this limited staff often loses when its regulatory concerns clash with business interests. The intelligence agency concluded that the additional time needed to eradicate the diversion systems will consequently limit the degree of technological security available for several years. The question suggested by this situation is, if technology from a U.S. defense contractor owned by interests of Country E is transferred to Country E, will this U.S. defense technology then be diverted to countries to which the United States would not sell?

Assessment of Control Structures

Foreign ownership or control of U.S. firms performing classified contracts for DOD poses a special security risk. The risk includes unauthorized or inadvertent disclosure of classified information available to the U.S. firm. In addition, foreign owners could take action that would jeopardize the performance of classified contracts. To minimize the risks, the ISR and NISPOM require voting trusts and proxy agreements to insulate the foreign owners from the cleared U.S. defense firm or SSAs to limit foreign owners' participation in the management of the cleared U.S. firm. The ISR also required visitation agreements to control visitation between foreign owners and their cleared U.S. firms. The new industrial security program manual does not address visitation control agreements or procedures. DOD eliminated separate visitation agreements in favor of visitation procedures in the security agreements themselves.

In May 1992, a former Secretary of Defense testified before the House Committee on Armed Services that under proxy agreements and voting trusts, the foreign owners of U.S. companies working on classified contracts had "virtually no say except if somebody wants to sell the company or in very major decisions." He indicated that for the purposes of the foreign parent company, proxy agreements and voting trusts are essentially "blind trusts." Further, he testified that a number of companies were "functioning successfully" under SSAs.

Of the three types of arrangements used to negate or reduce risks in majority foreign ownership cases, SSAs were the least restrictive. Accordingly, SSA firms pose a somewhat higher risk associated with classified work. The ISR and the NISPOM generally prohibit SSA firms from being involved in Top Secret and other highly sensitive contracts, but allow for exceptions if DOD determines they are in the national interest. SSA firms we reviewed were working on 47 contracts classified as TS, SCI, SAP, RD, and COMSEC. In addition, we observed that ISR-required visitation agreements permitted significant contact between the U.S. firms and the foreign owners.

Higher Degree of Risk With SSA Structure

Unlike voting trusts and proxy agreements, which insulate foreign owners from the management of the cleared firm, SSAs allow foreign owners to appoint a representative to serve on the board of directors. Called an "inside director," this individual represents the foreign owners and is often a foreign national. The inside director is to be counterbalanced by DOD-approved directors, called the "outside directors." The principal function of the outside directors is to protect U.S. security interests.

Inside directors cannot hold a majority of the votes on the board, but because of their connection to the foreign owners, their views about the company's direction on certain defense contracts or product lines reflect those of the owners. Depending on the composition of the board, the inside director and the company officers on the board could possibly combine to out vote the outside directors. In addition, unlike voting trusts and proxy agreements, the SSAs we examined allow the foreign owner to replace "any member of the [SSA company] Board of Directors for any reason." DOD recently provided us with new boilerplate SSA language that will require DIS to approve the removal of a director.

Foreign owners of SSA firms can also exercise significant influence over the U.S. companies they own in other ways. For example, at two SSA firms we examined, the foreign owners used export licenses to obtain unclassified technology from the U.S. subsidiary that was vital to the U.S. companies' competitive positions. Officers of the U.S. companies stated that they did not want to share these technologies, but the foreign owners required them to do so. Subsequently, one of these U.S. companies faced its own technology in a competition with its foreign owner for a U.S. Army contract.

SSA Firms Working on Contracts Requiring Access to Top Secret, Special Access, and Other Sensitive Information

Because of the additional risk previously mentioned, companies operating under SSAs are normally ineligible for contracts allowing access to TS, SAP, SCI, RD, and COMSEC information. However, during our review, 12 of the 33 SSA companies were working on at least 47 contracts requiring access to this highly classified information.

Before June 1991, DOD reviewed an SSA firm to determine whether it would be in the national interest to allow the firm to compete for contracts classified TS, SCI, SAP, RD, or COMSEC. New guidance was issued in June 1991 requiring the responsible military service to make a national interest determination each time a highly classified contract was awarded to an SSA firm. We found only one contract-specific national interest determination had been written since the June 1991 guidance. According to DOD officials, the other 46 highly classified contracts performed by SSA companies predated June 1991 or were follow-on contracts to contracts awarded before June 1991. Since information on some contracts awarded to SSA companies is under special access restrictions, DOD officials may be authorized to conceal the contracts from people not specifically cleared for access to the program. We, therefore, could not determine with

confidence if the requirement for contract-specific national interest determinations was carried out.

One Company Operates Under an Alternative Agreement

One company performs on contracts classified as TS, SCI, SAP, RD, and COMSEC under an alternative arrangement called an MOA. The MOA (a unique agreement) was created in 1991 because the company has classified DOD contracts and, although foreign interests do not hold a majority of the stock, they own 49 percent of the company and have special rights to veto certain actions of the majority owners.

Normally, under the ISR, minority foreign investment in a cleared U.S. defense contractor required only a resolution of the board of directors stating that the foreign interests will not require, nor be given, access to classified information. DOD did not consider the board resolution appropriate for this case, partially because of the board membership of the foreign owners and their veto rights over certain basic corporate decisions. The company board of directors consists of six representatives appointed by the U.S. owners and one representative for each of the four foreign minority interests. Any single foreign director can block any of 16 specified actions of the board of directors. These actions include the adoption of a company strategic plan or annual budget as well as the development of a new product that varies from the lines of business set forth in the strategic plan. In addition, any two foreign directors can block an additional 11 specified actions. These veto rights could give the foreign interests significantly more control and influence over the U.S. defense contractor in certain instances than would be permitted in an SSA. In 1991, DIS objected to an agreement less stringent than an SSA because of the veto rights of the foreign directors and, unlike an SSA, an MOA does not require any DOD-approved outside members on the board of directors. However, the Office of the Under Secretary of Defense for Policy determined that the company would not be under foreign domination and that the MOA was a sufficient control.

DOD reexamined the MOA during a subsequent (1992) foreign investment in the company and made some modifications. Although the MOA does not provide for outside members on the board, it does require DOD-approved outside members on a Defense Security Committee to oversee the protection of classified and export-controlled information. The first version of the MOA did not give the outside security committee members the right to attend any board of directors meetings. Under the revised (1992) version of the MOA, the outside security committee members still do

not have general rights to attend board meetings; however, their attendance at board meetings is required if the foreign interests are to exercise their veto rights. Also, the first version of the MOA did not require any prior security committee approval for representatives of the foreign interests to visit the cleared U.S. defense contractor. The newer version requires prior approval when the visits concern performance on a classified contract.¹

Visitation Agreements Give Foreign Owners a High Degree of Access

Unlike the new NISPOM, the ISR required the foreign owners of a cleared U.S. defense contractor to be segregated from all aspects of the U.S. company's defense work. The ISR provided the following:

"In every case where a voting trust agreement, proxy agreement, or special security agreement is employed to eliminate risks associated with foreign ownership, a visitation agreement shall be executed . . ."

Further:

"The visitation agreement shall provide that, as a general rule, visits between the foreign stockholder and the cleared U.S. firm are not authorized; however, as an exception to the general rule, the trustees, may approve such visits in connection with regular day-to-day business operations pertaining strictly to purely commercial products or services and not involving classified contracts."

The visitation agreements are to guard against foreign owners or their representatives obtaining access to classified information without a clearance and a need to know.

At all 14 companies we reviewed, visitation agreements permitted the foreign owners and their representatives to visit regarding military and dual-use products and services. The visitation agreements permitted visits to the U.S. company (1) in association with classified contracts if the foreign interests had the appropriate security clearance and (2) under State or Commerce Department export licenses.

The large number of business transactions between the U.S. defense contractors and their foreign owners granted representatives of the foreign owners frequent entry to the cleared U.S. facilities. Eight of the

¹The 1995 NISPOM now requires a Security Control Agreement (SCA) in cases where minority foreign owners are represented on the board of directors. The SCA is more stringent in some respects than the MOA, and is essentially an SSA for cases of minority foreign investment. For example, the SCA requires that outside directors be placed on the company's board of directors.

14 firms we reviewed had contractual arrangements with their foreign owners that led to a high (often daily) degree of contact. In one case, the U.S. company sold and serviced equipment produced by the foreign firm, so the two firms had almost continual contact at the technician level to obtain repair parts and technical assistance. During a 3-month period in 1993, this company approved 167 extended visit authorizations.

At one SSA firm we reviewed, 236 visits occurred between the U.S. firm and representatives of the foreign owners over a 1-year period, averaging about 7 days per visit. At a proxy company, there were 322 approved requests for contact with representatives of the owners during a 1-year period; 94 of the requests were blanket requests for multiple contacts over the subsequent 3-month period. Not all foreign-owned defense contractors had this degree of contact with representatives of their foreign owners. One SSA firm had only 44 visits with representatives of its foreign owners during a 1-year period.

Some visitation agreements permitted long-term visits to the cleared U.S. companies by employees of the foreign owners. Five companies we reviewed had employees of the foreign owners working at the cleared U.S. facilities. In a number of these cases, they were technical and managerial staff working on military and dual-use systems and products under approved export licenses. One company covered by a proxy agreement had a foreign national technical manager from the foreign parent firm review the space and military technologies of the U.S. defense contractor to determine if there were opportunities for technical cooperation with the foreign parent firm. At another firm we reviewed, representatives of the foreign partners are permanently on site. At yet another company, a foreign national employee of the foreign parent company worked on a computer system for the B-2 bomber and had access to export-controlled information without the U.S. company obtaining the required export license.

Lack of Post-Visit Reporting Requirements

Post-visit contact reports are the primary means for DIS and the trustees to monitor the substance of contacts between the foreign-owned U.S. contractor and representatives of its foreign owners. Such records should be used to determine if the contact with representatives of the foreign owners was appropriate and in accordance with the ISR and the visitation agreement. Some visitation agreements do not require employees of the U.S. firm to document and report the substance of the discussions with employees of the foreign parent firm. At three of the firms we reviewed,

the only record of contact between employees of the U.S. company and the foreign owners were copies of forms approving the visit. However, at other foreign-owned U.S. defense contractors, post-visit contact reports were available for DIS to review when it inspected the firms and when DIS held its annual agreement compliance review with the foreign-owned companies.

Telephonic Contacts Not Controlled

The ISR, the NISPOM, and most of the visitation agreements we reviewed do not require telephonic contacts between the U.S. defense contractor and representatives of its foreign owners to be controlled and documented. One of the firms covered by a proxy agreement documented 1,912 telephonic contacts between the U.S. company and representatives of its foreign owners for a 1-year period. After examining telephone bills at other companies, we found 1 SSA company had over 550 telephone calls to the country of the foreign owners in 1 month. Company officials said these calls were primarily to representatives of the foreign owners. In contrast, our review of telephone bills at another SSA company showed only 47 telephone calls to the country of the foreign owners during 1 month in 1993.

If an individual intends to breach security, it would be easier to transfer classified or export-controlled information by telephone, facsimile, or computer modem than it would be in person. Documenting telephone contacts would not prevent such illegal activity, but might make it easier to detect. During our review, DIS also recognized this and asked companies to establish a procedure for documenting telephonic contacts with representatives of their foreign owners.

National Industrial Security Manual Has No Requirement for Visitation Agreements

We were initially told the NISPOM section dealing with foreign ownership, control, and influence would replace the FOCI section of the ISR. The new manual does not address visitation control agreements or procedures to restrict visitation between the cleared U.S. defense contractor and representatives of its foreign owners. Instead, it appears to allow unlimited visitation. However, in its comments on our report, DOD stated that the ISR will be retained and revised to reflect the NISPOM. DOD also said that the revised ISR will require visitation approval procedures, but instead of separate visitation agreements, these procedures will be incorporated into each voting trust, proxy agreement, and SSA.

Conclusions

Under the ISR and the new NISPOM, majority foreign-owned facilities cleared to perform classified contracts must enter into agreements with DOD to negate, or at least reduce to an acceptable level, the security risks associated with foreign ownership, control, and influence. Voting trusts and proxy agreements are designed to insulate cleared U.S. defense firms from their foreign owners. SSAs limit the foreign owners' participation in company management. None of these security arrangements is intended to deny U.S. defense contractors the opportunity to do business with their foreign owners. However, the frequent contact engendered by legitimate unclassified business transactions can heighten the risk of unauthorized access to classified information. Also, existing visitation agreements and procedures permit a high degree of contact. Often this contact is at the technical and engineer level where U.S. classified information could most easily be compromised. The draft NISPOM does not address visitation controls, but DOD has stated that a visitation approval procedures section will be included in the revised ISR.

Assessment of Control Implementation

At a few of the 14 companies we reviewed, DOD-approved trustees were actively involved in company management and security oversight. At most of the companies, however, the trustees did little to protect classified or export-controlled information from access by foreign owner representatives. At proxy agreement companies, we observed cases where foreign owners were exercising more control than the ISR allowed and foreign-owned U.S. defense firms whose independence was degraded because of their financial reliance on the foreign owners. We also observed that some DOD-approved trustees appeared to have conflicts of interest. Finally, DIS did not tailor its inspections of these foreign-owned facilities to specifically address FOCI issues or the implementation of the control agreements, but has recently promulgated new inspection guidelines to address these issues.

Little Involvement by Trustees in Security or Company Management Oversight

Some DOD-approved trustees were more actively involved in management and security oversight than others. For example, at some companies, the trustees retained, and did not delegate, their responsibility for approving all visits by representatives of the foreign owners as required in the visitation agreements. The more active trustees also reviewed post-visit contact reports and interviewed a sample of technical staff who met with the foreign owners' representatives to ascertain the substance of their discussions, questioned potentially adverse business conditions caused by arrangements with the foreign parent, and attended business meetings at the company more often than quarterly.

At most of the companies we reviewed, however, the trustees (or proxy holders or outside directors) did little to ensure that company management was not unduly influenced by the foreign owners or that the control structures in the security agreements were being properly implemented. Instead, they viewed their role as limited to ensuring that policies exist within the company to protect classified information. At six of the firms we reviewed, monitoring the security implementation and the business operations of the company by the trustees ranged from limited to almost nonexistent. In only two of the firms did the trustees appear to be actively involved in company management and security oversight.

The need for trustee oversight of the business management of foreign-owned companies was highlighted at one SSA firm we examined. At this company, the foreign owners exercised their SSA powers to replace two successive director/presidents of the U.S. company. The first claimed he was terminated because he attempted to enforce the SSA. The second

president contested his dismissal because the outside directors were not given prior notice of the owners' intent to replace him. The owners stated that in both cases, poor business performance was the cause for termination and, in these cases, the outside directors agreed. Nevertheless, outside directors need to remain actively involved in monitoring the companies' business management to ensure that foreign owners exercise these powers only for legitimate business reasons and not for reasons that could jeopardize classified information and contracts.

Implementation and monitoring of the information security program was usually left to the facility security officer (FSO), an employee of the foreign-owned U.S. company. At the companies we reviewed, a variety of personnel served as FSO, including a general counsel, secretaries, and professional security officers. In any case, the FSO often performed the administrative functions of security and lacked the knowledge to determine the proper parameters for the substance of classified discussions, given a cleared foreign representative's need to know. This limitation and the FSO's potential vulnerability as an employee of the foreign-owned company pose a risk without active trustee involvement.

Another potential problem associated with trustees relinquishing implementation and monitoring responsibilities to the FSO was illustrated at an SSA firm we reviewed. At the SSA firm, the FSO wanted to establish a new security procedure, but was overruled by the president of the foreign-owned U.S. defense company. In this instance, the FSO had enough confidence in the outside directors to go to them and complain. The outside directors agreed with the need for the new control and required its implementation. In this case, the outside directors led the officials of the foreign-owned firm to believe that the new security measure was an outside director initiative. If the circumstances and individuals had been different, the FSO might have lacked the confidence to seek the assistance of the outside directors.

At the foreign-owned companies we reviewed, trustees were paid between \$1,500 and \$75,000 a year. In return for this compensation, the usual trustee involvement was attendance at four meetings annually. Typically, one of the trustees is designated to approve requests for visits with representatives of the foreign owners. This additional duty involves occasionally receiving, reviewing, and transmitting approval requests by facsimile machine.

The ISR requires that a trustee approve visitation requests. However, in most of the firms we reviewed, trustees only directly approved visits between senior management of the U.S. firm and the foreign parent firm. The FSO approved visits below this senior management level, including visits with the technical and engineering staff; the trustees only reviewed documentation of these visits during their quarterly trustee meetings, if at all. In addition, when required, most post-visit contact reports lacked the detail needed for the trustees or DIS to determine what was discussed between the foreign-owned company and the owners' representatives. Trustee inattention to contact at the technical level is of particular concern, since that is where most of the U.S. defense contractor's technology is located, not in the board room where senior management officials are found.

Trustees rarely visited or toured the foreign-owned company's facility to observe the accessibility of classified or export-controlled information, except during prearranged tours at the time of their quarterly meetings. The trustees also rarely interviewed managerial and technical staff to verify the level and nature of their contact with employees of the foreign parent firm. Government officials suggested that trustees at two companies involve themselves in a higher degree of monitoring. Some flatly refused and stated that they have held important positions in government and industry and feel that it is not their role to personally provide such detailed oversight.

The ISR requires that proxy holders and trustees of voting trusts "shall assume full responsibility for the voting stock and for exercising all management prerogatives relating thereto" and that the foreign stockholders shall "continue solely in the status of beneficiaries." However, as an example of minimal proxy involvement, at one proxy company the three proxy holders only met twice a year. Only one of the three proxy holders was on the company's board of directors, and the board had not met in person for 4 years. All board action was by telephone, and the board's role was limited to electing company officers. The proxy holders' were minimally involved in selecting and approving these company officials. The parent firm selected the current chief executive officer (CEO) of the company and the proxy holders affirmed this selection after questioning the parent firm about the individual's background. The FSO was required to approve all visits to this firm by employees of the foreign parent rather than the proxy holders as required by the ISR.

At the company we reviewed operating under an MOA, the Defense Security Committee consists of four company officials and the three outside members. These outside members visited the company only for the quarterly committee meetings. The president of the company, who is also the security committee chairman, set the meeting agenda and conducted the meetings. Further, his presentations to the outside members usually focused on current and future business activities rather than security matters. Any plant tours the outside members received were prearranged and concurrent with the quarterly meetings. There were no off-cycle visits to the company to inspect or monitor security operations.

Foreign Owners Acted in Capacities Beyond That of Beneficiary in Proxy Firms

To eliminate the risks associated with foreign control and influence over foreign-owned U.S. defense contractors, the ISR requires that voting trust and proxy agreements “unequivocally shall provide for the exercise of all prerogatives of ownership by the trustees with complete freedom to act independently without consultation with, interference by, or influence from foreign stockholders.”

Further,

“the trustees shall assume full responsibility for the voting stock and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign stockholders, except for the approvals just enumerated, [sale, merger, dissolution of the company; encumbrance of stock; filing for bankruptcy] shall be insulated from the cleared facility and continue solely in the status of beneficiaries.”

However, at one of the proxy firms we reviewed, the foreign owners acted in more than the status of beneficiaries. The proxy firm’s strategic plan and annual budget were regularly presented to the foreign owners for review. At least once the foreign parent firm rejected a strategic plan and indicated that it would continue to object until the plan specified increased collaboration between the proxy firm and the foreign parent firm. At another time, the foreign owners had employees of this U.S. firm represent them in an attempt to acquire another U.S. aerospace firm more than 10 times the size of the proxy firm. Although decisions on mergers are within the rights of the foreign owners, during this acquisition effort, officers and employees of the U.S. defense contractor were operating at the direction of the foreign owners. In this case, because the parent firm directed staff of the proxy firm, it clearly acted as more than a beneficiary, the role to which foreign owners are limited under the ISR.

Another proxy firm has a distribution agreement with its foreign owners that restricts the proxy firm to marketing electronic equipment and services to the U.S. government. In addition, the agreement will only allow the proxy firm to service hardware that is used on classified systems. Although this distribution agreement was approved by DIS at the time of the foreign acquisition, it controls the strategic direction of the proxy firm. The proxy firm reported to DIS that it is important for the survival of the U.S. company to be able to pursue business opportunities that are currently denied by the distribution agreement.

Some Foreign-Owned Firms Are Financially Dependent on Foreign Owners

The ISR states that a company operating under a proxy agreement “shall be organized, structured, and financed so as to be capable of operating as a viable business entity independent from the foreign stockholders.” During our review, we saw examples of firms that depended on their foreign owners for financial support or had business arrangements with the foreign owners that degraded the independence of the proxy firm.

The president of one company operating under a proxy agreement told us that his company was basically bankrupt. His company is financed by banks owned by the government where the parent company is incorporated. The company’s foreign parent firm guarantees the loans, and two of the government banks are on the parent firm’s board of directors. The foreign owners paid several million dollars to the U.S. company to relocate one of its divisions. According to officials of the U.S. company, they could not otherwise have afforded such a move, nor could they have obtained bank loans on their own.

Another proxy firm had loans from the foreign owners that grew to exceed the value of the proxy firm. One proxy holder said the company would probably have gone out of business without the loans. Even with the loans, the company’s financial position was precarious. It was financially weak, could not obtain independent financing, and was considerably burdened by making interest payments on its debt to the foreign owners. During our review, a DIS official acknowledged that DIS should have addressed the risk imposed by this indebtedness.

Some Trustees Have Appearance of Conflicts of Interest

Under the ISR provisions, voting trustees and proxy holders “shall be completely disinterested individuals with no prior involvement with either the facility or the corporate body in which it is located, or the foreign interest.” At one of the companies we reviewed, a proxy holder was

previously involved as a director of a joint venture with the foreign owners. These foreign owners later nominated this individual to be their proxy holder. He withheld the information about his prior involvement from DIS at the time he became a proxy holder. After DIS became aware of this relationship, it concluded that this individual was ineligible to be a proxy holder and should not continue in that role. Thereafter, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence wrote to the company about irregularities in proxy agreement implementation, such as allowing the foreign owners prerogatives that were not allowed under the proxy agreement. However, he did not address the appearance of a conflict of interest, and the individual has remained as a proxy holder.

This same proxy holder is also now the part-time CEO of the foreign-owned U.S. defense firm and received an annual compensation of approximately \$272,000 (as compared to the \$50,000 proxy holder stipend) for an average of 8 days' work per month in his dual role of CEO and proxy holder. This appears to be a second conflict of interest: as CEO his fiduciary duty and loyalty to the foreign-owned company takes primacy; as proxy holder, his primary responsibility is to protect DOD's information security interests.

In addition, at this company, the conflict between the proxy holders' responsibility to DOD and their perceived fiduciary responsibility was illustrated during a DIS investigation into possible violations of the proxy agreement. Citing their fiduciary responsibility, the proxy holders refused to allow DIS investigators to interview employees without company supervision. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence found this action to be contrary to the firm's contractual obligations under its security agreement with DOD.

The company just discussed is not the only one where a proxy holder also holds the title of CEO. At another firm, the proxy holder's salary as CEO is approximately \$113,000 (as compared to the \$22,000 proxy holder stipend). Again, there appears to be a conflict of interest because of the CEO's fiduciary duty and loyalty to the foreign-owned company, and his responsibility to protect DOD's information security interests.

At another proxy firm, the lead proxy holder owns a consulting firm that has a contract with the foreign-owned U.S. company. In this case, there appears to be a conflict of interest because as proxy holder, his primary responsibility is to protect the information security interests of DOD, but as

a consultant to the foreign-owned firm, it is in his interest to please the foreign-owned company.

At another firm, the agreement requires that the outside members of the security committee be independent of the foreign investors and their shareholders. The French government owns 12-1/4 percent of this U.S. company. Even though the outside members of the security committee are to protect classified and export-controlled information from this foreign government, one outside member created the appearance of a conflict of interest by representing a French government-owned firm before DOD in its efforts to buy another cleared U.S. defense contractor. This outside member also created the appearance of a conflict of interest when his consulting firm became the Washington representative for a French government-owned firm in its export control matters with the State Department.

Finally, the ISR does not expressly require that outside directors serving under an SSA comply with the independence standards applicable to voting trustees and proxy holders. The reason for this omission is not clear. However, all of the SSAs we reviewed stated that individuals appointed as outside directors can have “no prior employment or contractual relationship” with the foreign owners. Since the outside directors perform the same function as voting trustees and proxy holders in ensuring the protection of classified information and the continued ability of the cleared U.S. company to perform on classified contracts, it seems reasonable that they should also be disinterested parties when named to the board and should remain free of other involvement with the foreign owners during their period of service.

DIS Inspections Did Not Focus on Foreign Ownership Issues

DIS inspectors told us that their inspections of foreign-owned U.S. defense contractors vary little from the type of facility security inspections they do at U.S.-owned facilities. Their inspections concentrated on such items as classified document storage, amount and usage of classified information, and the number of cleared personnel and their continuing need for clearances.

During the time of our review, DIS developed new guidelines for inspections of foreign-owned firms by its industrial security staff to specifically address foreign ownership issues. They call for the inspectors to examine issues such as changes to the insulating agreement, business relationships between the U.S. company and its foreign owners, foreign

owner involvement in the U.S. company's strategic direction, the number and nature of contacts with representatives of the foreign owners, and the number of foreign staff working at the facility. These guidelines were promulgated in September 1994.

DIS is beginning to implement the new inspection guidelines. According to DIS officials at the regional and field office levels, before they use the new guidelines, they must educate the inspection staff on foreign ownership issues as well as how the issues should be addressed during their inspections. They also said that implementing these new inspection procedures would probably double the length of an inspection at the foreign-owned facilities.

Currently, DIS must inspect each cleared facility twice a year, but it is having difficulty maintaining this inspection schedule. Industrial security inspectors are responsible for around 70 cleared facilities, and inspections at some larger facilities take a number of days. Doubling the inspection time at the foreign-owned facilities under the new guidelines might require some realignment of DIS resources. According to DOD officials, DIS inspections will occur no more often than annually under the NISPOM.

Recommendations

We recommend that the Secretary of Defense develop and implement a plan to improve trustee oversight and involvement in the foreign-owned companies and to ensure the independence of foreign-owned U.S. defense contractors and their trustees from improper influence from the foreign owners. As part of this effort, the Secretary should make the following changes in the implementation of the existing security arrangements and under the National Industrial Security Program.

1. Visitation request approvals: The trustees should strictly adhere to the ISR visitation agreement provision that requires them to approve requests for visits between the U.S. defense contractor and representatives of its foreign owners. This duty should not be delegated to officers or employees of the foreign-owned firm.

2. Trustee monitoring: The trustees should be required to ensure that personnel of the foreign-owned firm document and report the substance of the discussions they hold with personnel of the foreign parent firm. The trustees should review these reports and ensure that the information provided is sufficient to determine what information passed between the parties during the contact. The trustees should also select at least a sample

of contacts and interview the participants of the foreign-owned firm to ensure that the post-contact reports accurately reflect what transpired.

3. Trustee inspections: To more directly involve trustees in information security monitoring, the trustees should annually supervise an information security inspection of each of the cleared facilities. The results of these inspections should be included in the annual report to DIS.

4. FSO supervision: To insulate the FSO from influence by the foreign-owned firm and its foreign owners, the trustees should be empowered and required to review and approve or disapprove the selection of the FSO and all decisions regarding the FSO's pay and continued employment. The trustees should also supervise the FSO to ensure an acceptable level of job performance, since trustees are charged with monitoring information security at the U.S. defense contractor.

5. Financial independence: To monitor the financial independence of the foreign-owned firm, the annual report to DIS should include a statement on any financial support, loans, loan guarantees, or debt relief from or through the foreign owners or the government of the foreign owners that have occurred during the year.

6. Trustee independence: To help avoid conflicts of interest for the trustees, require them to certify at the time of their selection, and then annually, that they have no prior or current involvement with the foreign-owned firm or its foreign owners other than their trustee position. This certification should include a statement that they are not holding and will not hold positions within the foreign-owned company other than their trustee position. It should be expressly stated that these independence standards apply equally to voting trustees, proxy holders, and outside directors of firms under SSAs.

7. Trustee duties: The selected trustees should be required to sign agreements acknowledging their responsibilities and the specific duties they are required to carry out those responsibilities, including those in numbers 1 through 4. The agreement should provide that DOD can require the resignation of any trustee if DOD determines that the trustee failed to perform any of these duties. This agreement should ensure that the trustees and the government clearly understand what is expected of the trustees to perform their security roles.

Agency Comments and Our Evaluation

DOD stated that it generally agreed with the thrust of our recommendations in this report, but did not agree that the specific actions we recommended were necessary, given DOD efforts to address the issues involved. DOD said it had addressed these issues through education, advice, and encouragement of trustees to take the desired corrective actions. We and DOD have both seen instances in which this encouragement has been rejected. Because of the risk to information with national security implications, we believe that requiring, rather than encouraging, the trustees to improve security oversight would be more effective. Therefore, we continue to believe our recommendations are valid and believe they should be implemented to reduce the security risks.

DOD's comments and our evaluation are presented in their entirety in appendix I.

Comments From the Department of Defense

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



COMMAND, CONTROL,
COMMUNICATIONS
AND
INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

April 14, 1995

Mr. Henry L. Hinton, Jr.
Assistant Comptroller General
U.S. General Accounting Office
National Security and International
Affairs Division
Washington, DC 20548

Dear Mr. Hinton:

This is the Department of Defense (DoD) response to the General Accounting Office (GAO) draft report "DEFENSE INDUSTRIAL SECURITY: Weaknesses in DoD Security Arrangements at Foreign Owned Companies," dated March 1, 1995 (GAO Code 463831), OSD Case 9874-X. The DoD partially concurs with the draft report.

While the DoD generally agrees with most of the report, the Department disagrees on several matters. For example, the report implies that classified and controlled unclassified information may not be sufficiently protected under the special security agreement (SSA) clearance arrangement. The DoD disagrees. The SSA was approved for use by the DoD in 1983, following a thorough examination of its ability to satisfy multiple and sometimes competing interests. The SSA arrangement has undergone numerous improvements since its inception and, importantly, several reviews in recent years have reaffirmed that SSAs are fundamentally sound and that they fulfill their primary purpose of protecting classified information.

The DoD also disagrees with the implication that the recently approved National Industrial Security Program Operating Manual (NISPOM) replaced the Industrial Security Regulation and that, as a result, some needed visitation controls may have been eliminated. For the past two years, the visitation procedures formerly embodied in separate visitation agreements have been incorporated into newly executed voting trusts, proxies, and special security agreements, obviating the need for a separate visitation agreement.

The DoD also disagrees that Defense Investigative Service (DIS) inspections do not currently focus on foreign

See p. 7.

See pp. 12 and 32.

Appendix I
Comments From the Department of Defense

See pp. 40-41.

ownership issues. The DoD acknowledges that special attention is needed during its inspections of foreign owned companies. As a result of an internal review completed in 1993, the DIS developed and implemented detailed guidelines for security inspections of companies with foreign involvement. These guidelines were formally promulgated in the DIS Foreign Ownership, Control or Influence (FOCI) Handbook, dated September 1994.

See p. 6.

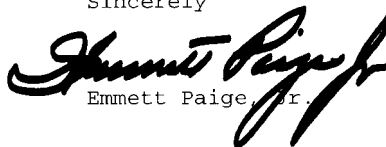
The DoD also acknowledges that more active involvement by some trustees is needed, but disagrees with the GAO assertion that trustees generally did little to ensure that company management was not unduly influenced by the foreign owners, or that the control structure in the security agreements were being properly implemented. The DoD also agrees that trustees need to remain actively involved in monitoring the companies' business management and information security program. However, reasonable and appropriate delegation of authority should be permitted beyond that which the GAO considers acceptable.

See p. 7.

With regard to the GAO recommendations, the DoD would like to point out that the Department has already established requirements for most of the actions recommended by the GAO. The DoD does not agree that the Secretary of Defense should develop and implement a plan to make the individual improvements specified by the GAO. That plan is not necessary since the Department has either already accomplished or is in the process of accomplishing those improvements necessary.

The detailed DoD comments on the draft report findings and recommendations are provided in the enclosure. The DoD appreciates the opportunity to comment on the GAO draft report.

Sincerely


Emmett Paige, Jr.

Enclosure

GAO DRAFT REPORT - DATED MARCH 1, 1995
(GAO CODE 463831) OSD CASE 9874-X

"DEFENSE INDUSTRIAL SECURITY: WEAKNESSES IN DOD SECURITY
ARRANGEMENTS AT FOREIGN-OWNED COMPANIES"

DEPARTMENT OF DEFENSE COMMENTS

FINDINGS

FINDING A: Government Required Security Controls. The GAO explained that under a January 1993 executive order, the National Industrial Security Program Operating Manual (NISPOM) has been drafted to replace various agencies' industrial security requirements, including the DoD Industrial Security Regulation (ISR). The GAO noted that the NISPOM section dealing with Foreign Ownership, Control, or Influence (FOCI) contains provisions on voting trusts, proxy agreements, and Special Security Agreements (SSAs) similar to those in the ISR. According to the GAO, until the manual is issued, the ISR continues to apply.

The GAO reported that both the ISR and the NISPOM require a company to obtain a facility clearance before it can work on a classified DoD contract and prescribe procedures for Defense contractors to protect classified information released to them. The GAO explained that DoD policy generally provides that a firm was ineligible for a facility clearance if it is under FOCI, however, such a firm may be eligible for a facility clearance if actions are taken to effectively negate or reduce associated risks to an acceptable level. The GAO reported that when the firm is majority foreign-owned, the control structures used to negate or reduce such risks include voting trusts, proxy agreements, and SSAs. (The GAO provided detailed descriptions of the control structures on pages 16 to 19 of the draft report). The GAO noted that the Defense Investigative Service (DIS) administers the DoD Industrial Security Program and is required to conduct compliance reviews of Defense contractors operating under voting trusts, proxy agreements, and SSAs. The GAO explained that the reviews are aimed at ensuring compliance with special controls, practices, and procedures established to insulate the facility from foreign interests.

The GAO asserted that the ISR required a visitation agreement for each voting trust, proxy agreement, or SSA. According to the GAO, the agreements are signed by the foreign owners; the foreign-owned U.S. firm; the voting trustees, proxy holders, or SSA outside directors--collectively referred to as trustees--and the DoD. According to the GAO, the visitation agreement identifies the

Appendix I
Comments From the Department of Defense

Now on pp. 2-3 and
12-14.

representatives of the foreign owners allowed to visit the cleared U.S. firm, the purposes for which they are allowed to visit, the advance approval that is necessary, and the identity of the approval authority. (pp. 3-4, pp. 15-19/GAO Draft Report)

See comment 1.

DoD Response: Partially concur. The NISPOM was published in January 1995 and issued to government agencies and industry in February 1995. The NISPOM was designed to replace various agencies' industrial security issuances, including the DoD Industrial Security Manual, a companion document to the ISR which is intended for Government entities. The ISR will require amendment to conform to the NISPOM, but it will not be replaced by the NISPOM. Moreover, there are no plans to remove the requirement for effective visitation procedures from the amended ISR. In addition, outside directors are not signatories to the SSA.

FINDING B: Agreements Are Negotiated and Vary. The GAO reported that voting trust agreements, proxy agreements, SSAs, and the attendant visitation agreements are negotiated between the foreign-owned company and the DoD. Although the DoD has boiler-plate language that can be adopted, the GAO noted that many cases have unique circumstances that call for flexible application of the ISR provisions. The GAO explained that the flexible approach leads to negotiations that can result in company-specific agreements containing provisions that provide stronger or weaker controls. The GAO pointed out that generally, the foreign owners negotiate to secure the least restrictive agreements possible.

Now on pp. 4 and 15.

The GAO reported that the DoD has approved more lenient visitation agreements over time. The GAO commented that a DoD official explained that the flexible approach to FOCI arrangements and the resulting negotiations are the probable cause of the relaxation of controls over visitation. The GAO pointed out that each negotiated visitation agreement that relaxed controls became the starting point for subsequent negotiations on new agreements as the foreign-owned companies' lawyers would point to the last visitation agreement as precedent. While recognizing the need to tailor the agreements to specific company circumstances and to permit international Defense work, the GAO concluded that the lack of a baseline set of controls in the agreements made DIS inspection very difficult. (p. 6, p. 20/GAO Draft Report)

DoD Response: Partially concur. The terms of voting trust agreements, proxy agreements, and SSAs are negotiated between the DoD, the foreign-owned U.S. company, and all intermediate owners through the ultimate foreign shareholder. The foreign owners may recommend a particular agreement, but the DoD determines which

agreement, if any, will be required. Foreign owners are permitted to negotiate the terms of a particular agreement with the DoD, provided the substance of the baseline "boilerplate" language is preserved. The DoD serves as the final approval authority for those agreements. The company-specific agreements take into account unique factors, such as risk, threat, and transaction particulars, to ensure that final agreements, include protection which is neither inadequate, nor excessive.

The DoD does not agree that the last visitation agreement serves as a precedent for new agreements. As a practical matter, lawyers for a new client would not necessarily be aware of visitation terms previously negotiated. The DoD also disagrees with the inference that baseline controls do not currently exist. Baseline visitation controls were developed for each FOCI agreement in 1993, when DoD eliminated the visitation agreement as a separate document.

FINDING C: Agreements Were Not Designed to Protect Unclassified Export-Controlled Technologies. The GAO reported that almost all the foreign-owned U.S. firms reviewed possessed unclassified information and technologies that are export-controlled by the Departments of State and Commerce. According to the GAO, some of the technologies have been deemed to be militarily critical by the DoD, such as carbon/carbon material manufacturing technology and flight control systems technology. The GAO pointed out that many classified Defense contracts involve classified applications of unclassified export-controlled items and technologies, however, the ISR and most agreements were not designed to protect unclassified export-controlled information. According to the GAO, the DIS does not review for the protection of unclassified export-controlled technology during inspections of cleared contractors and there is no established means for the U.S. Government to monitor compliance and ensure enforcement of Federal regulations regarding the transfer of export-controlled technical information. The GAO explained that the new NISPOM reflects this concern and requires trustees in future voting trusts, proxy agreements, and SSAs to take necessary steps to ensure the company complies with U.S. export control laws. (p. 21/GAO Draft Report)

DoD Response: Concur. The acquisition of a U.S. company by a foreign buyer does not present an inherently greater risk to controlled unclassified information than might arise in connection with other alliances between U.S. companies and foreign partners, e.g., cooperative programs and joint ventures. Under any circumstance, the unlawful transfer of export controlled information is prohibited by criminal laws of the United States. Moreover, FOCI agreements require that extraordinary controls be put in place,

See comment 2.

Now on pp. 15-16.

See comment 3.

e.g., a Defense Security Committee with significant responsibility over classified and controlled unclassified information and a technology control plan to guard against the risk of even an inadvertent export of controlled unclassified information. The inclusion of standard protections in FOCI agreements, coupled with criminal sanctions for violation of the export laws provides substantial protection against improper export of controlled unclassified information.

It should be noted that unclassified export-controlled information resides at a large number of uncleared foreign-owned U.S. companies and cleared U.S.-owned companies without the strong oversight and enforcement measures inherent with FOCI agreements. It has been estimated that 46 percent of legal entities cleared by the DoD have some reportable foreign involvement. That involvement typically involves data exchange agreements, foreign contracting, joint ventures, technical exchange programs, foreign indebtedness and the like, which also presents a risk of unauthorized transfer of controlled unclassified information. Industrial security rules are important, but they do not actually prevent individuals from compromising sensitive information willfully. Even the most rigorous industrial security policies and procedures are only as effective as the personal qualities of the individuals responsible for protection.

The chief goal of industrial security policy is to protect classified information. The DIS has not been delegated responsibility to oversee contractor compliance with export control laws. It is the DoD position that, as a matter of priority, current available resources must be applied to the protection of classified information.

FINDING D: Firms Operating Under Voting Trusts, Proxy Agreements or SSAs. The GAO reported that as of August 1994, 54 foreign-owned U.S. Defense contractors were operating under voting trusts, proxy agreements, or SSAs. According to the GAO, six of the companies operate under voting trusts, 15 under proxy agreements, and 33 under SSAs. The GAO found that the 54 firms held a total of 657 classified contracts, valued at \$5.4 billion. The GAO noted that the foreign owners of the 54 firms are from Australia, Austria, Canada, Denmark, France, Germany, Israel, Japan, the Netherlands, Sweden, Switzerland, and the United Kingdom. (p. 22/GAO Draft Report)

DoD Response: Concur. This finding underscores the importance of an effective FOCI policy to address the protection of classified information under circumstances where the U.S. Government allows a U.S. company performing such work to be acquired by a foreign

Now on p. 16.

Appendix I
Comments From the Department of Defense

interest. By way of update, several of the foreign-owned firms reviewed by the GAO are no longer operating under a FOCI agreement, because they are either owned by U.S. interests or are no longer a cleared U.S. defense contractor.

FINDING E: Information at Risk. The GAO provided a table on page 31 of the draft report describing the classification levels of information requiring access by foreign-owned U.S. Defense contractors. Examples of some of the sensitive contract work being performed by the 14 foreign-owned U.S. companies included in the GAO review are:

- development of computer software for planning target selection and aircraft routes in the event of a nuclear war (a Top Secret contract);
- maintenance of the DoD Worldwide Military Command and Control System (the contract was classified because of the information the computer-driven communications system contains);
- production of signal intelligence gathering radio receivers for the U.S. Navy;
- production of command destruct receivers for military missiles and National Aeronautics and Space Administration rockets (to destroy a rocket that goes off course);
- production of carbon/carbon composite Trident D-5 missile heat shields; and
- production of the flight controls for the B-2, the F-117, and the F-22.

The GAO explained that some of the contracts the foreign-owned U.S. companies are working on are Special Access Programs, while others involve less sensitive technologies. The GAO reported that one firm operating under an SSA is required to have a Secret-level clearance because it installs alarm systems in buildings that hold classified information. In addition to classified information, most of 14 the foreign-owned companies the GAO reviewed possessed unclassified technical information and hardware items that are export-controlled by the State or Commerce Departments. According to the GAO, many of the technologies are deemed to be militarily critical by the DoD. (pp. 30-33/GAO Draft Report)

Now on pp. 20-22.

Appendix I
Comments From the Department of Defense

DoD Response: Concur. The DoD did not independently verify the accuracy of the GAO's list of classified and sensitive contract work being performed by the 14 foreign-owned U.S. companies surveyed.

FINDING F: Higher Degree of Risk with SSA Structure. The GAO reported that unlike voting trusts and proxy agreements, which insulate foreign owners from the management of the cleared firm, SSAs allow foreign owners to appoint a representative to serve on the board of directors, known as an "inside director," who represents the foreign owners and is often a foreign national. The GAO explained that the inside director is to be counterbalanced by DoD-approved directors--the "outside directors"--who are to protect U.S. security interests.

The GAO found that inside directors are not permitted to hold a majority of the votes on the board, but because of their connection to the foreign owners, their views about the company's direction on certain Defense contracts or product lines reflect those of the owners. The GAO pointed out that depending on the composition of the board, the inside director and the company officers on the board could possibly combine to out-vote the outside directors. In addition, the GAO noted that unlike voting trusts and proxy agreements, the SSAs included in the review stated that the foreign owner can replace "any member of the (SSA company) Board of Directors for any reason."

The GAO found that foreign owners of SSA firms can also exercise significant influence over the U.S. companies they own in other ways. The GAO reported that at two SSA firms reviewed, the foreign owners obtained under export licenses unclassified technology from the U.S. subsidiary that was vital to the U.S. companies' competitive positions. According to the GAO, officers of the U.S. companies did not want to share the technologies, but were required to do so by the foreign owners and, as a result, one of the U.S. companies faced its own technology in a competition with its foreign owner for a U.S. Army contract.

The GAO explained that because of the additional risk, companies operating under SSAs are normally ineligible for contracts allowing access to Top Secret(TS), Special Access Programs(SAP), Sensitive Compartmented Information(SCI), Restricted Data(RD), and Communications Security Information(COMSEC). The GAO found, however, that 12 of the 33 SSA companies were working on at least 47 contracts requiring access to this highly classified information.

Appendix I
Comments From the Department of Defense

According to the GAO, prior to June 1991, the DoD reviewed an SSA firm to determine whether or not it would be in the national interest to allow the firm to compete for contracts classified TS, SCI, SAP, RD, or COMSEC. New guidance was issued in June 1991 that the GAO explained required the responsible Military Service to make a national interest determination to support each specific award of a highly classified contract to an SSA firm. The GAO found only one contract-specific national interest determination had been written since the June 1991 guidance. The GAO explained that DoD officials stated that the other 46 highly classified contracts performed by SSA companies predated June 1991, or were follow-on contracts to contracts awarded prior to June 1991. Because some contracts awarded to SSA companies are under special access restrictions, DoD officials may be authorized to conceal the contracts from those not specifically cleared for access to the program; therefore, the GAO stated it could not determine with confidence if the requirement for contract-specific national interest determinations was carried out.

The GAO reported that one company performs on contracts classified as TS, SCI, SAP, RD, and COMSEC under an alternative arrangement-- a Memorandum of Agreement (MOA). The GAO explained that the unique agreement was created because the company has classified DoD contracts and, although foreign interests do not hold a majority of the stock, they own 49 percent of the company and have special rights to veto actions of the majority owners.

The GAO explained that normally, under the ISR, minority foreign investment in a cleared U.S. Defense contractor required only a resolution of the board of directors stating that the foreign interests will not require, nor be given, access to classified information. The GAO reported, however, that in this case, the DIS argued in favor of a full SSA, due to veto rights the foreign investors have over basic corporate decisions. According to the GAO, the veto rights could give the foreign interests significant control and influence over the U.S. Defense contractor. The GAO found that, although the DIS objected to an agreement less stringent than an SSA, the Office of the Under Secretary of Defense for Policy determined that the MOA was a sufficient control. The GAO explained that the MOA lacks some of the protections of the SSA, since there are no DoD-approved outside members on the board of directors, while the board does contain representatives of the foreign partners. The GAO further explained that, although the MOA requires a Defense Security Committee to oversee the protection of classified information, it permits substantially less active involvement by DoD-approved outside members. The GAO also noted that prior security committee approval for visits by representatives of the foreign interests to the cleared U.S. Defense contractor is only needed if the visit

Appendix I
Comments From the Department of Defense

Now on pp. 4 and 27-30.

concerns performance on a classified contract. (pp. 7-9, pp. 47-52, p. 58/GAO Draft Report)

See comment 4 and p. 28.

DoD Response: Partially concur. The SSA structure incorporates the risk management concept of the NISPOM, which takes appropriate threat assessments into account. Studies as recent as the DIA/DIS survey of 1993 have demonstrated that FOCI agreements are basically sound and fulfill their stated purpose. That survey found heightened awareness of security and export-controlled matters at those firms. The GAO statement that the foreign owner can replace "any member of the (SSA company) Board of Directors for any reason" is misleading in that the provision of the SSA includes several qualifying safeguards, such as DIS notification and approval.

See p. 30.

The security control agreement (SCA), which did not exist in 1992, was developed and codified in the NISPOM for U.S. control cases, such as the one cited by the GAO where an MOA was used. Consistent with security controls under the SCA option for U.S.-controlled companies, certain provisions of the extant MOA need not be as stringent as those found in SSAs, which are reserved for foreign control cases.

FINDING G: Visitation Agreements Give Foreign Owners a High Degree of Access. The GAO reported that unlike the new NISPOM, the ISR required segregation of the foreign owners of a cleared U.S. Defense contractor from all aspects of the U.S. company's Defense work. The GAO found that at all 14 companies reviewed, visitation agreements permitted the foreign owners and their representatives to visit with regard to military and dual-use products and services. According to the GAO, the visitation agreements permitted visits to the U.S. company in association with classified contracts if the foreign interests have the appropriate security clearance, and under State or Commerce Department export licenses.

The GAO pointed out that the large number of business transactions between the U.S. Defense contractors and their foreign owners granted representatives of the foreign owners frequent entry to the cleared U.S. facilities. The GAO reported that eight of the fourteen firms reviewed had contractual arrangements with their foreign owners that led to a high (often daily) degree of contact. The GAO also reported that some visitation agreements permitted long-term visits to the cleared U.S. companies by employees of the foreign owners. The GAO found that five companies reviewed had employees of the foreign owners working at the cleared U.S. facilities. According to the GAO, in a number of those cases

Appendix I
Comments From the Department of Defense

technical and managerial staff were working on military and dual-use systems and products under approved export licenses.

The GAO commented that post-visit contact reports are the primary means for the DIS and the trustees to monitor the substance of contacts between the foreign-owned U.S. contractor and representatives of its foreign owners. The GAO explained that such records should be used to determine if the contact with representatives of the foreign owners was appropriate and in accordance with the ISR and the visitation agreement. Some visitation agreements, the GAO explained, do not require personnel of the foreign-owned U.S. firm to document and report the substance of the discussions with personnel of the foreign parent firm. The GAO reported that at three of the firms reviewed, the only record of contact between the personnel of the U.S. company and the foreign owners were copies of forms granting approval for the visit. However, the GAO reported that at other foreign-owned U.S. Defense contractors, post-visit contact reports were available for DIS use.

The GAO also reported that the ISR, the NISPOM, and most of the visitation agreements reviewed do not require telephonic contacts between the U.S. Defense contractor and representatives of its foreign owners to be controlled and documented. The GAO explained that if an individual intends to breach security, it would be easier to transfer classified or export-controlled information by telephone, facsimile, or computer modem than it would be in person. The GAO concluded that documenting telephone contacts would not prevent such illegal activity, but might make it easier to detect. (pp. 7-9, pp. 52-59/GAO Draft Report)

Now on pp. 5 and 30-32.

DoD Response: Concur. Each voting trust, proxy and SSA contains visitation procedures. Inclusion of those procedures in each FOCI agreement eliminates the need for separate visitation agreements. The DoD requires that visit requests and "post-contact" reports include sufficient information upon which informed decisions can be rendered, consistent with the terms of FOCI agreements and NISP policies and procedures. The access afforded foreign nationals under a DoD visitation procedures is consistent with applicable U.S. law and regulation.

FINDING H: National Industrial Security Manual Eliminates Requirement for Visitation Agreements. The GAO explained that the section of the NISPOM dealing with foreign ownership, control, and influence would replace the FOCI section of the ISR. The GAO commented that there is no requirement in the new manual to enter into agreements designed to restrict visitation between the cleared U.S. Defense contractor and representatives of its foreign

owners. According to the GAO, the manual appears to allow unlimited visitation between representatives of foreign owners and the cleared U.S. Defense contractor. The GAO explained that rather than require visitation agreements, the manual requires each company operating under a voting trust, proxy agreement, or SSA to develop a Technology Transfer Control Plan which would prescribe measures to reasonably foreclose the possibility of "inadvertent access" to information by unauthorized individuals. The GAO concluded that, although the concept of a Technology Transfer Control Plan seems to appropriately provide for some control, the lack of a visitation agreement means that representatives of the foreign owners could have greater access to the U.S. facilities where classified work is being performed. The GAO pointed out that once in the facility, preventing access to controlled information by the foreign representatives would hinge on the scrupulous implementation of technology transfer controls by company personnel and would require a significantly increased level of monitoring by the trustees and the DIS. (pp. 7-9, pp. 57-59/GAO Draft Report)

Now on pp. 5 and 32.

DoD Response: Concur. The NISPOM does not provide for uncontrolled visitation between a foreign investor and its cleared subsidiary. Visitation approval procedures are required to be included within all FOCI agreements. As stated previously, each voting trust, proxy and SSA executed since 1993 contains visitation procedures. Inclusion of those procedures in each FOCI agreement eliminates the need for separate visitation agreements. The DoD is revising the ISR to provide implementing policy to Government entities consistent with the NISPOM. That implementing policy will include the current ISR requirement respecting visitation approval procedures (as part of each FOCI agreement). It should also be recognized that technology control plans do not replace visitation approval procedures as inferred by the GAO.

See p. 32.

FINDING I: Little Involvement by Trustees in Security or Company Management Oversight. The GAO found that the DoD-approved trustees at certain companies were more actively involved in management and security oversight than at other companies. The GAO reported that at some companies, the trustees retained, and did not delegate, their responsibility for approving all visits by representatives of the foreign owners as required in the visitation agreements. The GAO explained that the more active trustees also reviewed post-visit contact reports and interviewed a sample of technical staff who met with the foreign owners' representatives to ascertain the substance of their discussions, questioned potentially adverse company business conditions caused by arrangements with the foreign parent, and attended business meetings at the company more often than quarterly.

Appendix I
Comments From the Department of Defense

In contrast, the GAO found that at most of the companies reviewed, the trustees (or proxy holders or outside directors) did little to ensure that company management was not unduly influenced by the foreign owners or that the control structures in the security agreements were being properly implemented. The GAO explained that instead, they viewed their role as limited to ensuring that policies exist within the company to protect classified information.

The GAO also commented that the need for trustee oversight of the business management of foreign-owned companies was highlighted at one SSA firm reviewed. According to the GAO, at the company, the foreign owners exercised their powers under the SSA to replace two successive director/presidents of the U.S. company. The GAO explained that the first claimed he was being terminated because he was attempting to enforce the SSA, while the second president contested his dismissal because the outside directors were not given prior notice of the owners' intent to replace him. The GAO commented that the owners stated that in both cases, poor business performance was the cause for termination and, in those cases, the outside directors agreed. The GAO pointed out that outside directors need to remain actively involved in monitoring the companies' business management to ensure that foreign owners exercise those powers only for legitimate business reasons and not for reasons that could jeopardize classified information and contracts.

The GAO reported that implementation and monitoring of the information security program was usually left to an employee of the foreign-owned U.S. company, the facility security officer (FSO). The GAO found that a variety of personnel served as the FSO, including a General Counsel, secretaries, and professional security officers, but in any case, the FSO often performed the administrative functions of security and was not usually in a position to determine the proper parameters for the substance of classified discussions, given a cleared foreign representative's need to know. The GAO concluded that the limitation and the FSO's potential vulnerability as an employee of the foreign-owned company pose a risk without active trustee involvement.

Additionally, the GAO found that when required, most post-visit contact reports lacked the detail needed for the trustees or the DIS to determine what was discussed between the foreign-owned company and the owners' representatives. The GAO concluded that trustee inattention to contact at the technical level is of particular concern, since that is where most of the U.S. Defense contractor's technology is located.

The GAO found that trustees rarely visited or toured the foreign-owned company's facility to observe the accessibility of classi-

Now on pp. 5-6 and
34-37.

fied or export-controlled information, except during prearranged tours at the time of their quarterly meetings. The GAO reported that the trustees also rarely interviewed managerial and technical staff to verify the level and nature of their contact with personnel of the foreign parent firm. (pp. 10-11, pp. 60-66/ GAO Draft Report)

DoD Response: Partially concur. While the DoD acknowledges that more active involvement by some trustees in business management and security affairs is needed, the DoD disagrees that the control structures in the security agreements were being improperly implemented or that trustees largely did little to ensure that company management was not unduly influenced by the foreign owners. Duties and responsibilities that the DoD expects trustees to carry out personally are prescribed in the requisite security agreements and related implementation documents. Where a duty is not explicitly required to be performed personally by a trustee, the trustee may delegate the duty. Trustees cannot delegate overall responsibility and they are held fully accountable should delegated duties be performed in a substandard way. It is incumbent upon trustees to ensure that their personal involvement is sufficient to maintain the integrity of the FOCI agreement.

The DIA/DIS 1993 survey of FOCI agreements disclosed varying degrees of involvement by trustees in security or company management oversight. That survey recommended that special attention should be given to the activities of trustees in implementing the terms of the FOCI agreement. The DIS has developed and implemented procedures to improve trustee oversight and involvement.

See p. 7.

The designation of an individual to serve as the FSO at a U.S. firm within the cleared defense industrial base is frequently a collateral duty, especially when the U.S. firm is small and does little classified work. However, the 1993 DIA/DIS survey disclosed that the FSOs at foreign-owned firms cleared through a FOCI agreement are afforded a greater degree of access to board members and senior management officials than typically exists at comparable U.S.-owned companies.

FINDING J: Foreign Owners Acted in Capacities Beyond That of Beneficiary in Proxy Firms. The GAO found that at one of the proxy firms reviewed, the foreign owners acted in more than the status of beneficiaries. The GAO explained that the strategic plan and annual budget of the proxy firm were regularly presented to the foreign owners for review and at least once the foreign parent firm rejected a strategic plan and indicated that it would continue to object to the plan until the plan provided for an

Appendix I
Comments From the Department of Defense

increase in future collaboration between the proxy firm and the foreign parent firm. The GAO reported that at another time, the foreign owners used the staff of the U.S. contractor as their representatives in an attempt to acquire another U.S. aerospace firm more than 10 times the size of the proxy firm. The GAO explained that, although decisions on mergers are within the rights of the foreign owners during the acquisition effort, officers and employees of the U.S. Defense contractor were operating at the direction of the foreign owners. The GAO concluded that directing staff of the proxy firm is clearly acting as more than a beneficiary, the status to which foreign owners are limited under the ISR.

The GAO also reported that another firm operating under a proxy agreement has a distribution agreement with the foreign owners that restricts the proxy firm to marketing electronic equipment and services to the U.S. Government. The GAO explained that in addition, the agreement will only allow the proxy firm to service hardware that is used on classified systems. The GAO concluded that although the distribution agreement was approved by the DIS at the time of the foreign acquisition, it controls the strategic direction of the proxy firm. According to the GAO, the proxy firm reported to the DIS that it is important for the survival of the U.S. company to be able to pursue business opportunities that are currently denied by the distribution agreement. (pp. 8-10, pp. 66-67/GAO Draft Report)

Now on pp. 37-38.

DoD Response: Concur. The DIS raised identical concerns at the same two companies cited by GAO with regard to foreign owners acting in capacities beyond that of beneficiary. In the first case, the DIS opened an inquiry into the effectiveness of the proxy agreement in early 1993. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) personally participated in resolution of the inquiry with the DIS through meetings with and correspondence to the proxy holders. The ASD(C3I) advised the proxy holders of the findings of the DIS inquiry; most significantly, that material misunderstandings and serious breaches of the proxy agreement had occurred. As a result of the inquiry, the proxy holders were required to develop and implement a plan of action in coordination with the DIS to prevent a recurrence. In 1994, the foreign owner sold the majority of the assets (including all assets related to classified contracts) to another U.S.-cleared firm and the proxy agreement was terminated.

The second case cited by the GAO was also investigated by the DIS in 1993 to determine if the foreign owner was being provided prerogatives to which it was not entitled under the proxy agreement. The proxy holders ascertained that the cleared firm required flexibility in marketing electronic equipment and

See comment 5.

services to the U.S. government. The extant distribution agreement with the foreign owner did not provide for such flexibility. The proxy holders exercised their prerogatives of ownership to ensure the viability of the cleared firm during lengthy negotiations with the foreign owner to revise the terms of the distribution agreement. The DIS participated in several meetings with the parties at their request, but the proxy holders took the lead in resolving the matter. That firm was sold in 1995 to another U.S.-cleared firm and the proxy agreement was terminated.

See comment 6.

By way of perspective, that the two cases cited were aberrations from conditions existing at other companies operating under FOCI insulating agreements. The DoD did not find any instance in which classified information had been compromised or was suspected of having been compromised. The two cases serve to illustrate the effectiveness of DIS oversight of foreign-owned companies and the importance of maintaining adequate capabilities during this period of downsizing and fiscal constraint.

FINDING K: Some Foreign-Owned Firms Are Financially Dependent on Foreign Owners. The GAO found examples of firms that depended on their foreign owners for financial support or had business arrangements with the foreign owners that degraded the independence of the proxy firm. The GAO explained that the president of one company operating under a proxy agreement advised that his company was basically bankrupt and that financing for his company comes from banks owned by the a foreign government. The GAO noted that the foreign parent firm of the U.S. company guarantees the loans, and two of the foreign government banks are on the board of directors of the foreign parent firm. The GAO reported that recently, the foreign owners gave \$6 million to the U.S. company to relocate one of its divisions. According to the GAO, the officials of the U.S. company stated that they could not otherwise have afforded such a move, nor could they have obtained bank loans on their own.

Now on p. 38.

The GAO reported that another U.S. Defense contractor operating under a proxy agreement had loans from the foreign owners that grew to exceed the value of the foreign-owned firm. The GAO commented that one proxy holder said the foreign-owned firm would probably have gone out of business without the loans, and that even with the loans, the foreign-owned company's financial position was precarious. According to the GAO, the foreign-owned firm was financially weak, could not obtain independent financing, and was considerably burdened by making interest payments on its debt to the foreign owners. The GAO reported that during the review, a DIS official acknowledged that the risk imposed by the indebtedness to the foreign owners should have been an issue for the DIS to address. (pp. 8-10, pp. 68-69/GAO Draft Report)

Appendix I
Comments From the Department of Defense

DoD Response: Concur. The DoD agrees that the financial independence of the proxy company mentioned requires more active monitoring to assure that the foreign owner is not exercising control or influence through such support. The DIS already requires information be provided on any financial support from the foreign investor to its cleared subsidiary. However, greater emphasis will be placed on such support and its potential to undermine the effectiveness of the FOCI agreement.

FINDING L: Some Trustees Have Appearance of Conflicts of Interest.

The GAO reported that at one of the companies reviewed, a proxy holder was previously involved as a director of a joint venture with the foreign owners who later nominated the individual to be their proxy holder. The GAO reported that the proxy holder withheld the information on his prior involvement from the DIS at the time he became a proxy holder and, upon learning of his prior involvement with the foreign parent, the DIS concluded that the individual was ineligible to be a proxy holder and should not continue in that role. The GAO reported that the ASD(C3I) wrote to the company about irregularities in proxy agreement implementation, such as allowing the foreign owners prerogatives which were not allowed under the proxy agreement, but did not address the appearance of a conflict of interest, and the individual has remained as a proxy holder.

The GAO further reported that the proxy holder is also now the part-time Chief Executive Officer of the foreign-owned U.S. Defense firm and received an annual compensation of approximately \$272,000 (as compared to the \$50,000 proxy holder stipend) for an average of eight days work per month in his dual role. The GAO explained that there appears to be a conflict of interest as follows: as Chief Executive Officer his fiduciary duty and loyalty to the foreign-owned company takes primacy; as proxy holder, his primary responsibility is to protect the information security interests of the DoD.

The GAO further reported that at this company, the conflict between the proxy holders' responsibility to the DoD and what they saw as their fiduciary responsibility was illustrated recently during a DIS investigation into possible violations of the proxy agreement. The GAO explained that citing fiduciary responsibility, the proxy holders refused to allow DIS investigators to interview company personnel without company supervision. According to the GAO, the ASD(C3I) found the action to be in contravention of the firm's contractual obligations under its security agreement with the DoD.

The GAO reported that the ISR does not expressly require that outside directors serving under an SSA comply with the conflict

Now on pp. 6 and 38-40.

of interest standards applicable to voting trustees and proxy holders. The GAO concluded that since the outside directors perform the same function as voting trustees and proxy holders in ensuring the protection of classified information and the continued ability of the cleared U.S. company to perform on classified contracts, it seems reasonable that they should also be disinterested parties when named to the board and that they should remain free of other involvement with the foreign owners during their period of service. (pp. 8-10, pp. 69-72/GAO Draft Report)

DoD Response: Concur. As a result of the 1993 DIA/DIS survey of FOCI agreements, the DIS has redoubled its efforts to ensure the "disinterested" status (no prior or current contractual, financial, or employment relationship) of individuals nominated to serve as trustees. The DIS has developed a questionnaire designed to elicit information on any involvement the trustee nominee may have had with the foreign owner, the cleared corporation, or any of their affiliates. That questionnaire, the nominee's resume, and a certificate attesting to U.S. citizenship, willingness to be cleared, and acceptance of trustee responsibilities, are reviewed in the aggregate by the DIS to ensure that the nominee has no disqualifying prior involvement. Although the subsequent discovery by the DIS of disqualifying prior involvement is rare, the matter is of sufficient importance to warrant codification in the ISR.

The DoD agrees that proxy holders generally should not occupy officer positions. However, exceptions may be granted when appropriate. At the inception of a proxy agreement, compensation for proxy holders is usually set by the foreign parent and borne by the cleared U.S. subsidiary. The compensation for the principal officers of the cleared subsidiary is set and borne by that company's board of directors.

FINDING M: DIS Inspections Do Not Currently Focus on Foreign Ownership Issues. The GAO reported that DIS inspectors advised that their inspections of foreign-owned U.S. Defense contractors vary little from the type of facility security inspection they do at U.S.-owned facilities. According to the GAO, the inspections concentrate on items such as classified document storage, amount and usage of classified information, and the number of cleared personnel and their continuing need for clearances.

The GAO acknowledged that since the GAO review began, the DIS has developed draft guidelines for future inspections of foreign-owned firms by its industrial security staff to specifically address foreign ownership issues. The GAO explained that the inspectors are required to examine issues such as changes to the insulating agreement, business relationships between the U.S. company and its

Appendix I
Comments From the Department of Defense

Now on pp. 40-41.

foreign owners, foreign owner involvement in the strategic direction of the U.S. Defense contractor, the number and nature of contacts with representatives of the foreign owners, and the number of foreign staff working at the facility. (pp. 8-10, pp. 73-74/GAO Draft Report)

See pp. 40-41.

DoD Response: Partially concur. The DoD agrees that in the past inspection focus has been lacking; however, it is no longer considered a problem. As a result of an internal DoD review conducted in 1993, the DIS has implemented guidelines for security reviews at cleared U.S. companies with foreign involvement. Those guidelines provide the basis for review and analysis by industrial security personnel of all FOCI issues (e.g. foreign ownership, indebtedness, income, contracts, etc.), and provide suggested areas of inquiry during aperiodic security reviews. The guidelines also include areas of inquiry for annual compliance reviews of foreign-owned U.S. firms cleared through the auspices of a FOCI agreement. The guidelines were formally promulgated in the DIS FOCI Handbook in September 1994.

Non-U.S. citizens at cleared U.S. firms, whether or not foreign-owned, are made a matter of special interest during security reviews to ensure that appropriate controls are in place to preclude unauthorized disclosure of classified or unclassified export-controlled information.

RECOMMENDATIONS

Now on p. 41.

RECOMMENDATION 1: The GAO recommended that the Secretary of Defense develop and implement a plan to improve trustee oversight and involvement in the foreign-owned companies and to ensure the independence of foreign-owned U.S. defense contractors and their trustees from improper influence from the foreign owners. (p. 74/GAO Draft Report)

DoD Response: Partially concur. The DoD agrees with the thrust of the recommendation. The DoD does not agree, however, that the Secretary of Defense needs to develop and implement such a plan. As a result of several reviews since 1990, needed improvements concerning trustee oversight and involvement have been developed and implemented. The DoD is continuously evaluating the FOCI policy to ensure that it is neither unreasonably stringent, nor irresponsibly weak and ineffective. That has never been a static process.

Appendix I
Comments From the Department of Defense

The DIS provides trustees with security education and advises them of training opportunities in the area of information security. Tailored threat awareness briefings are being administered by the DIS to trustees in newly created trusts, proxies and SSAs. Additionally, the DIS is working with the DIA to update risk assessments for extant trusts, proxies, and SSAs.

Improvements in training and oversight have also been effected by the DIS to preserve or enhance required company and trustee independence from foreign-owner inspired improper influence. Measures to ensure the "disinterested" status of trustee nominees have also been significantly improved.

Additionally, the Director, DIS, recognized the need for his inspector cadre to assume a more proactive posture concerning the oversight of foreign-owned companies. The DIS has taken greater responsibility for providing guidance to trustees, identifying potential problems in advance, and resolving problems as they arise. The efforts help to achieve a common government/industry understanding of requisite obligations and responsibilities and for communicating interpretations of policy or its implementation.

RECOMMENDATION 2: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to require strict adherence to the ISR visitation agreement provision requiring trustee approval of requests for visits between the foreign-owned firm and representatives of its foreign owners. The GAO explained that the duty should not be delegated to officers or employees of the foreign-owned firm. (pp. 74-75/GAO Draft Report)

DoD Response: Partially concur. The DoD agrees that more active involvement in the visitation approval process by some trustees is needed. The DoD does not agree, however, that trustees should be required to personally approve all visits between the foreign-owned firm and representatives of its foreign owners. The DIS FOCI Handbook emphasizes more proactive contractor oversight, and involvement by trustees is given priority consideration during inspections and annual meetings with trustees. Under the new system, most of the trustees will have been contacted by the DIS by the end of 1995.

The DoD maintains that reasonable and prudent delegation is warranted in many instances. Trustees remain responsible and accountable for their assigned duties, including maintaining effective visitor control, whether delegated or not. Many trustees must devote a significant portion of their time

Now on p. 41.

Appendix I
Comments From the Department of Defense

See comment 7.

protecting the economic interests of the shareholder by ensuring the success and growth of the U.S. company's business. To require trustees to personally approve all foreign visits may discourage some distinguished individuals from accepting appointments as trustees -- a result that would not be in the interest of the Department of Defense.

Now on pp. 41-42.

RECOMMENDATION 3: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to require that trustees ensure that personnel of the foreign-owned firm document and report the substance of the discussions they hold with personnel of the foreign parent firm. The GAO further recommended that the trustees should review those reports and ensure that the information provided is sufficient to determine what information passed between the parties during the contact. The GAO explained that the trustees should also select at least a sample of contacts and interview the participants of the foreign-owned firm to be sure their post-contact reports accurately reflect what transpired. (p. 75/GAO Draft Report)

DoD Response: Concur. Post-contact reporting requirements have been a standard element of DoD FOCI agreements since 1993. The DIS encourages trustees to ensure that sufficient information is provided in post-contact reports to enable identification of any inappropriate or unauthorized communication. In addition, trustees are now required to review contact reports to ensure that the scope and purpose of the visit was not exceeded, and encouraged to randomly sample when appropriate.

Now on p. 42.

RECOMMENDATION 4: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to more directly involve trustees in information security monitoring. The GAO explained that the trustees should supervise an information security inspection of each of the facilities of the foreign-owned firm annually and that the results of the inspections should be included in the annual report to the DIS. (pp. 75-76/GAO Draft Report)

See comment 8.

DoD Response: Partially concur. The DoD agrees with the need for an effective self inspection regimen and encourages trustees to oversee the inspection process. However, the DoD does not agree that the trustees should be required to "supervise" each inspection effort. Trustees are expected to provide general

Appendix I
Comments From the Department of Defense

supervision of security matters. The facility security officer is responsible for the operational oversight of the U.S. company's compliance with industrial security requirements. The NISPOM requires that all cleared companies, whether foreign-owned or not, conduct formal self inspections at intervals consistent with the risk. At least once each year, the trustees are required to report to the DIS significant actions, to include security problems, and to meet with the DIS to discuss all matters pertaining to acts of compliance or non-compliance with the terms of the FOCI agreements. The DIS will ensure that, beginning July 1995, the written standard procedures prepared by the trustees will include a requirement to provide the results of the self inspections in the annual report.

RECOMMENDATION 5: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to insulate the FSO from influence by the foreign-owned firm and the foreign owners. The GAO explained that the trustees should be empowered and required to review and approve or disapprove the selection of the FSO and all decisions regarding the FSO's pay and continued employment. The GAO further explained that the trustees should also supervise the FSO to ensure an acceptable level of job performance, since trustees are charged with monitoring information security at the U.S. defense contractor. (p. 76/GAO Draft Report)

Now on p. 42.

DoD Response: Concur. The DoD agrees that the FSO should be insulated from the foreign owners. To the knowledge of the DoD, the FSOs are not currently operating under inappropriate foreign influence. The trustees are already empowered (voting trustees and proxy holders) to review and approve or disapprove the selection of the FSO, along with FSO compensation and performance matters. Nonetheless, as a result of a March 1995 policy change, the advice and consent of the Chairman of the Defense Security Committee will be required to select the FSO. That policy change is now operative.

See comment 9.

RECOMMENDATION 6: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to monitor the financial independence of the foreign-owned firm. The GAO explained that the annual report to the DIS should include a statement on any financial support, loans, loan guarantees, or debt relief from or through the foreign owners or the government of the foreign owners that occurred during the past year. (p. 76/GAO Draft Report)

Now on p. 42.

Appendix I
Comments From the Department of Defense

DoD Response: Concur. It is DoD policy that the issue of foreign financing and any matter of possible financial dependence be examined thoroughly. All cleared Defense contractors, regardless of ownership, are required to report to the DIS details of loan arrangements, significant financial obligations, and income derived from foreign interests. The DIS will ensure that immediate steps are taken to reinforce the requirement that the annual report by the trustees include a statement on any financial support, loans, loan guarantees, or debt relief from or through the foreign owners or the government of the foreign owners that occurred during the preceding year.

RECOMMENDATION 7: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to help avoid conflicts of interest for the trustees, by requiring them to certify at the time of their selection, and then annually, that they have no prior or current involvement with the foreign-owned firm or its foreign owners other than their trustee position. The GAO explained that the certification should include a statement that the trustees are not holding and will not hold positions within the foreign-owned company other than their trustee position. The GAO further explained that it should be expressly stated in the regulations that the trustee independence standards apply equally to voting trustees, proxy holders, and outside directors of firms under SSAs. (pp. 76-77/GAO Draft Report)

Now on p. 42.

DoD Response: Partially concur. The DoD agrees that trustee independence standards apply equally to voting trustees, proxy holders, and outside directors. Trustees are currently required to certify at the time of their nomination that they are "disinterested" individuals with no prior or current contractual, employment, or financial involvement with the foreign investor, the cleared firm or any of its affiliates. However, the DoD does not agree that an annual reaffirmation of "disinterested" status is necessary. The DIS provides an initial briefing to the trustees and advises them of their ongoing responsibility to advise the DIS of any contact with the foreign owner which may affect their "disinterested" status. When such information is received, the DIS provides guidance to the trustee to assure that the new involvement does not impair the independence of the trustee. The DoD agrees that trustees generally should not occupy officer positions. However, exceptions may be granted when appropriate.

See comment 10.

Appendix I
Comments From the Department of Defense

Now on p. 42.

RECOMMENDATION 8: The GAO recommended that as part of the effort addressed in Recommendation 1, the Secretary make changes in the implementation of the existing security arrangements and under the National Industrial Security Program to require selected trustees to sign agreements acknowledging their responsibilities and the specific duties they are required to perform to carry out those responsibilities, including those referenced above. The GAO explained that the agreement should provide that the DoD can remove any trustee if the DoD determines that the trustee failed to perform any of those duties. The GAO further explained that the agreement should ensure that the trustees and the Government have a clear understanding of what is expected of the trustees in performing their security roles. (p. 77/GAO Draft Report)

See comment 11.

DoD Response: Partially concur. Current DoD policy requires trustee acknowledgment of responsibilities in writing. Voting trustees and proxy holders are signatories to the voting trust and proxy agreements. Because SSAs are fundamentally different from trusts and proxies, outside directors under an SSA do not, and need not, be signatories to the SSA. Voting trustees, proxy holders and outside directors are already required to sign a certificate acknowledging the terms and conditions of the FOCI agreement and agree to be bound by, and to accept their responsibilities under those agreements.

See comment 12.

The DoD agrees that trustees should be removed for cause when determined necessary by the DoD. However, removal of trustee directors must be effected by the shareholder, pursuant to applicable law or regulation. Failure of a trustee to fulfill his or her security obligations or other significant responsibilities under the terms of the FOCI agreement would constitute grounds for removal. Importantly, the DoD now has ample leverage to cause removal of trustees by the shareholder should it become necessary. Moreover, removal of trustees generally cannot become effective until the DIS has granted its approval and a qualified successor trustee has been approved by the DIS.

See comment 11.

The DoD does not agree that further enhancements are needed to ensure a clear understanding between trustees and the Government respecting trustee duties. Required certifications, reviews, meetings, and inspections involving the Government and trustees are fully sufficient for educational purposes. Should the DIS identify the existence of shortcomings by a trustee, the agency would work with the trustee to ensure elimination of misunderstanding and enforce compliance.

The following are GAO's comments on the Department of Defense's (DOD) letter dated April 14, 1995.

GAO Comments

1. We have revised the draft report to reflect DOD's comments on the National Industrial Security Program Operating Manual (NISPOM), the Industrial Security Regulation (ISR), and visitation agreements.

2. Lawyers negotiating a new agreement may have significant experience with foreign-owned firms operating under these agreements. Five of the 14 firms we reviewed used the same lawyer. Further, visitation agreements signed before 1993 demonstrate a trend toward loosening controls. For example, an older visitation agreement associated with a proxy agreement stated:

"As a general rule, visits between the Foreign Interest and the cleared Corporation are not authorized; however, the Proxy Holders may approve visits in connection with regular day-to-day business operations pertaining strictly to purely commercial products or services and not involving classified contracts or executive direction or managerial matters."

In contrast, the comparable provision in a newer visitation agreement associated with a proxy agreement was less limiting:

"As a general rule, visits between representatives of the Corporation and those of any Foreign Interest, are not authorized unless approved in advance by the designated Proxy Holder."

According to DOD's comments, baseline visitation controls were developed in 1993. At that time, visitation agreements ceased to exist as separate documents. The visitation controls are now a section of the voting trust, proxy agreement, and special security agreement (SSA). The terms of each agreement type continue to be negotiable.

3. The acquisition of a U.S. defense contractor by a foreign interest can present a higher degree of risk to export-controlled information than other international involvement. In international cooperative programs and joint ventures, the U.S. firm maintains an arms-length relationship with the foreign interests. That is not the case with foreign ownership, when the foreign owner has control or influence over the U.S. firm and access to the U.S. contractor's facilities. The risk of control and influence inherent in foreign ownership is justification for DOD's special foreign ownership,

control, or influence (FOCI) controls. However, the controls used to protect unclassified export-controlled information are limited. Although some of the newer SSAs we reviewed required the protection of export-controlled information, most of the agreements did not. Further, as we reported and DOD acknowledges, the Defense Investigative Service (DIS) does not review the protection of unclassified export-controlled information. In fact, there is no established means for the U.S. government to monitor compliance and ensure enforcement of federal regulations regarding the transfer of export-controlled technical information.

4. None of the six SSAs we reviewed required DIS to approve the replacement of directors. However, the requirement is included in boilerplate SSA language that DOD told us it plans to use in the future.

5. The terms of the distribution agreement were not revised. After negotiating with the proxy holders, the foreign owners agreed to a more liberal, “case-by-case” application of the distribution agreement.

6. DIS oversight did not bring these two cases to light. In both instances, DIS was notified about these situations some time after they occurred. In the first case, DIS was given an anonymous allegation and then pursued it vigorously. In the second case, the proxy holders brought the complaint to DIS, and DIS monitored the proxy holder negotiations with the foreign owner.

7. Trustee approval of visitation requests need not be onerous. This duty is typically carried out by a designated company trustee and involves the occasional receipt, review, and transmittal of approval requests by facsimile machine. Further, at the companies we reviewed, the trustees’ time was not consumed ensuring the economic health of the company. The usual trustee involvement was their attendance at four meetings a year. In making this recommendation, we do not intend to discourage distinguished individuals from accepting appointments as trustees, but rather believe that it would be in the best interest of DOD to encourage individuals who are interested in being proactive trustees to accept these positions.

8. Our recommendation is not that the trustees supervise “each inspection effort” at the company, but that they supervise an inspection of each of the company’s facilities annually. We believe it is a minimal requirement for the trustees to visit each of the company’s facilities once a year to personally assess security.

9. The cited March 1995 “policy change” is a positive step, but this new approach is not documented in any DOD regulation, directive, or policy memorandum. Its only documentation is in the DOD-approved implementing procedures for one recently signed SSA. Further, our recommendation calls for trustee approval of all decisions regarding the facility security officer’s (FSO) pay and continued employment and for trustee supervision of the FSO. Although voting trustees and proxy holders may be currently empowered to review and approve or disapprove the FSO’s selection, they are not required to do so and could delegate this responsibility.

10. Any involvement the trustees have with the foreign owners after their initial certification may not be reported to DOD unless the trustee in question heeds the advice of DIS to report such activities. We believe an annual certification, which should not be onerous, will prevent inadvertent disclosure omissions.

11. The “Acknowledgement of Obligations” portion of the FOCI agreements is too broad and general to clearly identify the trustees’ responsibilities in carrying out their security role. Trustees’ certification of acknowledgement of the broad and general obligations cited in the FOCI agreement will do little to ensure that trustees will play an active role in security oversight. Further, although DIS educational efforts may encourage some trustees to pay greater attention to the security aspects of their role, we feel that the agreement we are recommending will provide baseline performance criteria for all trustees.

12. Following their 1993 survey of foreign-owned U.S. defense contractors, the Defense Intelligence Agency (DIA) and DIS reported the following:

“Most agreements are silent on the authority of the DOD to terminate the arrangement or to dismiss a Proxy Holder, Trustee or outside director. While DIS is normally a party to Special Security Agreements, it is not a party to proxy or trust agreements and therefore lacks standing to intercede when appropriate.”

While DIS is a party to SSAS, if faced with outside directors who are not performing their security duties, the only means for DIS to force corrective action would be to terminate the agreement, thereby causing the company to lose its clearance, and halting all the company’s work on classified contracts. Our recommendation is a more moderate way of removing a nonperforming trustee than revoking a company’s clearance and terminating its classified contracts. We modified our recommendation in

Appendix I
Comments From the Department of Defense

recognition of DOD's comment that the shareholder must remove a trustee director.

Major Contributors to This Report

James F. Wiggins
Davi M. D'Agostino
Peter J. Berry
John W. Yaglenski

Norbert Trapp
Arthur Cobb

Odilon Cuero
Allen Westheimer

Eric L. Hallberg
Deena M. El-Attar

Cornelius P. Williams
Robert R. Tomcho

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

